Plan de Implementación del SGSI basado en la ISO/IEC 27001:2022 de la empresa TRADUX

ESTÍBALIZ BUSTO PÉREZ DE MENDIGUREN

Universitat Oberta de Catalunya

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

Junio 2024

Tutor:

Iñaki Moreno Fernández

Agradecimientos

Quiero expresar mi agradecimiento a todas y cada una de las personas que de forma directa o indirecta han hecho posible el presente Trabajo Fin de Máster.

En primer lugar, agradecer a mi tutor del TFM, Iñaki Moreno Fernández, por haberme permitido llevar a cabo este proyecto; su disposición desde el primer momento ha sido fundamental en su realización.

Asimismo, agradecer también la comprensión y el esfuerzo de todos los profesores que he tenido durante el máster por su dedicación docente.

A mi familia, por orientarme y ayudarme a lo largo de mis estudios para continuar formándome y creciendo tanto personal como profesionalmente. Gracias a su esfuerzo mi deseo se ha hecho realidad.

Finalmente, a todas las personas que he conocido durante mi formación, que han aportado conocimientos y un buen ambiente para seguir aprendiendo.

Poder finalizar el Máster en Ingeniería Informática es algo muy especial y me alegra haberlo podido compartir con todas estas personas mencionadas.
Por todo ello, muchísimas gracias.

Dedicatoria

"Algunas personas miran al mundo y dicen: '¿Por qué?' Otras miran al mundo y dicen '¿Por qué no?'"

George Bernard Shaw

Ficha del Trabajo Final

Título del trabajo:	*Plan de Implementación del SGSI basado en la ISO/IEC 27001:2022 de la empresa TRADUX*
Nombre del autor:	*Estíbaliz Busto Pérez de Mendiguren*
Nombre del consultor/a:	*Iñaki Moreno Fernández*
Nombre del PRA:	*Josep Maria Marco Simó*
Fecha de entrega	*06/2024*
Titulación o programa:	*Máster Universitario en Ingeniería Informática*
Área del Trabajo Final:	*Management de TI*
Idioma del trabajo:	*Castellano*
Palabras clave	*SGSI, ISO 27001:2022, ISO 27002:2022, MAGERIT*

Resumen del Trabajo

La información es uno de los principales activos que posee cualquier organización; por ello, se debe preservar su confidencialidad, integridad y disponibilidad para alcanzar los objetivos del negocio. El objetivo del presente proyecto es la elaboración de un Plan de Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) de la organización ficticia TRADUX, empresa de traducción e interpretación, siguiendo la ISO/IEC 27001:2022.

Se comienza con la descripción de la organización y un análisis diferencial de la ISO 27001:2022 e ISO 27002:2022 como las referencias básicas del documento. Seguidamente, se definen todos los documentos necesarios para el cumplimiento normativo de la ISO 27001:2022 utilizando la metodología de análisis de riesgos basada en MAGERIT. Posteriormente, se proponen diferentes proyectos con el propósito de reducir los principales riesgos encontrados y mejorar la seguridad de la información de dicha organización. Para finalizar, se llevará a cabo la auditoría de cumplimiento donde se evaluará el grado de madurez de los controles de la ISO 27002:2022 y así conocer el estado de seguridad de la información de TRADUX.

Abstract

Information is one of the main assets that any organization has. Its confidentiality, integrity and availability must be preserved to achieve business objectives. Therefore, the objective of this project is the preparation of an Implementation Plan for an Information Security Management

System (ISMS) of the fictitious organization TRADUX, translation and interpretation company, following the ISO/IEC 27001:2022.

It begins with the description of the organization and a differential analysis of ISO 27001:2022 and ISO 27002:2022 as the basic references of the document. Next, all the documents necessary for regulatory compliance with ISO 27001:2022 are defined using the risk analysis methodology based on MAGERIT. Subsequently, different projects are proposed with the purpose of reducing the main risks found and improving the information security of said organization. Finally, the compliance audit will be carried out where the degree of maturity of the ISO 27002:2022 controls will be evaluated and thus know the information security status of TRADUX.

Contenido

Índice de tablas

Índice de figuras

Acrónimos

CCEG: Competencia de Compromiso Ético y Global

CMM: Modelo de Madurez de Capacidad

ENS: Esquema Nacional de Seguridad

IEC: Comisión Electrotécnica Internacional (International Electrotechnical Commission)

ISO: Organización Internacional de Normalización (International Organization for Standardization)

ODS: Objetivos de Desarrollo Sostenible

PDS: Plan Director de Seguridad

PDCA: Plan-Do-Check-Act (PHVA: Plan-Hacer-Verificar-Actuar o Ciclo de Deming)

SGD: Sistema de Gestión Documental

SGSI: Sistema de Gestión de Seguridad de la Información

UOC: Universitat Oberta de Catalunya

IA: Inteligencia Artificial

LSP: Language Service Provider

TIC: Tecnologías de la Información y la Comunicación

CEO: Director Ejecutivo (Chief Executive Officer)

CPD: Centro de Procesamiento de Datos

1. INTRODUCCIÓN

1.1. Contexto y justificación

La **información** es uno de los principales activos que posee una organización; por lo que, si se quieren conseguir los objetivos de negocio, debemos preservar su confidencialidad, integridad y disponibilidad.

Si no se protege la información sensible disponible en la mayoría de los negocios, con casi total seguridad, habrá consecuencias operativas, financieras y legales graves, que incluso pueden llevar a su quiebra. Así que, el reto de las organizaciones es proporcionar una adecuada protección, cómo asegurar que han identificado los riesgos y cómo gestionarlos de forma proporcionada, sostenible y efectiva.

Dicho esfuerzo por incrementar los niveles de ciberseguridad ha dado como resultado la actualización de dos normas clave: el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS) y la norma ISO/IEC 27001:2022. Ambas han experimentado importantes modificaciones para afrontar los retos provocados por las nuevas amenazas, fortaleciendo los programas e iniciativas de seguridad, y facilitando la compatibilidad entre ambas y sus medidas y controles de seguridad.

Pese a la buena sinergia y reciprocidad entre las dos normas y la posibilidad de desplegar sistemas de gestión, también hay que canalizar sus particularidades y diferencias, sin las cuales, no se podrá optar a mantener un sistema capaz de afrontar la conformidad de ambas. Por lo que, dada la envergadura de las dos normas, este proyecto se basará en la elaboración de un Plan de Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) de la organización ficticia TRADUX, empresa de traducción e interpretación, basado en:

- La norma ISO/IEC 27001:2022 detalla y proporciona los requisitos para para la implementación, mantenimiento y mejora continua de un SGSI. Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.

- La norma ISO/IEC 27002:2022 proporciona buenas prácticas para seleccionar, implementar y mantener controles dentro del proceso de implantación de un SGSI basado en la norma ISO/IEC 27001:2022.

- La metodología de análisis de riesgos ligera basada en MAGERIT para analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas

que pueden afectarle y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

1.2. Motivación

Vivimos en un mundo globalizado donde los avances tecnológicos nos han permitido acortar distancias. Sin embargo, en ocasiones las diferencias culturales e idiomáticas pueden separarnos.

El **sector lingüístico** evoluciona vertiginosamente para adaptarse a las necesidades comerciales actuales y en gran parte se debe a la transformación digital. A medida que las empresas se vuelven más digitales, la **seguridad** de los datos también aumenta su complejidad; por ello, la evaluación de riesgos y las auditorías de seguridad son la norma habitual durante la presentación de propuestas de traducción.

Las nuevas tecnologías aumentan las vulnerabilidades de seguridad, de vital importancia para proteger los datos, activo que debe ser gobernado correctamente para alcanzar el éxito de cualquier negocio. Insistir, sin titubeos, en la importancia de la concienciación y sensibilización de todo el personal de cualquier tipo de organización, como punto de partida en el futuro éxito de la implementación de un SGSI.

Por ello, mi gran interés por la seguridad, unido a mi deseo de reducir distancias provocadas por las diferencias idiomáticas, ha hecho que me decidiera por este proyecto como Trabajo de Fin de Máster "Plan de Implementación del SGSI basado en la ISO/IEC 27001:2022 de la empresa TRADUX".

1.3. Objetivos

El objetivo principal de este Trabajo de Fin de Máster es elaborar, desarrollar e implementar el SGSI en TRADUX basado en los estándares ISO 27001:2022 e ISO 27002:2022 utilizando la metodología de análisis de riesgos ligera basada en MAGERIT, ya indicado anteriormente.

Para ello, los objetivos específicos son:

- Conocer el estado actual de Seguridad de TRADUX en torno al cumplimiento de las normas ISO 27001:2022 e ISO 27002:2022 (Anexo A).
- Identificar y gestionar los riesgos de seguridad de la información.
- Utilizar la metodología de análisis de riesgos ligera basada en MAGERIT.
- Definir las propuestas de proyectos para implementar mejoras y medidas de control adecuadas que permitan mitigar los riesgos encontrados.

- Realizar una auditoría de cumplimiento que evaluará el grado de madurez de los controles realizados en torno al cumplimiento de la ISO 27002:2022.
- Crear un plan de concienciación y formación para todo el personal de la organización encaminado a conseguir una mejor seguridad de los activos de la información.

Todos estos objetivos se irán consiguiendo a lo largo de las entregas parciales que se realizarán en el tiempo marcado por la ficha docente correspondiente.

1.4. Impacto ético, social y ambiental

La Universitat Oberta de Catalunya (UOC) está públicamente comprometida con la Competencia de compromiso ético y global (CCEG) y los Objetivos de Desarrollo Sostenible (ODS), los cuales se incluyen en el programa del máster con la siguiente definición:

> *"Actuar de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional, y diseñar soluciones para mejorar estas prácticas."*

La CCEG aborda tres grandes dimensiones (Tabla 1-1) alineadas con los ODS. De los 17 objetivos que integran los ODS se señalarán y analizarán únicamente aquellos objetivos relacionados con el presente documento en sus diferentes etapas [1]:

DIMENSIONES ALINEADAS CON LOS OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS) RELACIONADOS CON LA COMPETENCIA DE COMPROMISO ÉTICO Y GLOBAL (CCEG)			
	DISEÑO	**DESARROLLO**	**CONCLUSIONES**
Dimensión I. Sostenibilidad			
ODS 7. Energía asequible y limpia. **ODS 9. Industria, innovación e infraestructura.** **ODS 11. Ciudades y comunidades sostenibles.** **ODS 12. Consumo y producción responsable.** **ODS 13. Acción climática.** **ODS 14. La vida bajo el agua.** **ODS 15. La vida en la tierra.**	ODS 9	ODS 9 ODS 12	ODS 9
Dimensión II. Comportamiento ético y responsabilidad social (RS)			
ODS 1. No pobreza. **ODS 2. Hambre cero.** **ODS 3. Salud y bienestar.** **ODS 6. Agua limpia y saneamiento.** **ODS 8. Trabajo decente y crecimiento económico.** **ODS 16. Paz, justicia e instituciones sólidas.** **ODS 17. Alianzas para lograr objetivos.**		ODS 8 ODS 16 ODS 17	ODS 16

Dimensión III. Diversidad (género entre otros) y derechos humanos			
ODS 4. Educación de calidad. **ODS 5. Igualdad de género.** **ODS 10. Desigualdades reducidas.**	ODS 4 ODS 5 ODS 10	ODS 4 ODS 5	ODS 4 ODS 5

Tabla 1-1. Dimensiones alineadas con los Objetivos de Desarrollo Sostenible (ODS) relacionados con la Competencia de Compromiso Ético y Global (CCEG).
Fuente: Elaboración propia a partir de https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

A la hora de diseñar este documento, se ha tenido en cuenta que su información sea accesible a todos los usuarios potenciando la inclusión de todas las personas independiente de su edad, sexo, discapacidad, raza, origen, religión o situación económica garantizando la igualdad de oportunidades como indica el **ODS 10** (Desigualdades reducidas) sobre Diversidad y derechos humanos.

Durante el desarrollo del presente TFM, se ha considerado el **ODS 12** (Consumo y producción responsable) sobre Sostenibilidad. Debido a la gran demanda de sitios Web no debemos usar las tecnologías modernas sin control, sino ayudar a los países en desarrollo a fortalecer su capacidad científica y tecnológica para avanzar hacia un consumo y producción más responsable.

Por otro lado, si trabajamos con tecnologías modernas, la seguridad y protección de datos de los usuarios estará mejor garantizada. Esta es una manera de prevenir injusticias imposibilitando el cometido del delito en sí y abordando el **ODS 16** (Paz, justicia e instituciones sólidas) sobre Comportamiento ético y responsabilidad social. Todo ello, en base a conseguir la paz, justicia e instituciones sólidas ya que la inseguridad, las instituciones débiles y el acceso limitado a la justicia continúan suponiendo una grave amenaza para el desarrollo sostenible.

Además, promover el desarrollo de tecnologías, así como su divulgación y difusión a los países en desarrollo en condiciones favorables, según lo convenido de mutuo acuerdo, como indica el **ODS 17** (Alianzas para conseguir los objetivos). Para alcanzar este Objetivo de Desarrollo Sostenible, los gobiernos, la sociedad, los científicos, el mundo académico y el sector privado deben estar unidos.

Tanto en el diseño como en las conclusiones de este documento, se reafirmará cómo la innovación y el progreso tecnológico son claves para descubrir soluciones duraderas para los desafíos económicos; por ello, se apoya el acceso a la tecnología y comunicaciones esforzándose por proporcionar el acceso a Internet en los países menos adelantados, como se indica en el **ODS 9** (Industria, innovación e infraestructura) sobre la Sostenibilidad.

Además, en las tres fases de este proyecto (diseño, desarrollo y conclusiones), se ha tenido en cuenta la importancia de recibir una educación de calidad para llevar a cabo proyectos como el presente. Gracias al progreso económico y social aumenta el número de jóvenes y adultos con competencias necesarias, en particular técnicas y profesionales, para acceder al empleo, el trabajo decente y el emprendimiento, abordando el **ODS 4** (Educación de calidad).

Por último, en ninguno de los tres momentos claves citados en el párrafo anterior, se percibe la discriminación de género. La igualdad de género no sólo es un derecho humano, sino que es uno de los fundamentos esenciales para construir un mundo pacífico, próspero y sostenible, aspecto abordado en el **ODS 5** (Igualdad de género) sobre Diversidad y derechos humanos.

1.5. Metodología

Los métodos y las técnicas de investigación son los procedimientos seguidos por los investigadores para obtener los datos necesarios en su aproximación al objeto de estudio; según el objetivo deseado en la elaboración del presente proyecto, los tipos de metodología de investigación serán [2]:

- Según su propósito, se llevará a cabo un tipo de investigación **teórica**, cuyo objetivo es obtener información de diferente naturaleza. Estos conocimientos no son aplicados, únicamente son útiles para tener un conocimiento general centrado en el tema elegido.

- Según la profundidad del objeto de estudio, la metodología utilizada será tanto de investigación exploratoria como descriptiva y explicativa [3]:

    - Al comenzar la lectura de conceptos relacionados directamente con este TFM, así como con los estándares ISO 27001:2022 e ISO 27002:2022 y la metodología de Análisis de Riesgos basada en MAGERIT, se utiliza una metodología **exploratoria** cuyo objetivo es tener un primer contacto y una visión general que nos permita investigar, analizar y establecer las bases para la investigación, a partir de la información y documentación obtenida para dicho propósito.

    - Tanto para realizar un informe detallado sobre el Plan de Implementación del SGSI, sus características y configuración, como para profundizar en su desarrollo se utiliza una metodología **descriptiva.** Dicha investigación permite definir, clasificar, catalogar o caracterizar con minuciosidad el objeto de estudio ya definido en este párrafo.

    - Para tratar más profundamente se utiliza una metodología **explicativa**, que permite entender de forma eficiente el tema objeto de investigación del presente proyecto.

Las técnicas utilizadas en la elaboración de este TFM con el propósito de elaborar y desarrollar el Plan de Implementación del SGSI de TRADUX serán la **investigación documental** y la **recopilación de información** obtenida a través del estudio e investigación de diferentes guías, manuales, documentos, páginas webs, foros … previamente seleccionadas e indicadas al final de este documento en la BIBLIOGRAFÍA.

1.6. Planificación del Trabajo

La Figura 1-1 muestra la planificación temporal de este documento definida en el diagrama de Gantt:

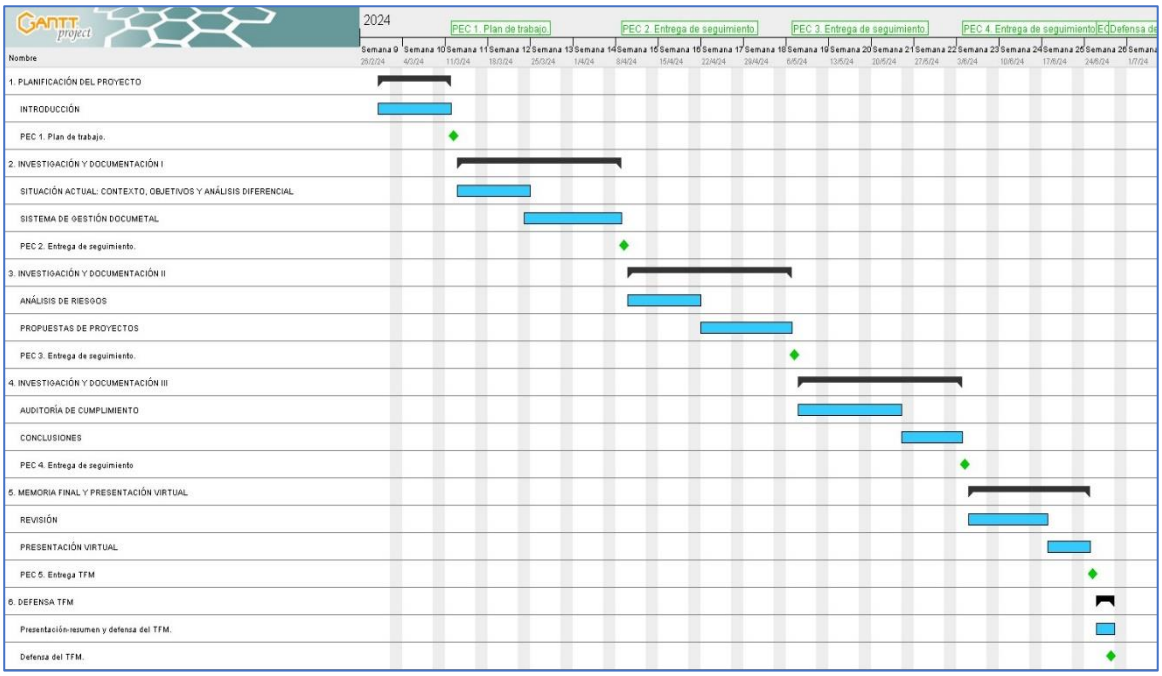

Figura 1-1. Planificación del Trabajo definida mediante el diagrama de Gantt.
Fuente: Elaboración propia.

1.6.1. Riesgos del proyecto

A modo de reflexión, en este subapartado dentro de la planificación del proyecto se llevará a cabo un breve análisis de los riesgos de este, ligado con los nuevos conocimientos sobre el Plan de Implementación de un SGSI objeto de estudio. Este nuevo conocimiento implica un alto grado de incertidumbre que conlleva superar los límites del denominado estado del arte, en este caso se refiere al límite del conocimiento humano acerca de dicha materia. Esto hace que la gestión de riesgos en este tipo de proyectos de investigación sea aún más crítica que en otros, ya que cuanto mayor sea el nivel de incertidumbre, mayor será el número de riesgos presentes en el mismo [4].

A continuación (Tabla 1-2), se analizarán los principales riesgos de este proyecto [5]:

TIPO DE RIESGO	DESCRIPCIÓN DEL PROBLEMA	PLAN DE ACCIÓN
Riesgos de objetivos	No se deben proponer objetivos que sean imposibles de alcanzar debido a la breve experiencia profesional en desarrollar el Plan de Implementación del SGSI.	Apoyarse en la experiencia de la dirección del proyecto y elegir documentación de fuentes fiables.

Riesgos de personal	El hecho de desarrollar nuevos conocimientos en este proyecto de investigación requerirá un equipo especializado integrado por investigadores con experiencia.	Dado que el proyecto se lleva a cabo por una persona investigadora, la dirección debe ser consciente tanto de sus aportaciones como sus limitaciones para no perder el ritmo de trabajo.
Riesgos de coordinación	La colaboración y comunicación entre la dirección y la persona investigadora del proyecto son dos aspectos prioritarios para llevar a cabo su realización: intercambio de información, resolución de dudas, comentarios sobre las diferentes entregas …	Desde el inicio del proyecto la dirección ha determinado tanto la forma de contacto como su flexibilidad para posibles modificaciones. Ambas partes están de acuerdo y en constante comunicación para evitar problemas al respecto y avanzar según lo previsto.
Riesgos de cumplimiento de plazo	El retraso de las entregas es uno de los grandes inconvenientes a los que se enfrenta este proyecto.	Aunque resulte complicado prever los tiempos de ejecución, la persona investigadora debe cumplir con las fechas de entrega para no realizar retrasos "en cascada".
Riesgos tecnológicos	Para poder cumplir lo referido en el apartado 1.3. Objetivos, el presente proyecto depende, en gran parte, del buen funcionamiento de la tecnología.	Ir avanzando según la planificación realizada para poder hacer frente a posibles complicaciones, si las hubiera.
Riesgos económicos	La variabilidad en los costes estimados afectaría a lo tratado en el apartado 1.9. Recursos necesarios y presupuesto del proyecto; sería un gran contratiempo totalmente inesperado.	Si bien es cierto que el material utilizado no resultaría difícil remplazarlo (en cuanto a su adquisición), conllevaría un sobrecoste económico imprevisto en el presente proyecto.

Tabla 1-2. Riesgos del proyecto.
Fuente: Elaboración propia a partir de HERRERO, P. Riesgos que se deben dominar al gestionar un proyecto. Sage Group. (2023). Obtenido de https://www.sage.com/es-es/blog/riesgos-que-se-deben-dominar-al-gestionar-un-proyecto/

1.7. Productos obtenidos

La Tabla 1-3 muestra los entregables obtenidos durante la elaboración del presente TFM:

ENTREGA	CONTENIDO	FECHA
PEC 1. Entrega del Plan de Trabajo	Primera entrega con el Plan de Trabajo desarrollado a lo largo del capítulo 1. INTRODUCCIÓN.	12/03/2024
PEC 2. Entrega de seguimiento	Segunda entrega de una parte de la memoria final donde se desarrollarán los capítulos: 2. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL. 3. SISTEMA DE GESTIÓN DOCUMENTAL.	9/04/2024
PEC 3. Entrega de seguimiento	Tercera entrega de una parte de la memoria final donde se desarrollarán los capítulos:	7/05/2024

	4. ANÁLISIS DE RIESGOS. 5. PROPUESTAS DE PROYECTOS.	
PEC 4. Entrega de seguimiento	Cuarta entrega de una parte de la memoria final donde se desarrollarán los capítulos: 6. AUDITORÍA DE CUMPLIMIENTO. 7. CONCLUSIONES.	4/06/2024
PEC 5. Entrega TFM	Memoria final del presente documento y su presentación virtual.	25/06/2024
Defensa del TFM	Tras la defensa del TFM, existe un período de tiempo en el cual el tribunal realiza una serie de preguntas a las que se debe responder.	30/06/2024

Tabla 1-3. Productos obtenidos durante la elaboración del presente proyecto.
Fuente: Elaboración propia a partir de las normas establecidas por la UOC.

1.8. Estructura del Trabajo

El presente documento se estructura en siete capítulos descritos a continuación:

1. INTRODUCCIÓN. Se establece el contexto y la justificación, así como la motivación que ha llevado a la realización del proyecto. Para ello, se enumeran los objetivos, se estudia el impacto ético, social y ambiental, se describe la metodología y las técnicas de investigación, así como la planificación temporal. Se continúa con la enumeración de los productos obtenidos durante su elaboración y se inicia la revisión del estado del arte. Para finalizar, se lleva a cabo una descripción de los recursos necesarios y el presupuesto del proyecto.

2. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL. Conocer la organización TRADUX, definir los objetivos y realizar un análisis diferencial con respecto la norma ISO/IEC 27001:2022 y las mejores prácticas descritas en ISO/IEC 27002:2022, consideradas como las referencias básicas del documento.

3. SISTEMA DE GESTIÓN DOCUMENTAL. Análisis de los documentos en los que se sustenta el Sistema de Gestión Documental (SGD) establecidos en la ISO/IEC 27001:2022: política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por la dirección, gestión de roles y responsabilidades, metodología gestión de riesgos y declaración de aplicabilidad.

4. ANÁLISIS DE RIESGOS. Identificar la situación actual de TRADUX utilizando la metodología de análisis de riesgos ligera basada en MAGERIT: inventario y valoración de activos, dimensiones de seguridad, análisis de amenazas, impacto potencial y nivel de riesgo aceptable y riesgo residual.

5. PROPUESTAS DE PROYECTOS. Identificar los proyectos para implementar en el SGSI en el marco de mejora de los controles de seguridad y poder reducir o mitigar los niveles de riesgos encontrados en la etapa anterior de análisis de riesgos.

6. AUDITORÍA DE CUMPLIMIENTO. Analizar la metodología, el alcance, la evaluación de la madurez y la presentación de resultados utilizando el Modelo de Capacidad de Madurez (CMM) de la ISO/IEC 27002:2022.

7. CONCLUSIONES. Se analizarán las conclusiones, las dificultades tenidas, los objetivos superados y las líneas de futuro trabajo a partir del presente proyecto.

GLOSARIO DE TÉRMINOS seleccionados y ordenados alfabéticamente para agilizar su búsqueda.

BIBLIOGRAFÍA con la lista numerada de las referencias bibliográficas utilizadas en la memoria.

ANEXOS con información extra o complementaria de algunos temas que poseen un especial interés para el lector y cuyo objetivo es ampliar el contenido del documento principal.

1.9. Recursos necesarios y presupuesto del proyecto

Antes de finalizar este capítulo, se hará referencia a cómo se ha presupuestado el presente proyecto en base a los recursos utilizados y el coste de cada uno de ellos (Tabla 1-4):

RECURSOS	USO	COSTES UNITARIOS	COSTES
Ordenador	Búsqueda y recopilación de la información para la posterior elaboración de la memoria final.	1.200 €	1.200 €
Conexión a Internet	Recopilación de datos.	38 € / mes	152 €
Herramientas	Aplicación de edición de textos.	0 €	0 €
Analista de seguridad	Número de horas para la preparación del TFM por un analista junior de seguridad 50+75+75+75+20+5 = 300 horas	28 € / h	8.400 €
COSTE TOTAL			**9.752 €**

Tabla 1-4. Costes asociados al proyecto.
Fuente: Elaboración propia.

2. SITUACIÓN ACTUAL: CONTEXTO, OBJETIVOS Y ANÁLISIS DIFERENCIAL

Antes de comenzar con el desarrollo del presente capítulo y como punto de partida en la elaboración del plan de implementación del SGSI, se considera de suma importancia tener una información básica sobre el origen, evolución, novedades y estructura tanto de las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 como de los beneficios de la implantación de un SGSI.

Para facilitar el acceso a dicha información, se indican los enlaces correspondientes:

Sobre el origen, la evolución, las novedades y la estructura de la ISO/IEC 27001:2022 con respecto a la versión anterior, véase el Anexo I. ISO/IEC 27001:2022

Sobre el origen, la evolución, las novedades y la estructura de la ISO/IEC 27002:2022 con respecto a la versión anterior, véase el Anexo II. ISO/IEC 27002:2022

Sobre los beneficios de la implantación de un SGSI y Ciclo de Deming o PDCA aplicado a los Sistemas de Gestión de Seguridad de la Información, véase el Anexo III. Beneficios de la implantación del SGSI y Ciclo de Deming o PDCA.

2.1. Contextualización

TRADUX es una pequeña empresa ficticia, creada a finales de 2022, especializada en proyectos de traducción e interpretación, en más de 18 idiomas para clientes de diferentes sectores.

2.1.1 Actividad de la empresa

La Tabla 2-1 muestra los servicios que TRADUX ofrece a sus clientes y, posteriormente, se define su modelo de negocio.

TRADU	
TRADUCCIÓN	**INTERPRETACIÓN**
Traducción de textos literarios, técnicos, científicos, jurídicos, cartas comerciales...	Interpretación simultánea en coloquios, congresos, formaciones, discursos...
Traducción de catálogos, manuales de instrucciones, páginas webs...	Interpretación bilateral en notarías, firmas de contratos, reuniones comerciales, llamadas telefónicas, conversaciones del día a día, visitas al médico…

Tabla 2-1. Servicios de TRADUX.
Fuente: Elaboración propia.

Modelo de negocio

Teniendo en cuenta que un modelo de negocio es la planificación que realiza una empresa para tratar de recibir ganancias y beneficios, el modelo de negocio de TRADUX (Figura 2-1) consta de los siguientes bloques tomados de Alexander Osterwalder, padre del Business Model Canvas y uno de los expertos más prestigiosos en el mundo de los negocios [14]:

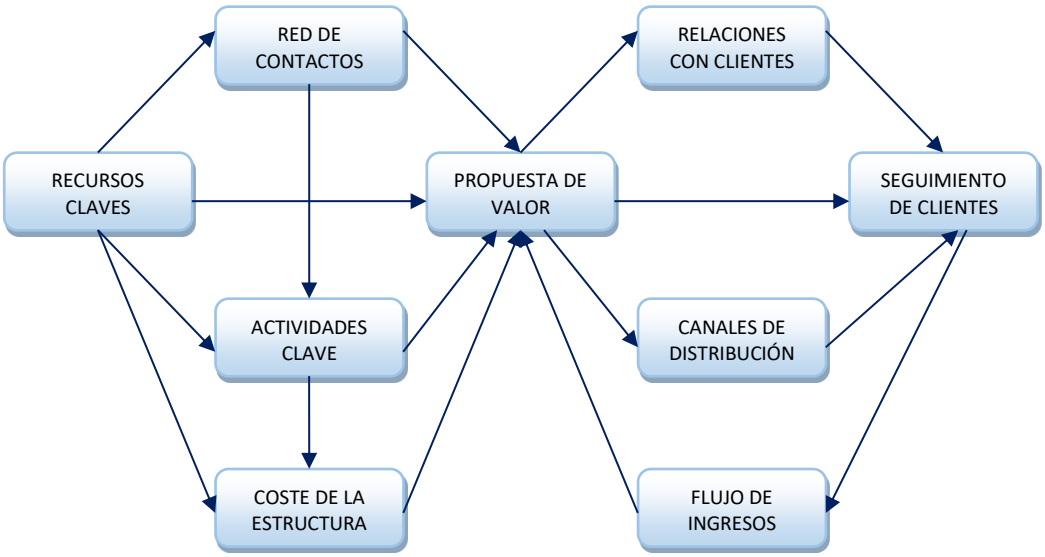

Figura 2-1. Relación entre bloques del modelo de negocio de la empresa.
Fuente: Elaboración propia a partir de https://anabenayasvaldes.wordpress.com/2011/11/06/modelo-de-negocio-para-una-empresa-de-traduccion-e-interpretacion/

La propuesta de valor se distingue por su amplia gama de idiomas y servicios, lo que permite ofrecer precios competitivos y tiempos de entrega rápidos. Además, TRADUX coordina proyectos de manera eficiente, siguiendo estrictas pautas de calidad para asegurar un servicio de traducción de alto nivel. Esta dedicación a la excelencia no sólo garantiza la satisfacción del cliente, sino que posiciona a la

empresa para aprovechar más oportunidades en concursos y licitaciones, respaldada por certificaciones de calidad que validad su compromiso con la excelencia en la traducción.

Los recursos claves que utiliza para llevar a cabo su trabajo incluyen software de traducción, memorias de traducción, base de datos con terminología, Internet y diccionarios, tanto electrónicos como manuales, un equipo humano altamente cualificado y la ubicación de la agencia, respaldando así su propuesta de ofrecer precios competitivos y tiempos cortos.

La red de contactos son los proveedores que les proveen de lo necesario para realizar su trabajo como son los softwares, el hardware, Internet, los materiales y el mobiliario de oficina, la red de traductores y la red de clientes.

Las actividades clave son la traducción, la interpretación, la revisión de textos, la maquetación, la creación de glosarios y de memorias, la gestión de proyectos y la formación de traductores.

El coste de la estructura es el dinero que gastan para pagar a los proveedores (hardware, software, Internet, materiales de referencia y de oficina), en comunicación y publicidad, en gastos del local puesto que es de alquiler, así como en la formación, seguridad social y salario de los trabajadores.

Las relaciones con los clientes son a través de diversos canales como correo electrónico, videollamada, teléfono, reuniones, visitas y conferencias.

El segmento de clientes es diverso, puesto que este incluye empresas de diversos sectores, instituciones gubernamentales, organizaciones sin fines de lucro y clientes particulares.

Los canales de distribución son directamente con el cliente final o mediante acuerdos con las instituciones.

El flujo de ingresos proviene de los servicios de traducción e interpretación, de la creación de recursos, de la revisión de textos y de los cursos de formación.

Identificar y evaluar los riesgos en cada bloque del modelo de negocio permite anticiparse a problemas potenciales y desarrollar estrategias de mitigación efectivas.

Por ello, resulta fundamental plasmar todos estos elementos en el análisis de riesgos, ya que cada uno de ellos puede presentar desafíos específicos que deben ser gestionados para asegurar la estabilidad y el crecimiento de TRADUX.

La competencia feroz, la dependencia de tecnología y personal calificado, las relaciones con proveedores y clientes, los costos operativos y las fuentes de ingresos son áreas que, si no se gestionan adecuadamente, pueden afectar significativamente la operatividad y la rentabilidad de la empresa.

Por ello, un análisis detallado y continuo de estos riesgos es esencial para la sostenibilidad y éxito a largo plazo de TRADUX.

A continuación, la Figura 2-2 sintetiza el modelo de negocio de la empresa objeto de estudio; para posteriormente, comenzar con un nuevo apartado sobre el organigrama de la empresa y las funciones del personal de TRADUX.

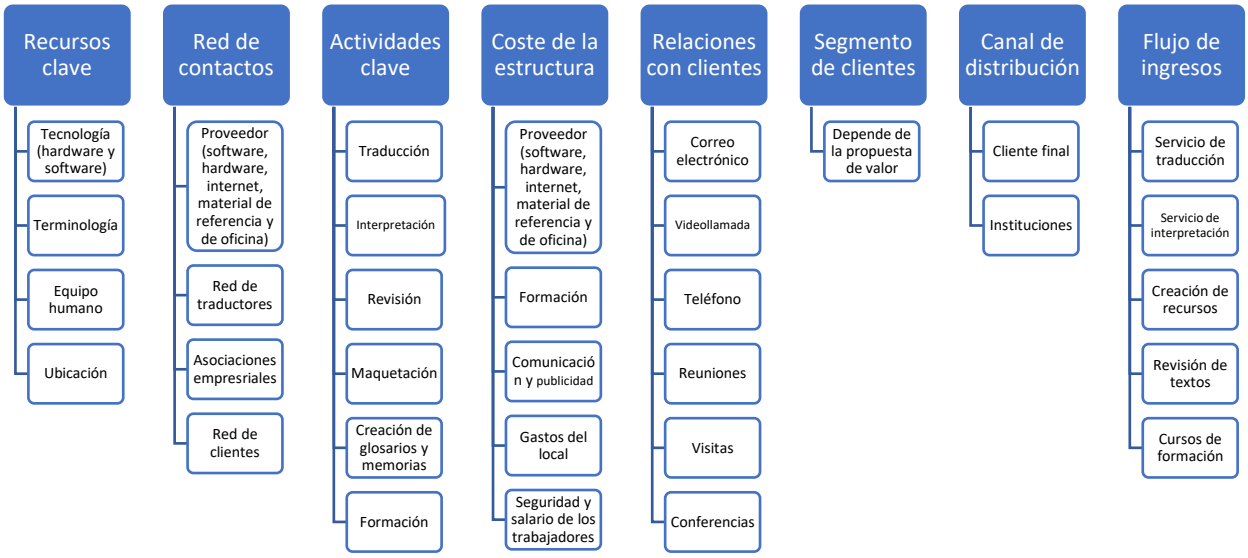

Figura 2-2. Modelo de negocio de TRADUX.
Fuente: Elaboración propia.

2.1.2 Organigrama de la empresa

A pesar de su corta trayectoria en el mercado, TRADUX centra su experiencia, talento y conocimiento de sus 24 profesionales altamente cualificados, quienes son fundamentales para brindar en la eficacia, rapidez y confianza a sus clientes, aspectos claves para el éxito de su negocio. Todos los empleados poseen titulados universitarios en diversas áreas, incluyendo traducción, interpretación, lingüística, maquetación, ingeniería informática, marketing, contabilidad, gestión de proyectos, recursos humanos, tecnologías de traducción, etc. Dichos profesionales se distribuyen como se muestra en el organigrama (Figura 2-3) y realizan las funciones que se indican a continuación:

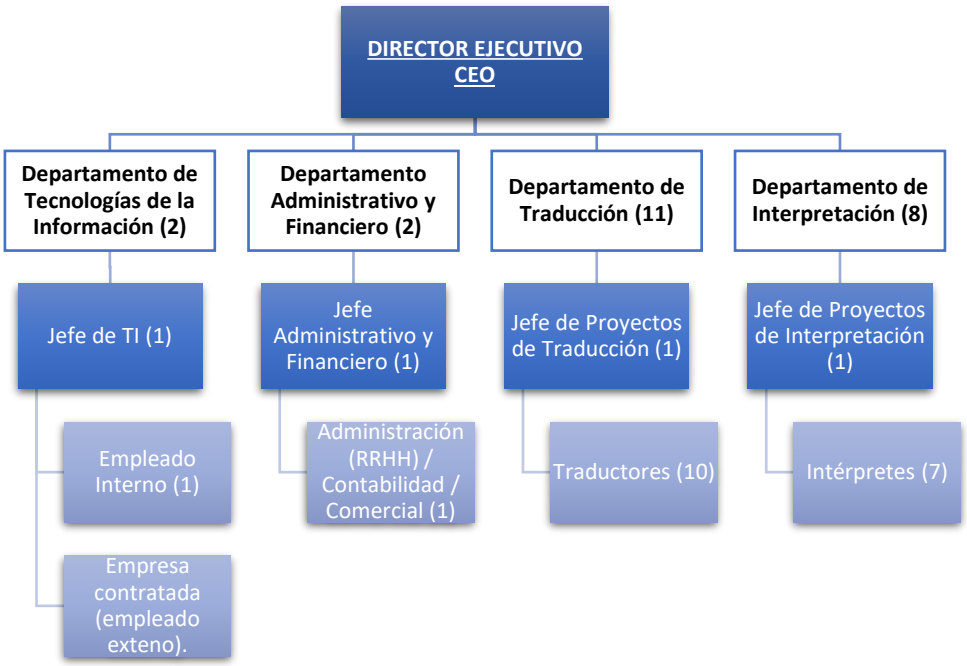

Figura 2-3. Organigrama de la empresa TRADUX.
Fuente: Elaboración propia.

2.1.3 Funciones del personal

El equipo directivo está formado por el Director Ejecutivo (CEO), el Jefe de Tecnologías de la Información (TI), el Jefe Administrativo y Financiero, el Jefe de Traducción y el Jefe de Interpretación. A su vez, estos jefes son los máximos representantes de los cuatro departamentos de la empresa.

Las funciones de los 24 profesionales que trabajan en TRADUX son las siguientes:

- Director Ejecutivo (1). Fundador y director ejecutivo. Como máximo responsable, toma las decisiones más importantes y dirige las estrategias para que la empresa alcance sus objetivos.

- Jefe de Tecnologías de la Información (TI) (1). Como responsable de la tecnología y la información, garantiza y fomenta la innovación tecnológica, gestiona los recursos informáticos y se asegura de que los empleados estén capacitados y actualizados en las nuevas tecnologías, así como de mantener la competitividad de la empresa en el mercado digital. Lleva el registro de activos y pasivos de la empresa.

- Empleado interno (1). Responsable de instalar y configurar equipos (hardware y software), ya sean informáticos o de telecomunicaciones, e integrarlos en un sistema de redes. Se encarga de la instalación del sistema completo, con todos sus componentes (ordenadores, servidores, etc.). Depende directamente del jefe de TI. Además, es la persona que mantiene contacto con el proveedor, el cual es un empleado externo con quien trabaja.

- Jefe Administrativo y Financiero (1). Encargado de la planificación económica y financiera de la empresa. Como figura muy cercana al CEO, siempre se asegura del correcto funcionamiento y gestión de la inversión y la financiación. De esta figura dependen directamente Recursos Humanos, Contabilidad y Administración y compras.

- Responsable de Administración (RRHH) / Contabilidad / Comercial (1). Gestiona lo relacionado con las personas que trabajan en la empresa: reclutamiento, selección, contratación, bienvenida, formación, promoción, nóminas y despidos. Evalúa las necesidades de la empresa comparando y negociando precios, al tiempo que se ocupa de las relaciones con proveedores.

- Jefe de Proyectos de Traducción e Interpretación (2). Responsable de coordinar, gestionar y supervisar todo el proceso, desde que se aprueba el proyecto hasta que se entrega al cliente. Sus principales funciones son diseñar un plan de acción, tomar las decisiones necesarias para ejecutarlo y obtener los resultados que busca TRADUX. De esta figura dependen directamente su equipo de traductores y/o intérpretes.

- Traductores (11) / Intérpretes (8). Dada la corta vida de la empresa y aunque sus competencias están claramente diferenciadas, ambas figuras se reparten sus funciones dependiendo de la demanda (Tabla 2-2).

- Estudiantes de grado y/o máster. Sin definir el número de estudiantes de último curso que realizan prácticas tanto curriculares como extracurriculares y cuyo tutor es el gestor de proyecto y/o el traductor o intérprete del sector del servicio correspondiente.

2.1.4 Infraestructura tecnológica de la empresa

La infraestructura tecnológica de TRADUX se caracteriza por su enfoque descentralizado, donde se prioriza la distribución y colaboración de los recursos digitales. En lugar de depender de una única entidad centralizada, ha adoptado una arquitectura de red descentralizada que promueve la resiliencia y la seguridad de sus operaciones, esto lo convierte en una "empresa inteligente" [15].

Dicha infraestructura, compuesta por una variedad de equipos y tecnologías digitales, refleja la descentralización en varios aspectos clave:

- TRADUX ha implementado una red de ordenadores para el teletrabajo que se conectan a través de una VPN, lo que permite un acceso remoto seguro sin depender de una ubicación física centralizada. Además, la empresa utiliza un firewall central para proteger la red interna, lo que indica un enfoque distribuido en la seguridad de la red al filtrar el tráfico de Internet desde múltiples puntos de acceso.

- El enrutador y el conmutador se encargan de dirigir el tráfico de datos, conectando los ordenadores de oficina y distribuyendo la conexión a Internet de manera descentralizada, lo que garantiza una mayor redundancia y eficiencia en la comunicación interna.

- Por último, la infraestructura de TRADUX aprovecha la nube de Microsoft Azure, donde los datos de los servidores de bases de datos, correo y web se encuentran alojados. Esto refleja una distribución de recursos digitales fuera de las instalaciones físicas de la empresa, proporcionando un acceso flexible y seguro a los datos desde múltiples ubicaciones (Figura 2-4).

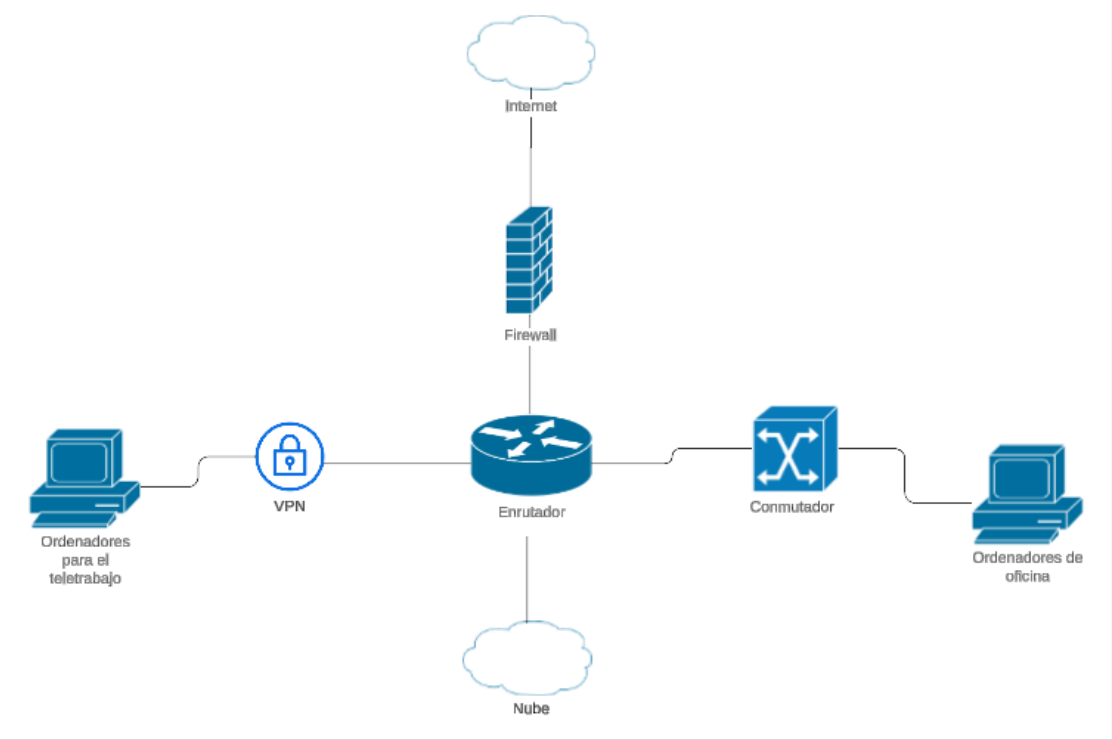

Figura 2-4. Infraestructura tecnológica de la empresa.
Fuente: Elaboración propia.

2.1.5 Estado inicial de la seguridad de la información

La seguridad de los datos es la máxima prioridad para todo proveedor de servicios lingüísticos (Language Service Provider). Los LSP poseen un papel fundamental ya que tratan con una enorme cantidad de datos sensibles de los clientes (información financiera, propiedad intelectual, datos de los empleados, etc.).

Aunque TRADUX es una empresa es de reciente creación y se encuentra en una fase inicial en cuanto a su seguridad se refiere, está comprometida con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022. Este compromiso busca proporcionar la máxima seguridad que le permita alcanzar su éxito empresarial, aumentar la confianza de sus clientes y aprovechar más oportunidades en conseguir nuevos proyectos.

Actualmente, las necesidades en cuanto a seguridad de la información de cualquier tipo de empresa se encuentran fundadas en tres principios (Figura 2-5) [16]:

Figura 2-5. Principios fundamentales para la seguridad de la información de una empresa.
Fuente: Elaboración propia. Obtenido de https://pe.isotools.us/iso-27001-requisitos-basicos-para-aumentar-seguridad-tic/

A continuación, se indicarán los aspectos más relevantes que afectan a dicho estado:

- Concienciación y formación de los empleados. Aunque TRADUX cuenta con el apoyo de la Dirección y empleados cualificados para obtener la certificación ISO/IEC 27001:2022, actualmente no existe un plan de acción estructurado ni asignaciones específicas para la seguridad de la información. Esta falta de planificación detallada podría resultar en una implementación ineficaz del SGSI, dejando a la organización vulnerable a riesgos de seguridad no identificados o mal gestionados. Además, la responsabilidad de la seguridad de la información recae en gran medida en los empleados, quienes, a pesar de su concienciación y formación, pueden no estar preparados para abordar todos los problemas de seguridad que surjan. Específicamente, la dependencia de un solo empleado interno del Departamento de TI para la seguridad general de la empresa y la gestión de los procesos y sistemas de todos los

servicios plantea un punto único de fallo que podría ser explotado o resultar en una sobrecarga de trabajo que comprometa la seguridad.

- Acceso físico a las instalaciones. El acceso a los diferentes pasillos donde se encuentran las salas o los despachos se realiza sin ningún tipo de control, no existen tarjetas de visita ni se registran los visitantes o clientes que entran en las instalaciones de la empresa. Cada empleado dispone de un despacho. Además, existen otras salas, de mayor tamaño, donde pueden reunirse con otros compañeros o clientes, que normalmente están cerradas con llave.

  Cada uno de los dos servicios ofrecidos por TRADUX, traducción e interpretación, dispone de un laboratorio propio en el que se encuentra disponible el equipamiento necesario para llevar a cabo sus proyectos. Estos laboratorios se abren con una llave diferente a las salas anteriores y suelen permanecer cerrados cuando no son utilizados.

- Inventario. La empresa tiene conocimiento de todos sus equipos, pero no posee ningún inventario de activos detallado ni ha realizado nunca un análisis de riesgos.

  Cada servicio dispone de una impresora de red ubicada en una de las salas del grupo a la que sólo se puede acceder si el empleado se encuentra en la misma LAN que la impresora, por lo que habitualmente sólo es utilizada por los trabajadores de cada servicio en el que se encuentra la impresora. Además, en la sala donde se encuentra el departamento Administrativo y Financiero hay otra impresora que puede utilizar cualquier empleado.

  En cada uno de los despachos del equipo directivo existe una pequeña caja fuerte con una combinación numérica que contiene la llave de cada una de las salas de mayor tamaño de cada servicio y de los laboratorios. La combinación numérica no suele cambiarse a menudo y es conocida por todos los miembros del equipo directivo y por el empleado interno del departamento de TI.

- Equipamiento y acceso a Internet. La seguridad de los equipos es limitada, no se realizan cambios periódicos de contraseñas y no existe una política de bloqueo de equipos de los empleados. El acceso a Internet está protegido con WPA2. Los equipos utilizados por los empleados son tanto ordenadores de mesa como portátiles. Para el acceso a los ordenadores, cada trabajador dispone de un usuario y contraseña. No se cambia la contraseña de forma periódica.

- Acceso y contraseñas. El acceso a los servidores se realiza mediante un usuario y contraseña conocida por el equipo directivo y el empleado interno del Departamento de TI, que se cambia una vez al año.

- Puesto de trabajo. No existe ningún control de los documentos que se quedan en las impresoras sin recoger y nadie borra nunca la memoria de las impresoras. Además, la mayoría de los trabajadores suelen tener en sus mesas apuntes, post-it notes, hojas y documentos relacionados con el proyecto que están realizando.

Tampoco existe ninguna política sobre el bloqueo de los equipos de los empleados; por lo que su bloqueo, depende de cada uno.

- Copias de seguridad. No existe una política de copias de seguridad, ni un proceso automatizado que las realice. Los empleados son los encargados de realizar las copias de seguridad de sus equipos cuando lo consideran oportuno. El empleado interno del Departamento de TI es el encargado de realizar las copias de seguridad de los servidores y las suelen realizar una vez por semana.

- Responsabilidad ante la finalización o cambio de empleo. Los trabajadores firman un acuerdo de confidencialidad al ser contratados, pero no existe ninguna responsabilidad en seguridad de la información después de finalizar su empleo. Se lleva a cabo un proceso trimestral para revisar los permisos de los trabajadores y dar de baja en la base de datos a aquellos que ya no forman parte de la empresa.

2.1.6 Alcance del SGSI

El alcance del SGSI de TRADUX abarca todos los procesos de negocio relacionados con la prestación de servicios de traducción e interpretación a clientes, que son fundamentales para la facturación y el éxito empresarial. Esto incluye todas las actividades relacionadas con la gestión de proyectos de traducción, interpretación, revisión de textos, maquetación, creación de glosarios y memorias, así como la formación de traductores.

Además, el alcance del SGSI abarca la coordinación eficiente de proyectos, seguimiento de estrictas pautas de calidad, y la utilización de recursos clave como software de traducción, memorias de traducción, bases de datos, Internet, diccionarios, equipo humano altamente cualificado y la ubicación de sus oficinas para garantizar precios competitivos y rápidos tiempos de entrega.

El SGSI se implementa con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información asociada a estos procesos de negocio, así como para garantizar la seguridad de los datos sensibles de los clientes y cumplir con los requisitos legales y reglamentarios aplicables en materia de seguridad de la información.

2.1.7 Plan de Seguridad de la Información

El Plan de Seguridad de la Información, también llamado Plan Director, implica la identificación y clasificación de una serie de iniciativas relacionadas con la seguridad de la información. Su propósito es reducir los riesgos a los que se enfrenta la organización a niveles aceptables, todo basado en un análisis inicial de la situación.

Para desarrollar un Plan Director efectivo es fundamental que incluya los objetivos estratégicos de la empresa, defina claramente el alcance de las medidas de seguridad y especifique las responsabilidades y prácticas de seguridad que deben seguir los empleados.

Los objetivos del Plan de Seguridad de la Información para TRADUX son los siguientes.

- Asegurar la protección de los activos y la información de la empresa: implementando medidas de seguridad para proteger los activos de información de TRADUX contra accesos no autorizados, pérdidas o alteraciones.

- Cumplir con la legislación y regulaciones vigentes en materia de seguridad de la información: garantizando el cumplimiento de todas las leyes y regulaciones pertinentes relacionadas con la seguridad de la información, especialmente en lo que respecta al tratamiento de datos sensibles de los clientes.

- Incrementar la confianza de los clientes en TRADUX: mejorando la percepción de seguridad de los clientes y socios comerciales respecto a los servicios de traducción ofrecidos por TRADUX, lo que fortalecerá las relaciones comerciales y aumentará la retención de clientes.

- Certificar el SGSI en la norma ISO/IEC 27001:2022: obteniendo la certificación ISO/IEC 27001:2022 para el SGSI de TRADUX, lo que no solo demostrará el compromiso de la empresa con la seguridad de la información, sino que también aumentará la credibilidad y la confianza de los clientes.

- Lograr la concienciación y colaboración de todos los empleados en materia de seguridad de la información: fomentando una cultura de seguridad de la información entre todos los empleados de TRADUX, promoviendo la conciencia sobre las amenazas y riesgos de seguridad y fomentando la colaboración en la implementación de medidas de protección.

Para lograr estos objetivos en TRADUX, es fundamental llevar a cabo una serie de acciones clave. En primer lugar, es necesario conocer el estado actual de la seguridad de la información mediante evaluaciones exhaustivas. Esto permitirá identificar los riesgos específicos que puedan afectar a la empresa y desarrollar estrategias efectivas para mitigarlos. Además, es crucial capacitar a los empleados de TRADUX en prácticas seguras de manejo de la información y concienciarlos sobre la importancia de la seguridad. Asimismo, se deben establecer roles claros y responsabilidades definidas para todos los empleados en relación con la seguridad de la información. Esto garantizará una distribución adecuada de tareas y una mayor eficacia en la protección de los activos de la empresa. Además, es necesario definir e implementar controles de seguridad adecuados para proteger los activos de la empresa de manera efectiva.

Por último, se deben establecer indicadores y métricas para medir y controlar el cumplimiento de las medidas de seguridad. Esto permitirá realizar un seguimiento continuo del nivel de seguridad y realizar ajustes según sea necesario para garantizar la protección óptima de la información en TRADUX.

2.1.8 Certificaciones de calidad

TRADUX dispone de las siguientes certificaciones oficiales:

- ISO 9001:2015. Sistema de gestión de calidad. Requisitos. Establece una serie de condiciones concretas que definen la idoneidad de un sistema de control de calidad "basado en una serie de principios para el control de la calidad entre los que destacan: la marcada orientación al cliente, la motivación y la implicación por parte de la dirección, la gestión de los procesos y su mejora constante" [17].

- ISO 17100:2015 - Servicios de traducción. Certifica la existencia de los "procesos, recursos y aspectos necesarios para la prestación de servicios de traducción de calidad conformes a las especificaciones aplicables". Esta ISO exige a los LSP la acreditación de las cualificaciones y las competencias de los traductores, las aptitudes de los Gestores de Proyectos, así como la gestión profesional de los procesos relacionados con la prestación de servicios de traducción de alta calidad [17].

- ISO 18587:2020 - Posedición del resultado de una traducción automática. Establece los requisitos para el proceso de posedición humana del resultado de las traducciones generadas por una máquina y regula las competencias y cualificaciones de los profesionales que la llevan a cabo.

  Mediante la posedición, se edita y se corrige el texto generado de manera automática por una aplicación de software, para obtener un resultado comparable o muy similar a la traducción humana. Para ello, poseditores nativos de la lengua de destino trabajan con las tecnologías más avanzadas en entornos que integran glosarios especializados y funciones de control de calidad. Además, el proceso puede incluir una revisión humana adicional que garantiza un acabado completamente genuino e idiomático [18].

2.2. Análisis Diferencial

Como ya se ha indicado anteriormente, TRADUX no tiene experiencia en la implantación de un SGS y no posee normas de seguridad; por lo que, para llevar a cabo su implementación es preciso hacer un análisis diferencial que permita determinar el estado actual de la seguridad en la empresa.

Para llevar a cabo dicho análisis, se tendrá en cuenta el Modelo de Madurez de las Capacidades (CMM) en base a las disposiciones o cláusulas de ISO 27001:2022 y de los controles descritos en la ISO

27002:2022, que permitirá elaborar un informe de resultados. CMM define los niveles útiles para la evaluación de la seguridad mostrados seguidamente en la Tabla 2-2 [19]:

NIVEL	EFECTIVIDAD	NIVEL CMM	DESCRIPCIÓN NIVEL ISO/IEC 27000
L0	**0%**	**Inexistente**	Carencia total de proceso reconocible. La organización no ha reconocido la existencia del problema a resolver.
L1	**10%**	**Inicial / Ad-hoc**	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. No existen procesos estándar, en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
L2	**50%**	**Repetible**	Se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
L3	**90%**	**Definido**	Los procedimientos en sí no son sofisticados, pero formalizan las prácticas existentes. Se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones.
L4	**95%**	**Administrado y medible**	Es posible monitorear, medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
L5	**100%**	**Optimizado**	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Tabla 2-2. Niveles de capacidad del Modelo de Madurez de Capacidades (CMM).
Fuente: Elaboración propia a partir de Auditoría Informática. Obtenido de https://chaui1701023085.wordpress.com/2018/02/01/cubo-cobit-4-1/

2.2.1 Valoración de las cláusulas de la ISO 27001:2022 frente al CMM

La síntesis del análisis diferencial de las medidas de seguridad que TRADUX tiene implantadas respecto a las cláusulas de la ISO 27001:2022 frente al Modelo de Madurez de Capacidades (CMM) se muestra en la Tabla 2-3:

N.º	REQUERIMIENTOS ISO 27001:2022	Valoración %	Nivel CMM
4.	Contexto de la organización	10	L1
5.	Liderazgo	23,3	L1
6.	Planificación	3,3	L0
7.	Soporte	24	L1
8.	Operación	10	L1
9.	Evaluación del desempeño	0	L0
10	Mejora	0	L0

Tabla 2-3. Análisis Diferencial con respecto a la ISO 27001:2022
Fuente: Elaboración propia a partir de la ISO 27001:2022

El análisis diferencial detallado de las medidas de seguridad que TRADUX tiene implantadas respecto a las cláusulas de la ISO 27001:2022 frente al Modelo de Madurez de Capacidades (CMM) se puede ver en el Anexo IV. Análisis diferencial con respecto a la ISO 27001:2022.

2.2.2 Valoración de las cláusulas de la ISO 27002:2022 respecto al CMM

A continuación, la Tabla 2-4, muestra la valoración resumida de los controles indicados en la ISO 27002, a partir del modelo CMM (Tabla 2-4):

N.º	CONTROL	Valoración %	Nivel CMM
5	Controles organizacionales	13,23	L1
6	Personas	35	L1
7	Infraestructura	17,85	L1
8	Tecnología	30,95	L1

Tabla 2-4. Análisis Diferencial con respecto a la ISO 27002:2022
Fuente: Elaboración propia a partir de la ISO 27002:2022

El análisis diferencial completo de la valoración de los controles indicados en la ISO 27002:2022 frente al Modelo de Madurez de Capacidades (CMM) se puede ver en el Anexo V. Análisis diferencial con respecto a la ISO 27002:2022.

2.2.3 Conclusiones

Los resultados del análisis de las cláusulas de la ISO/IEC 27001 frente al Modelo CMM se muestran en el siguiente gráfico (Figura 2-6).

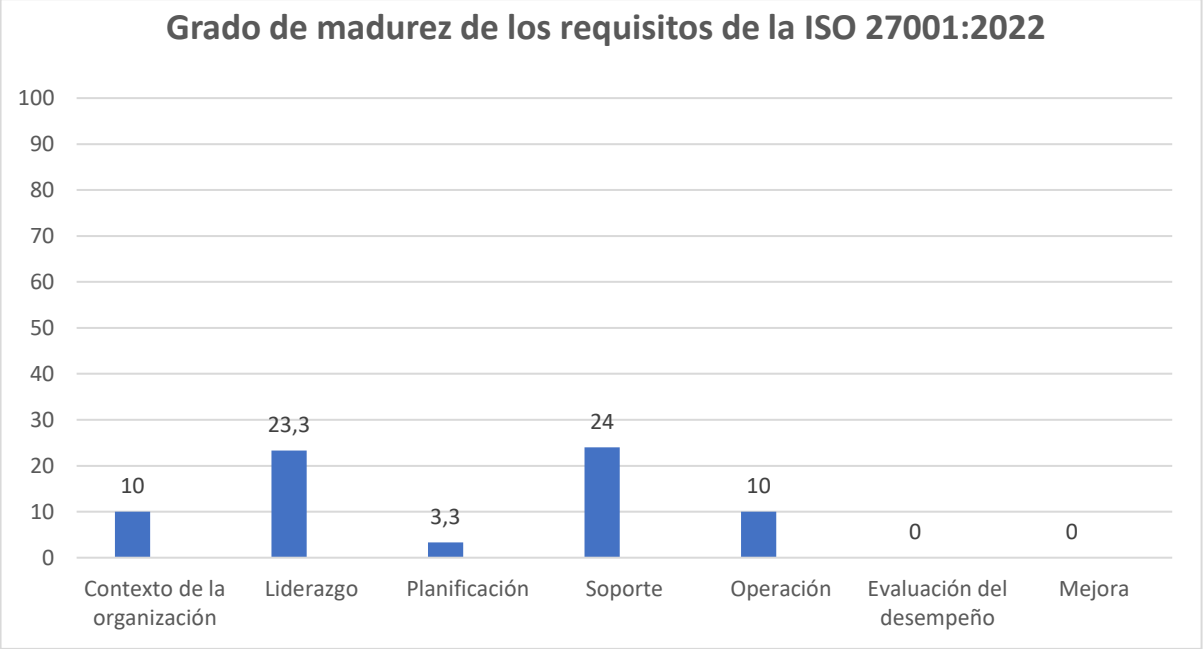

Figura 2-6. Grado de madurez de los requisitos de la ISO 27001:2022.
Fuente: Elaboración propia.

Por los valores obtenidos, puede observarse claramente, que el nivel de conocimiento de la organización respecto al SGSI es prácticamente inexistente, es decir, revelan un conocimiento limitado sobre el SGSI dentro de la organización. Aun mostrando en la cláusula de Soporte la valoración más alta con un 24%, estaría en el nivel L1 (inicial). Esto se ve seguido en orden descendente, por la cláusula de Liderazgo con un 23,3%. Las áreas de Contexto de la organización, Operación, Planificación, Evaluación del Desempeño y Mejora muestran cumplimientos significativamente bajos, con un 10%, 10%, 3,3%, 0% y 0% respectivamente.

Con estos valores podemos visualizar, mediante una gráfica radial (Figura 2-7), el estado de ellos respecto al que sería óptimo:

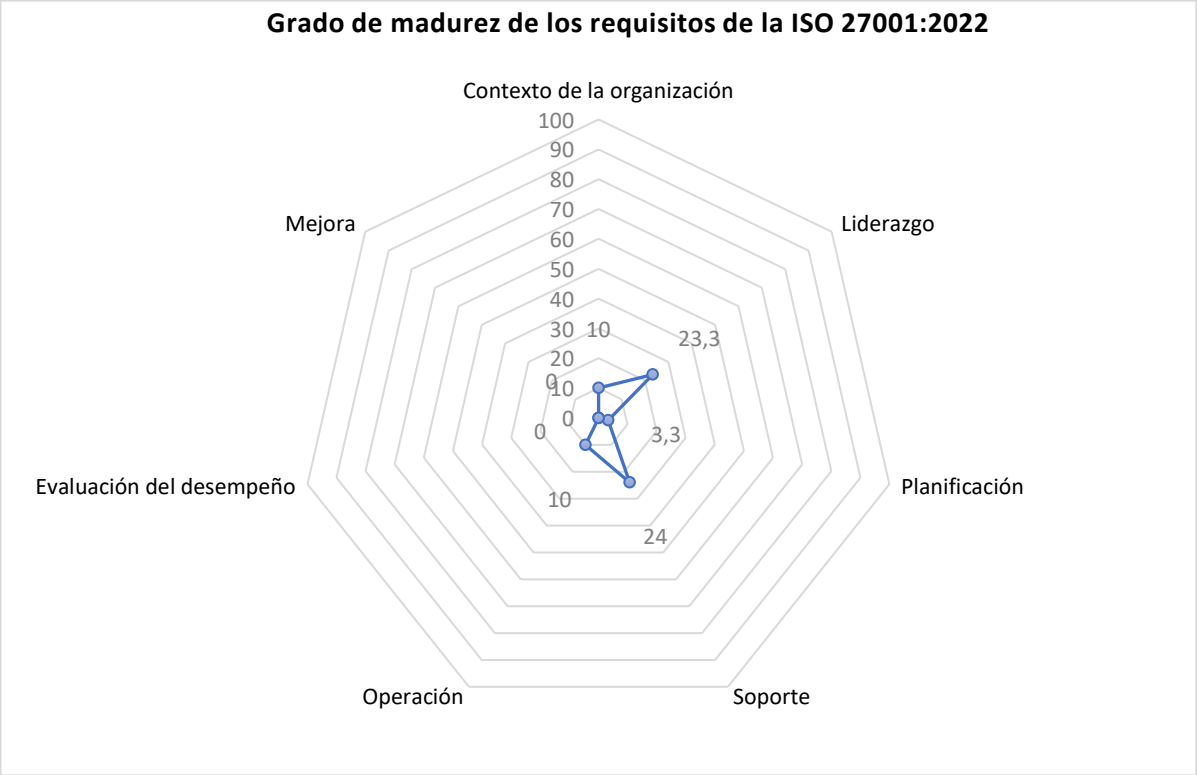

Figura 2-7. Gráfica radial sobre el Grado de madurez de los requisitos de la ISO 27001:2022.
Fuente: Elaboración propia.

Por otro lado, con respecto al análisis de los controles de la norma ISO 27002 con base al CMM se puede apreciar que todos los controles se encuentran en un nivel de madurez inicial (Figura 2-8), lo que indica la ausencia de procesos fuertemente establecidos que permitan abordar los problemas o peligros de la seguridad de la información en las diferentes áreas de la empresa.

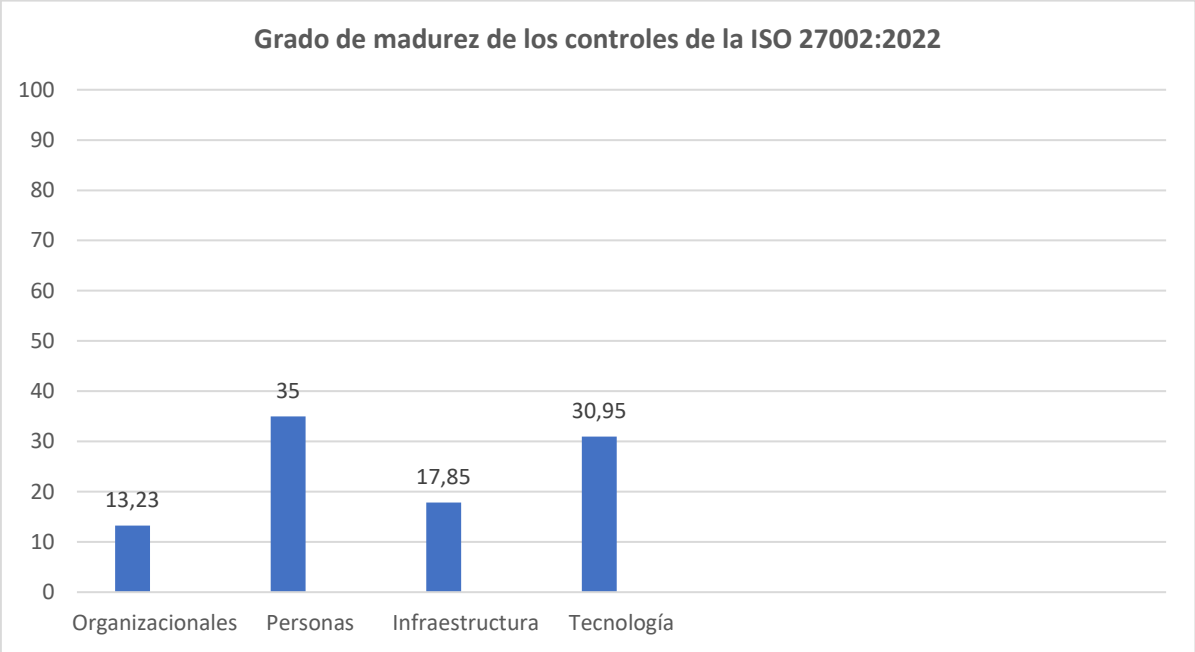

Figura 2-9. Grado de madurez de los controles de la ISO 27002:2022.
Fuente: Elaboración propia.

A continuación (Figura 2-9) se representa en forma de gráfica radial respecto al estado óptimo, donde se pueden ver cómo los valores de conformidad resultantes son bastante bajos:

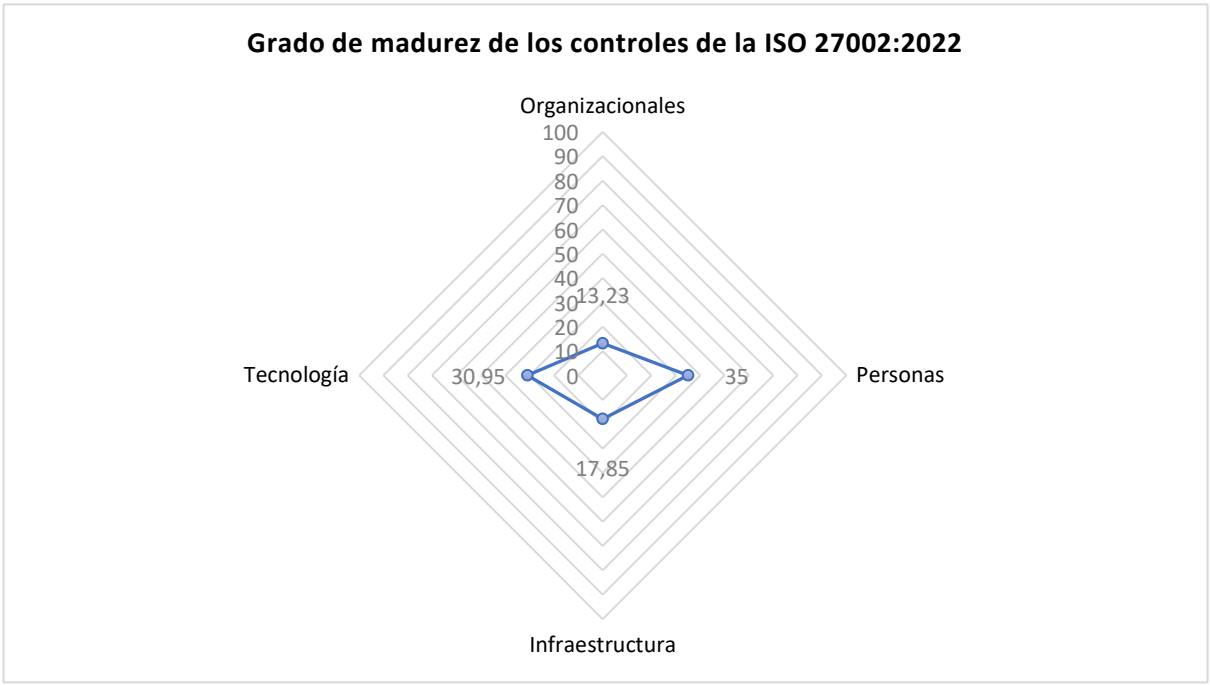

Figura 2-8. Gráfica radial respecto al Grado de madurez de los controles de la ISO 27002:2022.
Fuente: Elaboración propia.

A partir de estos datos obtenidos, se puede ver que la estimación inicial respecto al estado de la gestión de la seguridad era bastante adecuada. TRADUX no dispone de un sistema de gestión adecuado para el tratamiento de la seguridad de la información. Ni tan siquiera los porcentajes más elevados obtenidos en los controles de personas, de infraestructura o tecnológicos, se acercan a unos valores óptimos, por lo que resulta más que evidente su mejora en todos los ámbitos. Además, como TRADUX busca obtener la certificación ISO/IEC 27001:2022, es crucial que se adopte una estrategia de mejora integral que aborte todas las áreas identificadas en el análisis diferencial, lo que implica lo siguiente.

- Evaluación y Gestión de Riesgos: realización de una evaluación de riesgos exhaustiva para identificar y priorizar las áreas críticas que requieren atención inmediata.

- Desarrollo de Políticas y Procedimientos: establecimiento políticas de seguridad de la información claras y procedimientos operativos que cumplan con los requisitos de la norma.

- Formación y Concienciación: implementación de un programa continuo de formación y concienciación en seguridad de la información para todo el personal.

- Mejora Continua: establecimiento de un proceso de mejora continua que permita la revisión y actualización periódica de las prácticas de seguridad.

- Auditorías Internas: realización de auditorías internas regulares para asegurar el cumplimiento y la efectividad de las medidas implementadas.

- Gestión de Incidentes: desarrollo un plan de respuesta a incidentes robusto y ensayado para minimizar el impacto de cualquier brecha de seguridad.

Con un firme compromiso hacia la mejora continua y el cumplimiento de los estándares ISO/IEC 27001:2022, TRADUX no solo alcanzará la certificación, sino que también mejorará significativamente sus controles actuales de seguridad de la información. El objetivo tras la implementación de los proyectos propuestos en el capítulo 5 será lograr un mejor nivel que el inicial de madurez en sus controles, optimizando su postura de seguridad.

3. SISTEMA DE GESTIÓN DOCUMENTAL

En la ISO/IEC 27001:2022 se definen una serie de documentos a desarrollar para la implantación y control del SGSI. Los documentos básicos son los mostrados a continuación (Tabla 3-1):

Documento	Capítulo de ISO/IEC 27001:2022
Políticas de Seguridad de la Información	5.2
Procedimiento de Auditorías	9.2
Gestión de Indicadores	9.1
Procedimiento de Revisión por parte de la Dirección	9.3
Gestión de Roles y Responsabilidades	5.3
Metodología de Análisis de Riesgos	6.1.2, 6.1.3 (e)
Declaración de Aplicabilidad (SoA)	6.1.3 (d)

Tabla 3-1. Esquema documental en base a la ISO/IEC 27001:2022.
Fuente: Elaboración propia.

3.1. Política de Seguridad de la Información

El sistema de gestión de la 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. La norma ISO 27001:2022, en el apartado 5.2 Política, dispone los requisitos para su definición [12].

La alta dirección debe establecer una política de seguridad de la información que debe ser adecuada al propósito de la organización; incluir objetivos de seguridad de la información o proporcionar un marco de referencia para el establecimiento de dichos objetivos e incluir el compromiso de cumplir con los requisitos aplicables a la seguridad de la información y de mejora continua del SGSI.

La política de seguridad de la información y un conjunto de políticas temáticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.

El contenido de este documento establecido para TRADUX se puede verificar en el Anexo VI. Política de Seguridad de la Información.

3.2. Procedimiento de Auditorías Internas

La ISO/IEC 27001:2022 establece, en su apartado 9.2, la necesidad de llevar a cabo auditorías internas a intervalos planificados, Estas auditorías tienen como objetivo proporcionar información sobre si el SGSI cumple con los requisitos propios de la organización y con los requisitos de la ISO/IEC 27001:2022, así como si está implementado y mantenido de manera eficaz [12].

La existencia de este documento se puede constatar en el Anexo VII. Procedimiento de Auditorías Internas.

3.3. Gestión de Indicadores

La ISO/IEC 27001:2022 indica, en su apartado 9.1 Seguimiento, medición, análisis y evaluación, que la organización debe determinar [12]:

a) a qué es necesario monitorizar y medir, incluyendo procesos y controles de seguridad de la información;

b) los métodos de monitorización, medición, análisis y evaluación para garantizar resultados fiables;

c) cuándo se deben llevar a cabo el seguimiento y la medición, estableciendo un calendario adecuado;

d) quién debe hacer el seguimiento y la medición, designando responsabilidades claras;

e) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición, evaluando regularmente los datos recopilados;

f) quién debe analizar y evaluar esos resultados, asignando roles específicos para esta tarea.

La organización debe tener disponible la información documentada apropiada como evidencia de los resultados, así como debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

Se puede comprobar la existencia de este documento en el Anexo VIII. Gestión de Indicadores.

3.4. Procedimiento de Revisión por la Dirección

La norma ISO/IEC 27001:2022 establece en su apartado 9.3 que la alta dirección debe llevar a cabo revisiones planificadas del sistema de gestión de la seguridad de la información de la organización. Su objetivo es asegurar la conveniencia, adecuación y eficacia continuas del sistema [12].

La revisión por la dirección debe incluir consideraciones sobre:

a) el estado de las acciones de anteriores revisiones por la dirección;

b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;

c) cambios en las necesidades y expectativas de las partes interesadas que sean relevantes para el sistema de gestión de la seguridad de la información;

d) la información sobre el comportamiento de la seguridad de la información: tendencias relativas a no conformidades y acciones correctivas, seguimiento y resultados de las mediciones, resultados de auditoría y el cumplimiento de los objetivos de seguridad de la información;

e) los comentarios provenientes de las partes interesadas;

f) los resultados de la evaluación de los riesgos y el estado del plan de tratamiento de riesgos;

g) las oportunidades de mejora continua.

Los resultados de la revisión por la dirección deben incluir las decisiones relacionadas con las mejoras continuas y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

Este documento establecido para TRADUX se puede verificar en el Anexo IX. Procedimiento de Revisión por la Dirección.

3.5. Gestión de Roles y Responsabilidades

La ISO/IEC 27001:2022 establece en su apartado 5.3 que la alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización [12].

La alta dirección debe asignar la responsabilidad y autoridad para asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de la ISO/IEC 27001:2022 e informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información.

Para constatar la existencia de este documento véase el Anexo X. Gestión de Roles y Responsabilidades.

3.6. Metodología Gestión de Riesgos

La ISO/IEC 27001:2022 indica en sus puntos "6.1.2. y 6.1.3 (e) que la organización debe definir y aplicar un proceso de evaluación de los riesgos de seguridad de la información que [12]:

a) establezca y mantenga criterios sobre riesgos de seguridad de la información;

b) asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;

c) identifique, analice y evalúe los riesgos de seguridad de la información comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto (a) priorizando el tratamiento de los riesgos analizados.

La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información.

Este documento se puede verificar en el Anexo XI. Metodología Gestión de Riesgos.

3.7. Declaración de Aplicabilidad

Según lo establecido en el punto "6.1.3. Tratamiento de los riesgos de seguridad de la información", apartado (d), de la norma ISO/IEC 27001:2022, la organización debe desarrollar un proceso de tratamiento de riesgos de seguridad de la información para elaborar una "Declaración de Aplicabilidad" que contenga [12]:

- los controles necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información, comparar los controles determinados con los del anexo A y comprobar que no se han omitido controles necesarios;

- la justificación de las inclusiones;

- si los controles necesarios están implementados o no; y

- la justificación de las exclusiones de cualquiera de los controles del anexo A;

Para verificar la existencia de este documento véase el Anexo XII. Declaración de Aplicabilidad.

---

4. ANÁLISIS DE RIESGOS

El análisis de riesgos es un proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización. Además, permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema.

El análisis de los riesgos busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, servirá para descubrir qué necesidades de seguridad tiene TRADUX tras detectar cuáles son los puntos débiles en seguridad y las amenazas a las que se encuentra expuesta.

Como ya se indicó al comienzo de este proyecto, en este capítulo se va a llevar a cabo una metodología de análisis de riesgos ligera basada en MAGERIT – versión 3.0 "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" [24].

A continuación, se presenta la metodología de análisis de riesgos simplificada y ligera basada en MAGERIT, (Figura 4-1), diseñada específicamente para elaborar, desarrollar e implementar el SGSI en TRADUX, según los estándares ISO 27001:2022 e ISO 27002:2022:

1. **Definición del alcance del SGSI:** identificar los elementos dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de TRADUX, siguiendo los estándares ISO 27001:2022 e ISO 27002:2022.

2. **Identificación y valoración de activos:** identificar y clasificar los activos de información y servicios críticos para TRADUX.

3. **Identificación de amenazas relevantes:** seleccionar las amenazas más relevantes para TRADUX, basándose en la metodología de análisis de riesgos ligera basada en MAGERIT y adaptada a los estándares ISO 27001:2022 e ISO 27002:2022.

4. **Evaluación de vulnerabilidades:** evaluar la frecuencia de ocurrencia de las amenazas utilizando información histórica de incidentes de seguridad, tomando en cuenta los estándares y recomendaciones de MAGERIT y las normas ISO.

5. **Gestión del riesgo:** abordar la gestión de los riesgos identificados, incluyendo la toma de decisiones para tratar, aceptar, transferir o evitar dichos riesgos. Este proceso se llevará a cabo

en línea con los objetivos y políticas de seguridad de TRADUX, así como con los requisitos establecidos por las normas ISO.

6. **Riesgo residual y plan de tratamiento:** elaborar los planes de tratamiento de riesgos con el objetivo de reducir los riesgos residuales a un nivel aceptable. Estos planes garantizarán la continuidad y seguridad de las operaciones de TRADUX, estableciendo acciones específicas para abordar cada riesgo identificado.

Figura 4-1. Metodología de análisis de riesgos simplificada basada en MAGERIT.
Fuente: Elaboración propia.

4.1. Definición del alcance del SGSI

El alcance del SGSI de TRADUX cubre todos los procesos esenciales relacionados con la prestación de servicios de traducción e interpretación a clientes, incluyendo la gestión de proyectos, la coordinación eficiente, el seguimiento de pautas de calidad y el uso de recursos clave.

Se implementa para proteger la confidencialidad, integridad y disponibilidad de la información asociada a estos procesos, así como para garantizar la seguridad de los datos sensibles de los clientes y cumplir con los requisitos legales y reglamentarios aplicables. Este apartado se ha descrito detalladamente en el apartado 2.4.6 Alcance del SGSI.

4.2. Identificación y valoración de activos

En primer lugar, se ha llevado a cabo una exhaustiva identificación e inventariado de todos los activos necesarios para los servicios dentro del alcance de TRADUX. Para este fin, se ha seguido la división de

activos propuesta por MAGERIT. Este enfoque garantiza la representación de cómo las tecnologías y sistemas de información respaldan las operaciones del negocio.

El inventario de activos se ha documentado en la siguiente tabla, donde cada activo se identifica por su clase y el propietario correspondiente. Los activos identificados incluyen:

- Datos: información esencial almacenada en diversas plataformas como bases de datos, servidores de archivos, almacenamiento en red, etc.
- Proveedor: empresas externas con las que TRADUX mantiene relaciones contractuales para la realización de procesos específicos o la prestación de servicios.
- Hardware: equipos físicos que respaldan los servicios de la organización, incluyendo servidores, routers, switches, dispositivos de almacenamiento, entre otros.
- Software: aplicaciones utilizadas para gestionar y procesar datos, incluyendo tanto software desarrollado internamente como soluciones de terceros.
- Licencia de Software: licencias para el uso de software comercial.
- Carpeta de red: recursos compartidos utilizados para el almacenamiento de información por parte de los distintos departamentos.
- Puesto de trabajo: equipos utilizados por los usuarios para realizar sus tareas, como computadoras de escritorio y portátiles.
- Red: infraestructura de comunicaciones, incluyendo redes locales, acceso a Internet y otros servicios contratados.
- Elemento auxiliar: equipos de soporte para los sistemas de información, como sistemas de alimentación ininterrumpida (SAI), equipos de climatización y sistemas de extinción de incendios.
- Personal: roles y funciones críticas desempeñadas por el personal de la empresa.
- Instalación: locaciones físicas donde se alojan los sistemas de información y comunicaciones, como edificios y centros de procesamiento de datos.

La valoración de los activos se realiza en función de su importancia para TRADUX, siguiendo una escala de 1 (Muy Bajo) a 5 (Muy Alto) basada en los criterios de valoración definidos en MAGERIT. Esta valoración se asocia a las dimensiones de seguridad establecidas en la norma ISO 27001:2022:

- Disponibilidad [D]: impacto de la falta de acceso al servicio cuando se necesita.

- Confidencialidad [C]: consecuencias de la divulgación de información a personas no autorizadas, incluida la autenticidad de quienes acceden al servicio.

- Integridad [I]: impacto de la modificación no autorizada de la información asociada al servicio, incluida la trazabilidad de los accesos.

La valoración se realiza considerando la "necesidad de proteger", donde activos más valiosos requerirán un mayor nivel de protección en las dimensiones de seguridad pertinentes. Se utiliza la siguiente tabla de valoración (Tabla 4-1) para determinar la valoración de estas dimensiones, asegurando así una evaluación completa y adecuada:

NIVEL	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD
1 Muy Bajo	Prescindible por tiempo indefinido (RTO > 1 semana)	Información de carácter público, accesible por cualquier persona (Incumplimiento leve de una ley o regulación).	Errores en la información fácil y rápidamente reparables.
2 Bajo	RTO entre 1 y 7 días	La información no deben conocerla personas ajenas a la organización (datos de uso interno) (Incumplimiento medio de una ley o regulación).	Datos cuya falsedad afectaría de una forma leve.
3 Medio	RTO entre 4 y 24 horas	La información deben conocerla solo quienes lo necesitan para su trabajo, con autorización explícita (datos de uso restringido) (Incumplimiento grave de una ley o regulación).	Datos cuya falsedad afectaría de una forma importante.
4 Alto	RTO inferior a 4 horas	La información deben conocerla un número reducido de personas (confidencial) (Incumplimiento muy grave de una ley o regulación).	Datos cuya falsedad afectaría de una forma grave.
5 Muy Alto	RTO inferior a 1 hora	Datos clasificados como reservados o secretos (Incumplimiento muy grave de una ley o regulación).	Datos cuya falsedad afectaría de una forma muy grave.

Tabla 4-1. Valoración de activos.
Fuente: Elaboración propia.

IDENTIFICADOR	NOMBRE DEL ACTIVO	CATEGORÍA DEL ACTIVO	PROPIETARIO DEL ACTIVO	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	VALOR DEL ACTIVO
I-001	Información financiera	Datos	Jefe Administrativo y Financiero	5	5	5	5
I-002	Propiedad intelectual	Datos	Director Ejecutivo	4	5	4	4
I-003	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	5	4	4
I-004	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	5	5	5
I-005	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	5	4	5	5
I-006	Información de acceso de las visitas	Datos	Dpto. TI	1	2	2	2
I-007	Proveedor informático	Proveedor	Jefe de Tecnologías de la Información	5	4	5	5
I-008	Proveedor de servicios en la nube (Microsoft Azure)	Proveedor	Jefe de Tecnologías de la Información	5	5	5	5
I-009	Ordenadores de escritorio	Hardware	Dpto. TI	4	4	3	4
I-010	Ordenadores para el teletrabajo (portátiles)	Hardware	Dpto. TI	4	4	3	4
I-011	Enrutadores	Hardware	Dpto. TI	3	2	2	2
I-012	Conmutadores	Hardware	Dpto. TI	3	2	2	2
I-013	Firewall	Hardware	Dpto. TI	3	3	2	3
I-014	Impresora	Hardware	Dpto. TI	2	3	0	2
I-015	Sistema operativo	Software	Dpto. TI	5	4	5	5
I-016	Antivirus	Software	Dpto. TI	4	3	5	4

I-017	Adobe Acrobat Professional	Software	Dpto. TI	4	3	5	4
I-018	Microsoft Office 365	Software	Dpto. TI	5	3	5	4
I-019	Aplicaciones internas de administración	Software	Dpto. TI	5	3	5	4
I-020	Herramientas de traducción	Software	Dpto. TI	5	3	5	4
I-021	Licencia del sistema operativo	Licencia de software	Dpto. TI	4	3	2	3
I-022	Licencia del antivirus	Licencia de software	Dpto. TI	4	3	2	3
I-023	Licencia del software especializado (traducción)	Licencia de software	Dpto. TI	4	4	4	4
I-024	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	5	4	5	5
I-025	Archivos de configuración de red	Carpeta de red	Dpto. TI	5	4	5	5
I-026	VPN	Red	Dpto. TI	5	4	1	3
I-027	Cableado eléctrico	Red	Dpto. TI	5	4	1	3
I-028	Cableado telecomunicaciones	Red	Dpto. TI	5	4	1	3
I-029	Servicio Internet	Red	Dpto. TI	4	5	4	4
I-030	Red inalámbrica	Red	Dpto. TI	2	5	4	4
I-031	Sistema climatización	Elemento auxiliar	Instalaciones	4	1	1	2
I-032	Sistema detección incendios	Elemento auxiliar	Instalaciones	5	1	1	2
I-033	Caja fuerte	Elemento auxiliar	Jefe Administrativo y Financiero	5	4	4	4
I-034	Destructor de papeles	Elemento auxiliar	Dpto. TI	1	1	1	1
I-035	Director Ejecutivo	Personal	Él mismo	5	1	1	2
I-036	Jefe de Tecnologías de la Información	Personal	Él mismo	5	1	1	2
I-037	Empleado interno de TI	Personal	Él mismo	5	1	1	2
I-038	Jefe Administrativo y Financiero	Personal	Él mismo	5	1	1	2
I-039	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	5	1	1	2
I-040	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	5	1	1	2
I-041	Traductores e Intérpretes	Personal	Él mismo	5	1	1	2
I-042	Estudiantes en prácticas	Personal	Él mismo	4	1	1	2
I-043	Oficinas	Instalación	Dpto. TI	3	1	0	1

I-044	Despacho del director	Instalación	Dpto. TI	3	1	0	1
I-045	Despacho de cada empleado	Instalación	Dpto. TI	3	1	0	1
I-046	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	3	1	0	1
I-047	Salas	Instalación	Dpto. TI	3	1	0	1

Tabla 4-2. Identificación y Valoración de los Activos.
Fuente: Elaboración propia.

4.3. Identificación de amenazas relevantes

En la identificación de amenazas, se hace uso del catálogo de amenazas proporcionado por MAGERIT. Dado que este catálogo es extenso, se adopta un enfoque práctico y simplificado, seleccionando únicamente las amenazas más relevantes para el contexto específico de la organización analizada. Una vez identificadas estas amenazas, se establece su relación con los diversos activos, evaluando si estos se ven afectados por cada una de las amenazas identificadas.

Los activos que sostienen los servicios esenciales de la infraestructura crítica son identificados y valorados inicialmente. Luego, se procede a la identificación de las amenazas asociadas a cada activo. Para esta tarea, se seleccionan los eventos de amenaza de acuerdo con el catálogo de amenazas de MAGERIT (sección 5 del "Libro II - Catálogo de Elementos"), considerando factores como el tipo de activo, su ubicación, historial de problemas y experiencias previas. Los eventos de amenaza se clasifican en cuatro tipos: Desastres Naturales (N), Desastres de Origen Industrial (I), Errores y Fallos No Intencionados (E), y Ataques Deliberados (A).

Las amenazas identificadas por cada tipo de activo y la dimensión de seguridad afectada se muestran a continuación (Tabla 4-3):

ACTIVO	CATEGORÍAS DE LOS ACTIVOS	AMENAZAS	DISPONIBILIDAD	CONFIDENCIALIDA	INTEGRIDAD
Datos	Activos de tipo información, necesaria para los servicios y procesos de negocio esenciales. Información almacenada en la base de datos, SAN, NAS, etc.	[E.15] Alteración accidental de la información [I]			X
		[E.18] Destrucción de la información (D)	X		
		[E.19] Fugas de información (C)		X	
		[A.15] Modificación deliberada de la información [I]			X
		[A.18] Destrucción de la información (D)	X		
		[A.19] Divulgación de información (C)		X	

Proveedor	Terceras empresas que mantienen una relación contractual con la entidad por la cual asumen la realización de un determinado proceso o aportan un determinado tipo de servicio	[I.9] Interrupción de otros servicios y suministros esenciales (D)	X		
Hardware	Medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la organización, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones o responsables del procesado o la transmisión de datos. (Servidor, cluster, router, switch, appliance, SAN, NAS, librería de cintas, etc.).	[I.5] Avería de origen físico o lógico (D)	X		
		[E.2] Errores de administrador (D) (I) (C)	X	X	X
		[E.23] Errores de mantenimiento / actualización de equipos (D)	X		
		[E.24] Caída del sistema por agotamiento de recursos (D)	X		
Software	Aplicaciones que se ejecutan en un equipo informático y que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. (Aplicación de desarrollo propio, de desarrollo de terceros a medida y estándar, Bases de Datos, etc.).	[E.1] Errores de los usuarios (D) (I) (C)	X	X	X
		[E.3] Errores de monitorización (log) (I)			X
		[E.4] Errores de configuración (D) (I) (C)	X	X	X
		[E.20] Vulnerabilidades de los programas (D) (I) (C)	X	X	X
		[E.21] Errores de mantenimiento/actualización (D) (I) (C)	X	X	X
		[A.5] Suplantación de la identidad del usuario (I) (C)		X	X
		[A.6] Abuso de privilegios de acceso (D) (I) (C)	X	X	X
		[A.11] Acceso no autorizado (D) (I) (C)	X	X	X
Licencia software	Licencias de software comercial.	[E.7] Deficiencias en la organización (D)	X		
Carpeta de red	Recursos compartidos donde las áreas de negocio almacenan la información.	[E.3] Errores de monitorización (log) (I)			X
		[E.8] Difusión de software dañino (D) (I) (C)	X	X	X
		[E.15] Alteración accidental de la información [I]			X
		[E.18] Destrucción de la información (D)	X		
		[E.19] Fugas de información (C)		X	

		[A.11] Acceso no autorizado (D) (I) (C)	X	X	X
		[A.15] Modificación deliberada de la información [I]			X
		[A.18] Destrucción de la información (D)	X		
		[A.19] Divulgación de información (C)		X	
Puesto de trabajo	Equipo de trabajo de un usuario. (PC, portátil).	[I.5] Avería de origen físico o lógico (D)	X		
		[E.25] Pérdida de equipos (D)	X		
		[A.11] Acceso no autorizado (D) (I) (C)	X	X	X
		[A.25] Robo de equipos (D) (C)	X		
Red	Instalaciones, servicios de comunicaciones contratados a terceros y elementos de infraestructura propia. (LAN, Acceso Internet, Red Local, DIBA, Wifi, MacroLAN, etc.).	[I.8] Fallo de servicios de comunicaciones (D)	X		
		[A.11] Acceso no autorizado (D) (I)	X		X
		[A.14] Interceptación de información (escucha) (C)		X	
Elemento auxiliar	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. (SAI, grupo electrógeno, equipos climatización, sistema extinción de incendios, centralita, etc.).	[I.9] Interrupción de otros suministros y servicios esenciales (D)	X		
Personal	Roles, perfiles, funciones desempeñadas por personas y que son críticas para el proceso de negocio.	[E.7] Deficiencias en la organización (D)	X		
		[E.15] Alteración accidental de la información [I]			X
		[E.18] Destrucción de la información (D)	X		
		[E.19] Fugas de información (C)		X	
		[E.28] Indisponibilidad del personal (D)	X		
		[A.28] Indisponibilidad del personal (D)	X		
		[A.30] Ingeniería social (picaresca) (D) (I) (C)	X	X	X
Instalación	Lugares donde se hospedan los sistemas de información y comunicaciones y desde los que se desarrollan los procesos de negocio analizados. (Edificio, CPDs, etc.).	[N.*] Desastres naturales (D)	X		
		[I.*] Desastres industriales (D)	X		
		[I.1] Fuego (D)	X		
		[I.2] Daños por agua (D)	X		
		[I.3] Contaminación mecánica (D)	X		
		[I.4] Contaminación electromagnética (D)	X		

		[I.6] Corte del suministro eléctrico (D)	X		
		[I.7] Condiciones inadecuadas de temperatura o humedad (D)	X		
		[A.11] Acceso no autorizado (D)	X		
		[A.26] Ataque destructivo (D)	X		

Tabla 4-3. Amenazas por tipo de activo y dimensión de seguridad.
Fuente: Elaboración propia.

4.4. Evaluación de vulnerabilidades

Para determinar el riesgo, se ha evaluado cada evento de amenaza asociado a los activos, considerando su frecuencia anual estimada y su impacto potencial en los servicios y procesos de negocio en todas las dimensiones analizadas. Se ha establecido el grado de deterioro del activo en cada dimensión de seguridad.

A continuación, se detallan las escalas utilizadas para valorar las amenazas, tanto para evaluar la frecuencia (Tabla 4-4) como para estimar el impacto (Tabla 4-5):

FRECUENCIA	DESCRIPCIÓN	VALOR
MB	Muy Baja (Muy Improbable) – Una vez cada 50 años	1
B	Baja (Improbable) – Una vez cada 10 años	2
M	Media (Posible) – Una vez al año	3
A	Alta (Probable) – Una vez al mes	4
MA	Muy Alta (Frecuente) – Diez veces al mes	5

Tabla 4-4. Escala de frecuencia de ocurrencia de eventos de amenaza.
Fuente: Elaboración propia.

IMPACTO	ESTADO DEL ACTIVO	VALOR
MB	Muy Baja – Activo en perfecto estado	1
B	Baja – Ligera degradación que no impide el funcionamiento	2
M	Media – Funcionamiento degradado, rendimiento bajo	3
A	Alta – Prácticamente inservible	4
MA	Muy Alta – El activo resulta totalmente inservible	5

Tabla 4-5. Escala de impacto en el estado de los activos.
Fuente: Elaboración propia.

4.5. Gestión del riesgo

En este apartado, se aborda la gestión integral de los riesgos en TRADUX, comprendiendo su definición, evaluación y tratamiento para salvaguardar la integridad y continuidad de las operaciones. El riesgo se define como la medida del posible daño que podría afectar al sistema de TRADUX. Esto se determina considerando el impacto de las amenazas sobre los activos, junto con la probabilidad de que ocurran.

El cálculo del riesgo actual se realiza mediante la fórmula que se indica a continuación:

$$riesgoActual = valoración * probabilidad * impacto$$

El riesgo aumenta proporcionalmente con el impacto y la probabilidad. Con base en esta fórmula, se han identificado cuatro zonas en las que se clasifican los riesgos, desde aquellos muy probables y de alto impacto hasta los improbables, pero de muy alto impacto (Figura 4-2).

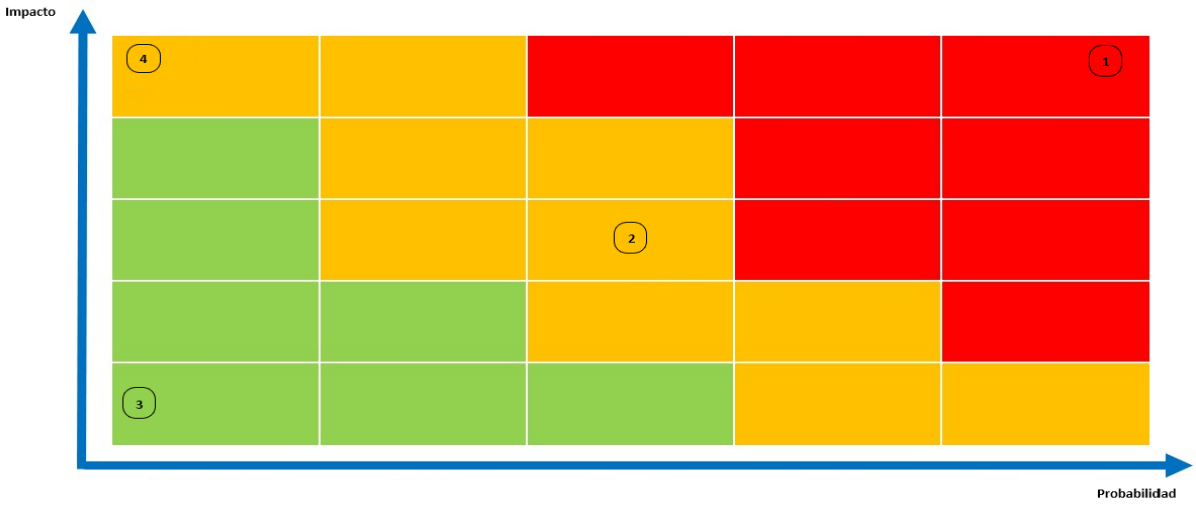

Figura 4-2. Mapa de riesgos.
Fuente: Elaboración propia.

Las cuatro zonas diferenciadas son las que se indican a continuación:

- Zona 1: se encuentran los riesgos altamente probables de ocurrir y que tendrían un impacto muy significativo en TRADUX si se materializaran.

- Zona 2: se agrupan una variedad de escenarios que van desde situaciones poco probables hasta aquellas muy probables, pero todas con un impacto moderado o bajo en comparación con otros riesgos.

- Zona 3: se incluyen los riesgos que son poco probables de ocurrir y, si suceden, tendrían un impacto bajo en las operaciones de TRADUX.

- Zona 4: se encuentran los riesgos que, aunque poco probables, tendrían un impacto muy significativo en TRADUX si llegaran a materializarse.

Una vez definido el mapa de riesgos con sus cuatro zonas diferenciadas; se procede a mostrar el riesgo actual en el Anexo XIII. Riesgo actual.

4.5.1 Riesgo residual

El riesgo residual de TRADUX se determina considerando la valoración ponderada del activo, la probabilidad de ocurrencia de la amenaza y el impacto potencial sobre el activo. En este caso, es la misma tabla que la tabla anterior, puesto que apenas existen salvaguardas en la empresa.

$$\boldsymbol{Riesgo\ residual = valorActivo * probabilidadActual * impactoActual}$$

- valorActivo: es la evaluación ponderada del activo, calculada como el promedio redondeado de la valoración en las tres dimensiones de seguridad.

- probabilidadActual: representa la probabilidad de que la amenaza se concrete, considerando las salvaguardas implementadas hasta la fecha de análisis.

- impactoActual: indica el impacto que la amenaza tendría en el activo, teniendo en cuenta las salvaguardas aplicadas hasta la fecha de análisis.

4.5.2 Riesgo aceptable

Los riesgos residuales que se sitúen por debajo del nivel de riesgo aceptable definido por la empresa no requerirán acciones adicionales. Este nivel de riesgo aceptable es fundamental para guiar las decisiones de tratamiento de los riesgos identificados. El nivel de riesgo definido es 45, por tanto, cualquier riesgo que su nivel sea por debajo de 45 se considerará como aceptable.

4.5.3 Riesgo no aceptable

Debido a que la empresa tiene un bajo presupuesto para asimilar los riesgos se ha indicado que el nivel de riesgo aceptable en TRADUX se ha establecido en 45. Los riesgos que superan este umbral son considerados no aceptables y deben ser tratados con prioridad.

Los riesgos identificados como no aceptables requieren la implementación de medidas correctivas para mitigar su impacto y/o reducir su probabilidad de ocurrencia. Las acciones para considerar incluyen la reducción del riesgo mediante la implementación de controles adicionales o mejoras en los existentes, la capacitación y concienciación del personal sobre prácticas seguras, y la revisión y actualización de políticas y procedimientos de seguridad. También se puede evitar el riesgo mediante la modificación o eliminación de procesos que lo introducen, o la sustitución de tecnologías o sistemas vulnerables por alternativas más seguras.

La transferencia del riesgo puede lograrse mediante la contratación de seguros específicos para cubrir posibles incidentes, o la externalización de servicios críticos a proveedores especializados con mejores controles de seguridad. En algunos casos, donde el coste de mitigación es mayor que el posible impacto, se puede decidir aceptar el riesgo y preparar un plan de contingencia.

Posteriormente, se establecerán unas propuestas de proyectos para poder tratar estos riesgos.

Los activos por tratar se muestran en el Anexo XIV. Riesgo no aceptable.

4.5.4 Propietario del riesgo

Cada riesgo identificado en TRADUX tiene un propietario asignado, responsable de proponer y llevar a cabo las medidas necesarias para su tratamiento.

4.5.5 Criterios para la toma de decisiones

La decisión sobre el tratamiento o aceptación de los riesgos debe considerar diversos aspectos, como los requisitos del negocio, los resultados del análisis de riesgos, las obligaciones legales y contractuales, así como los costos y las limitaciones técnicas.

4.5.6 Plan de acción ante riesgos detectados

Tras analizar los resultados de la evaluación de riesgos y determinar el nivel de riesgo aceptable, el responsable de Seguridad de TRADUX, en colaboración con el propietario de cada riesgo identificado, tomará medidas para abordar los riesgos detectados. Estas acciones pueden incluir: reducir el riesgo mediante la implementación de controles adecuados para disminuir la probabilidad y/o el impacto, asumir el riesgo sin aplicar medidas adicionales, evitar el riesgo eliminando el uso del activo, servicio, proceso o fuente de amenaza involucrada, o transferir el riesgo a terceros mediante seguros, proveedores externos.

4.6. Plan de Tratamiento

Para mitigar los riesgos identificados, se elaborará un Plan de Tratamiento de Riesgo que incluirá los siguientes elementos:

- Identificación de la medida de seguridad: se asignará un código único y un nombre descriptivo para cada medida de seguridad.
- Descripción: se proporcionará un resumen detallado de los contenidos e implicaciones de la medida de seguridad.
- Responsable: se designará el departamento o la persona responsable de llevar a cabo la implementación de la medida de seguridad.
- Fechas de inicio y fin previstas (duración): se establecerán las fechas de inicio y finalización para la ejecución de la medida de seguridad.
- Activos: se especificarán los activos sobre los cuales se aplicará la medida de seguridad.
- Listado de tareas: se detallarán las tareas necesarias para la implementación de la medida de seguridad, junto con una descripción de cada tarea.
- Seguimiento: se llevará a cabo un seguimiento periódico del progreso de la implementación de la medida de seguridad.
- Observaciones o comentarios: se incluirán observaciones adicionales o comentarios relevantes sobre la implementación de la medida de seguridad.
- Estado: se indicará el estado actual de la implementación de la medida de seguridad, que puede ser "Sin iniciar", "En proceso", "Parada" o "Finalizada".

5. PROPUESTAS DE PROYECTOS

Tras realizar el análisis de riesgos, se ha obtenido una visión clara del estado de la seguridad de la información de la empresa. En esta etapa, se propondrán diferentes proyectos con el objetivo de reducir el nivel de riesgo actual de TRADUX y mejorar su seguridad. Estos proyectos se derivan de las recomendaciones identificadas durante el análisis de riesgos y se centran en mejorar la gestión de la seguridad, así como en posibles beneficios adicionales como la optimización de recursos y la mejora en la gestión de procesos y tecnologías dentro de TRADUX.

5.1. Propuestas

A continuación, se presentan las propuestas de proyectos, agrupadas por las categorías de los activos:

- Medidas de seguridad para activos de Software.

PROYECTO - 001	**Implementación de Autenticación Multifactor (MFA)**
Descripción	Implementar un sistema de autenticación multifactor en los sistemas operativos para mitigar la amenaza de suplantación de identidad y acceso no autorizado.
Responsable	Dpto. TI.
Duración	Cuatro meses.
Categoría de activos	Software (sistema operativo).
Listado de tareas	Evaluar y seleccionar una solución de MFA.
	Configurar e implementar MFA en los sistemas operativos.
	Realizar pruebas de funcionamiento y ajustes necesarios.
Seguimiento	Revisiones semanales del avance del proyecto.

Observaciones o comentarios	Se deberá educar a los usuarios sobre el uso correcto del MFA.
Estado	En proceso.

Tabla 5-1. Proyecto 001. Implementación de Autenticación Multifactor (MFA).
Fuente: Elaboración propia.

- Medidas de seguridad para activos de datos (información financiera, propiedad intelectual, datos de los empleados, datos de los clientes, proyectos de traducción e interpretación).

PROYECTO - 002	**Implementación de Política de Seguridad de la Información**
Descripción	Desarrollar e implementar una política de seguridad de la información para prevenir la alteración accidental o intencional de datos.
Responsable	Jefe Administrativo y Financiero, Responsable de Administración (RRHH) / Contabilidad / Comercial, Jefes de Proyectos de Traducción e Interpretación.
Duración	Seis meses.
Categoría de activos	Todos los activos de la categoría datos.
Listado de tareas	Investigar y documentar los requisitos de seguridad de la información.
	Desarrollar la política de seguridad de la información.
	Implementar la política en todos los departamentos relevantes.
Seguimiento	Revisión mensual del cumplimiento de la política.
Observaciones o comentarios	Se deberá realizar una capacitación sobre la nueva política a todos los empleados.
Estado	En proceso.

Tabla 5-2. Proyecto 002. Implementación de Política de Seguridad de la Información.
Fuente: Elaboración propia.

- Medidas de seguridad para activos de red (almacenamiento de archivos compartidos, archivos de configuración de red).

PROYECTO - 003	Implementación de respaldo y recuperación de datos
Descripción	Establecer un sistema de respaldo automatizado y periódico de todos los activos de información crítica.
Responsable	Departamento de TI.
Duración	Cinco meses.
Categoría de activos	Almacenamiento de archivos compartidos, archivos de configuración de red.
Listado de tareas	Evaluar y seleccionar una solución de respaldo adecuada.
	Configurar y programar respaldos automáticos para todos los activos críticos.
	Realizar pruebas de restauración periódicas para garantizar la integridad de los datos.
Seguimiento	Revisiones semanales del estado de los respaldos.
Observaciones o comentarios	Se deberán establecer políticas claras sobre la retención de datos y la frecuencia de los respaldos.
Estado	En proceso.

Tabla 5-3. Proyecto 003. Implementación de respaldo y recuperación de datos.
Fuente: Elaboración propia.

- Medidas para la concienciación, educación y formación en seguridad de la información.

PROYECTO - 004	Formación Continua en Seguridad de la Información para los empleados
Descripción	Proporcionar a todos los empleados de la empresa una formación continua en seguridad de la información para aumentar la conciencia y promover las buenas y seguras prácticas en el manejo de los datos y de los sistemas.
Responsable	Departamento de RRHH en colaboración con el Departamento de TI.
Duración	Tres meses para la fase inicial, la fase de mantenimiento se realiza de forma continua.

Categoría de activos	Almacenamiento de archivos compartidos, archivos de configuración de red.
Listado de tareas	Evaluar y seleccionar las necesidades.
	Desarrollo del programa de formación que cubra los aspectos clave de la seguridad de la información.
	Implementación del programa.
	Seguimiento y evaluación, junto con una actualización continua.
Seguimiento	Reuniones periódicas del equipo del proyecto y revisiones de los resultados de las evaluaciones de formación.
Observaciones o comentarios	Se deberá fomentar la participación de los empleados y crear una cultura de seguridad en toda la organización. Además, la formación debe ser accesible y comprensible para todos los niveles de habilidad y experiencia.
Estado	En proceso.

Tabla 5-4. Proyecto 004. Formación Continua en Seguridad de la Información para empleados.
Fuente: Elaboración propia.

5.2. Planificación del proyecto de mejora

Después de analizar los riesgos, se ha elaborado una planificación detallada de los proyectos para reducir el nivel de riesgo en TRADUX. A continuación, se presenta la planificación por semanas de cada proyecto, considerando su inicio secuencial para garantizar una implementación eficiente y efectiva.

El diagrama de Gantt (Figura 5-1) mostrará las fechas de inicio y finalización de cada tarea, así como las dependencias entre ellas, lo que permitirá identificar posibles cuellos de botella o retrasos y tomar medidas correctivas según sea necesario.

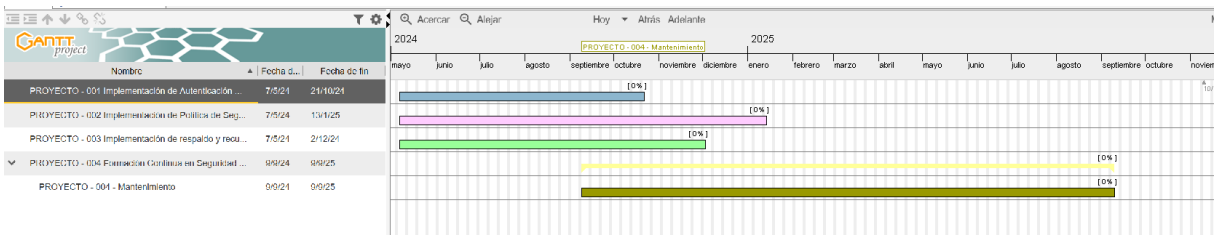

Figura 5-1. Planificación de los proyectos propuestos en el Diagrama de Gantt.
Fuente: Elaboración propia.

5.3. Resultados

A continuación, se han identificado los controles de seguridad de la norma ISO 27002:2022 que están relacionados con cada uno de los proyectos anteriores.

- Proyecto 001 - Implementación de Autenticación Multifactor (MFA).
    - Control de acceso (5.15) - Este control se relaciona directamente con la autenticación multifactor (MFA), que es una medida de seguridad para verificar la identidad de los usuarios.
    - Gestión de la identidad (5.16) - Este control aborda específicamente la autenticación multifactor.
- Proyecto 002 - Implementación de Política de Seguridad de la Información.
    - Políticas para la seguridad de la información (5.1) - Este control se refiere a la necesidad de desarrollar e implementar políticas de seguridad de la información, como se describe en el proyecto.
- Proyecto 003 - Implementación de respaldo y recuperación de datos.
    - Copias de seguridad (8.13) - Este control está relacionado con el establecimiento de un sistema de respaldo automatizado y periódico de los activos de información crítica.
- Proyecto 004 - Formación Continua en Seguridad de la Información para los empleados.
    - Concienciación, educación y formación en seguridad de la información (6.3) - Este control se centra en proporcionar formación continua en seguridad de la información para aumentar la conciencia y promover prácticas seguras en el manejo de datos y sistemas.

Tras la implementación de las propuestas de los proyectos del Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de mejorar los controles y reducir los riesgos, se ha llevado a cabo un análisis exhaustivo. En el gráfico radar se evidencia claramente la evolución positiva y el crecimiento de los diversos dominios una vez que los proyectos sean implementados y se ha mantenido un proceso de mejora continua.

El progreso es notable en la mayoría de los dominios, lo cual se refleja en un aumento sustancial en la efectividad de las medidas de seguridad. Este avance se ha traducido en un incremento generalizado en el nivel de seguridad de la organización. Aproximadamente, el porcentaje de mejora alcanza un promedio del 58,4%, según el análisis comparativo realizado con los datos anteriores (Figura 5-2).

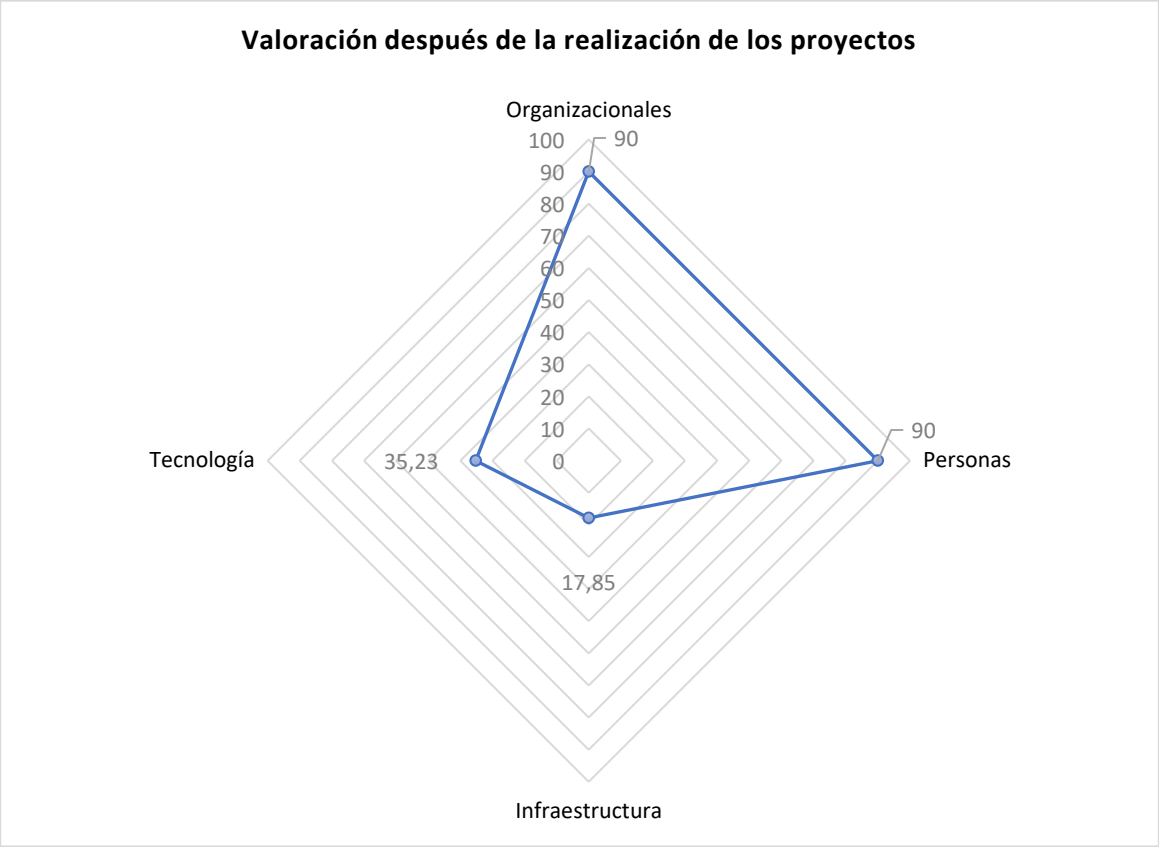

Figura 5-2. Valoración después de la realización de los proyectos.
Fuente: Elaboración propia.

Estos resultados son indicativos del compromiso de la organización con la seguridad de la información y su capacidad para adaptarse y responder de manera efectiva a los desafíos y amenazas en constante evolución. El enfoque en la implementación de proyectos específicos ha demostrado ser una estrategia efectiva para fortalecer la postura de seguridad y garantizar la protección de los activos críticos de la empresa. A continuación, se presentan las imágenes radiales con las mejoras de los proyectos y otra imagen con la comparativa ilustrada, siendo el color naranja el valor anterior a la realización de los proyectos (Figura 5-3).

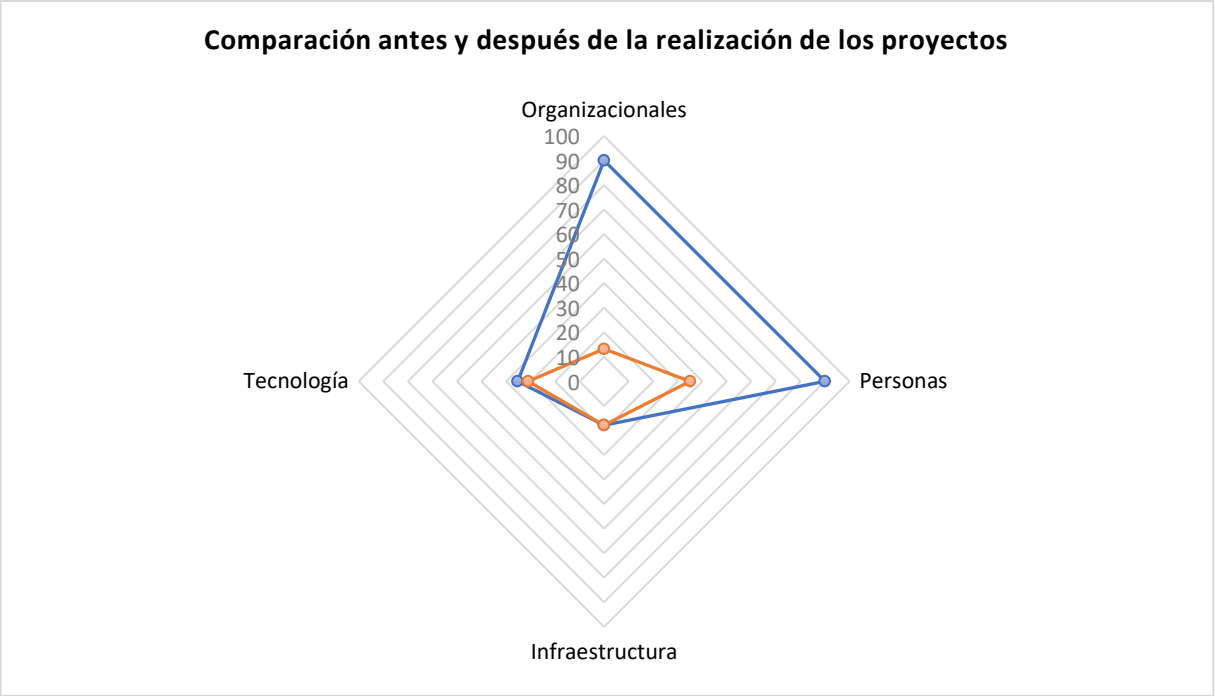

Figura 5-3. Comparación antes y después de la realización de los proyectos.
Fuente: Elaboración propia.

6. AUDITORÍA DE CUMPLIMIENTO

6.1. Introducción

En esta fase se llevará a cabo la auditoría de cumplimiento, cuyo objetivo es evaluar el estado de la seguridad de la información de TRADUX tras haber finalizado con éxito todas las fases anteriores. Para ello, se evaluará el grado de madurez en relación con los diferentes dominios y controles planteados por la ISO/IEC 27001:2022. Antes de comenzar la auditoría de cumplimiento, se asume que los proyectos propuestos en la fase anterior se han implementado correctamente en la organización. Por tanto, se parte de este supuesto para llevar a cabo la evaluación de la seguridad en TRADUX.

6.2. Metodología

Para evaluar de manera adecuada la madurez de la seguridad de la información en TRADUX, se emplea el estándar ISO/IEC 27001:2022, un marco reconocido a nivel internacional y ampliamente aplicable en diferentes organizaciones. Como se indicó a lo largo de este documento, dicho estándar incluye una serie de controles organizados en varios dominios y objetivos de control. Para determinar el estado de la seguridad de la organización, se medirá el nivel de madurez de cada uno de los controles definidos por la norma.

Para ello, se utilizará nuevamente el Modelo de Madurez de Capacidades (CMM), donde se definen los niveles útiles para la evaluación de la seguridad cuando se realizó el Análisis Diferencial del estado inicial de la seguridad en TRADUX.

Véase el apartado 2.2. Análisis Diferencial, Tabla 2-2.

6.3. Alcance

Para evaluar la madurez de la seguridad de la información, se analizarán los siguientes apartados de la ISO/IEC 27001:2022:

4. Contexto de la organización.

5. Liderazgo.
6. Planificación.
7. Soporte.
8. Operación.
9. Evaluación del desempeño.
10. Mejora.

Además, en cumplimiento del apartado 6, también se auditarán los controles de la ISO/IEC 27002:2022:

Controles Organizacionales.
Controles de Personas.
Controles de Infraestructura.
Controles Tecnológicos.

Con esta estructura se permitirá una evaluación exhaustiva y precisa de la madurez de la seguridad de la información en TRADUX, asegurando que todos los elementos claves de la norma ISO/IEC 27001:2022 sean abordados y que se apliquen las mejores prácticas dictadas por los controles de la ISO/IEC 27002:2022.

6.4. Evaluación de la madurez

A continuación, la Tabla 6-1, muestra el grado de madurez obtenido en cada una de las secciones de la ISO/IEC 27001:2022:

N.º	REQUERIMIENTOS ISO 27001:2022	Valoración %	Nivel CMM
4.	**Contexto de la organización**	**90**	**L3**
4.1	Comprensión de la organización y de su contexto	90	L3
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	90	L3
4.3	Determinación del alcance del sistema de gestión de la seguridad de la información	90	L3
4.4	Sistema de gestión de la seguridad de la información	90	L3
5.	**Liderazgo**	**90**	**L3**
5.1	Liderazgo y compromiso	90	L3
5.2	Política	90	L3
5.3	Roles, responsabilidades y autoridades en la organización	90	L3
6.	**Planificación**	**90**	**L3**
6.1	Acciones para tratar los riesgos y oportunidades	90	L3
6.1.1	Consideraciones generales	90	L3
6.1.2	Evaluación de los riesgos de seguridad de la información	90	L3

6.1.3	Tratamiento de los riesgos de seguridad de la información	90	L3
6.2	Objetivos de seguridad de la información y planificación para su consecución	90	L3
6.3	Planificación de cambios	90	L3
7.	**Soporte**	**90**	**L3**
7.1	Recursos	90	L3
7.2	Competencia	80	L2
7.3	Concienciación	100	L5
7.4	Comunicación	90	L3
7.5	Información documentada	90	L3
7.5.1	Consideraciones generales	90	L3
7.5.2	Creación y actualización	90	L3
7.5.3	Control de la información documentada	90	L3
8.	**Operación**	**90**	**L3**
8.1	Planificación y control operacional	90	L3
8.2	Evaluación de los riesgos de seguridad de la información	90	L3
8.3	Tratamiento de los riesgos de seguridad de la información	90	L3
9.	**Evaluación del desempeño**	**90**	**L3**
9.1	Seguimiento, medición, análisis y evaluación	90	L3
9.2	Auditoría interna	90	L3
9.2.1	Consideraciones generales	90	L3
9.2.2	Programa de auditoría interna	90	L3
9.3	Revisión por la Dirección	90	L3
9.3.1	Consideraciones generales	90	L3
9.3.2	Entradas de la revisión por la dirección	90	L3
9.3.3	Resultados de la revisión por la dirección	90	L3
10	**Mejora**	**90**	**L3**
10.1	Mejora continua	90	L3
10.2	No conformidad y acciones correctivas	90	L3

Tabla 6-1. Evaluación de la madurez de las secciones de la ISO/IEC 27001:2022.
Fuente: Elaboración propia.

Seguidamente, tras la mejora obtenida con los proyectos realizados, la Tabla 6-1, muestra el grado de madurez obtenido en cada uno de los controles de la ISO/IEC 27002:2022, junto con la justificación de la valoración:

N.º	CONTROL	Valoración %	Nivel CMM	JUSTIFICACIÓN DE LA VALORACIÓN
5	**Controles organizacionales**	**92,64**	**L3**	
5.1	Políticas para la seguridad de la información	100	L5	La política de seguridad de la información ha sido revisada y mejorada significativamente, y ahora está bien documentada y comunicada a todos los empleados.
5.2	Roles y responsabilidades en seguridad de la información	90	L3	Se han definido claramente los roles y responsabilidades en seguridad de la información, y

				se ha asegurado su comunicación y comprensión por parte de todos los empleados.
5.3	Segregación de tareas	90	L3	Existen procedimientos documentados y consistentes para la segregación de tareas, que se aplican de manera efectiva en toda la organización.
5.4	Responsabilidades de la dirección	95	L4	La dirección ha asumido un papel activo y formal en la seguridad de la información, con responsabilidades claramente definidas y comunicadas formalmente.
5.5	Contacto con las autoridades	90	L3	Se han formalizado los contactos con las autoridades relevantes, y se mantienen relaciones regulares y efectivas para la gestión de incidentes de seguridad de la información.
5.6	Contacto con grupos de interés especial	90	L3	La organización ha establecido contactos con grupos de interés especial, participando activamente en foros y colaboraciones que mejoran la seguridad de la información.
5.7	Inteligencia de amenazas			
5.8	Seguridad de la información en la gestión de proyectos	95	L4	Se han integrado procedimientos sólidos de seguridad de la información en la gestión de proyectos, asegurando la protección adecuada de los datos en todas las fases del ciclo de vida del proyecto.
5.9	Inventario de información y otros activos asociados	90	L3	Se ha realizado un inventario detallado de todos los activos de información, con una documentación adecuada y actualizada regularmente.
5.10	Uso aceptable de la información y otros activos asociados	90	L3	Existe una política formal y comunicada para el uso adecuado de los activos de información, y se asegura su cumplimiento.
5.11	Devolución de activos	90	L3	Los procedimientos de devolución de activos están formalizados y se aplican de manera consistente.
5.12	Clasificación de la información	90	L3	La información se clasifica siguiendo procedimientos formales y bien documentados, asegurando su adecuada protección.
5.13	Etiquetado de la información	90	L3	El etiquetado de la información se realiza de manera estandarizada y formalizada.
5.14	Transferencia de la información	90	L3	Se han implementado controles sólidos para la transferencia segura de la información.
5.15	Control de acceso	100	L5	Los controles de acceso están implementados de manera consistente y documentada, asegurando la protección adecuada de los recursos.
5.16	Gestión de la identidad	100	L5	Se han implementado procesos formales para la gestión de identidades, asegurando un control riguroso sobre el acceso a los recursos de información.
5.17	Información de autenticación	90	L3	La información de autenticación se gestiona de manera segura, siguiendo procedimientos formales y documentados.
5.18	Derechos de acceso	90	L3	Los derechos de acceso están formalmente definidos y se gestionan mediante procedimientos bien documentados.

5.19	Seguridad de la información en las relaciones con proveedores	95	L4	Se han establecido procesos robustos y formales para gestionar la seguridad de la información en las relaciones con proveedores, asegurando una protección adecuada.
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	90	L3	La seguridad de la información está formalmente incluida en los acuerdos con proveedores, asegurando su cumplimiento.
5.21	Gestión de información en la cadena de suministro TIC	90	L3	Existen procedimientos formales para la gestión de la información en la cadena de suministro TIC, asegurando su protección adecuada.
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	90	L3	Se realizan seguimientos y revisiones formales de los servicios de proveedores, asegurando una gestión efectiva del cambio.
5.23	Seguridad de la información para el uso de servicios en la nube	95	L4	Se han implementado controles sólidos y formales para asegurar la información en el uso de servicios en la nube.
5.24	Planificación y preparación para la gestión de incidentes de seguridad de información	95	L4	Existe un plan de gestión de incidentes de seguridad bien definido, coordinado con servicios externos y revisado regularmente.
5.25	Evaluación y decisión sobre los eventos de seguridad de la información	95	L4	Se han establecido procesos formales y continuos para la evaluación y toma de decisiones sobre eventos de seguridad, con evaluación continua del desempeño.
5.26	Respuesta a incidentes de seguridad de la información	95	L4	La respuesta a incidentes de seguridad está formalmente establecida y se realizan revisiones post-incidentes para identificar mejoras.
5.27	Aprender de los incidentes de seguridad de la información	95	L4	Se ha implementado un proceso formal para aprender de los incidentes de seguridad, promoviendo la mejora continua.
5.28	Recopilación de evidencias			
5.29	Seguridad de la información durante la interrupción	95	L4	Se han realizado ejercicios de recuperación ante desastres, mejorando la resiliencia de la empresa frente a interrupciones.
5.30	Preparación de las TIC para la continuidad del negocio			
5.31	Identificación de requisitos legales, reglamentarios y contractuales	95	L4	Se lleva a cabo un seguimiento adecuado de los cambios normativos, asegurando el cumplimiento continuo de la empresa.
5.32	Derechos de propiedad intelectual (DPI)	95	L4	Los esfuerzos para proteger los DPI están formalizados y son efectivos.
5.33	Protección de los registros	90	L3	Se han establecido políticas y procedimientos estandarizados para la protección de los registros.
5.34	Privacidad y protección de datos de carácter personal (DCP)	95	L4	Se han implementado medidas sistemáticas y efectivas para la protección de los datos de carácter personal.
5.35	Revisión independiente de la seguridad de la información	90	L3	Se realizan revisiones independientes de manera consciente y formalizada.

5.36	Conformidad con las políticas, reglas y estándares de seguridad de la información	90	L3	Las políticas de seguridad se siguen y se verifica su cumplimiento de manera regular.
5.37	Documentación de procedimientos operacionales	90	L3	Los procedimientos operacionales están documentados, revisados y actualizados de manera periódica.
6	**Personas**	**95,625**	**L4**	
6.1	Comprobación	95	L4	Las comprobaciones de antecedentes de las personas se realizan de manera estandarizada y efectiva.
6.2	Términos y condiciones de contratación	100	L5	Los términos y condiciones de contratación están claramente definidos y se aplican consistentemente.
6.3	Concienciación, educación y formación en seguridad de la información	100	L5	Los programas de formación en seguridad de la información están plenamente integrados en la cultura organizacional.
6.4	Proceso disciplinario	95	L4	El proceso disciplinario se aplica de manera uniforme y efectiva.
6.5	Responsabilidades ante la finalización o cambio	90	L3	Las responsabilidades ante la finalización o cambio de empleo están formalizadas y se gestionan adecuadamente.
6.6	Acuerdos de confidencialidad o no divulgación	95	L4	Los acuerdos de confidencialidad están plenamente implementados y su cumplimiento es verificado regularmente.
6.7	Teletrabajo	100	L5	Las políticas de teletrabajo están supervisadas y controladas de manera efectiva.
6.8	Notificación de eventos de seguridad de la información	90	L3	Existe un proceso estandarizado y formal para la notificación de eventos de seguridad de la información.
7	**Infraestructura**	**91,78**	**L3**	
7.1	Perímetro de seguridad física	90	L3	Se han mejorado los controles de acceso y registros de visitantes, reduciendo la vulnerabilidad a intrusiones no autorizadas.
7.2	Controles físicos de entrada	90	L3	Los controles físicos de entrada se revisan y mejoran regularmente, asegurando su eficacia.
7.3	Seguridad de oficinas, despachos y recursos	90	L3	La seguridad de las oficinas y recursos se gestiona internamente, con auditorías periódicas para identificar y corregir vulnerabilidades.
7.4	Monitorización de la seguridad física	95	L4	Se han implementado sistemas avanzados de monitorización de la seguridad física, mejorando la detección de amenazas.
7.5	Protección contra las amenazas externas y ambientales	90	L3	Las medidas contra amenazas externas y ambientales están implementadas de manera sistemática y efectiva.
7.6	Trabajo en áreas seguras	95	L4	Las áreas seguras están plenamente integradas en la operación diaria, garantizando la protección adecuada de la información.
7.7	Puesto de trabajo despejado y pantalla limpia	90	L3	Se han implementado políticas y prácticas para mantener los puestos de trabajo despejados y las pantallas limpias.

7.8	Emplazamiento y protección de equipos	90	L3	Se realizan auditorías regulares de seguridad de los equipos, asegurando su protección adecuada.
7.9	Seguridad de los equipos fuera de las instalaciones	95	L4	Las políticas para la seguridad de los equipos fuera de las instalaciones se aplican de manera consistente y efectiva.
7.10	Soportes de almacenamiento	90	L3	Se han formalizado las acciones para la protección de los soportes de almacenamiento.
7.11	Instalaciones de suministro	90	L3	La comunicación con el proveedor de servicios es fluida, asegurando la continuidad de los servicios esenciales.
7.12	Seguridad del cableado	90	L3	Se realizan revisiones regulares del cableado, asegurando su seguridad y funcionalidad.
7.13	Mantenimiento de los equipos	95	L4	El mantenimiento de los equipos está estandarizado y se realiza de manera consistente.
7.14	Eliminación o reutilización segura de equipos	95	L4	Los procesos para la eliminación o reutilización segura de equipos están formalizados y se verifican regularmente.
8	**Tecnología**	**92,85**	**L3**	
8.1	Dispositivos de punto final de los usuarios	95	L4	Los dispositivos de punto final de los usuarios están asegurados de manera consistente y con una cobertura completa.
8.2	Gestión de privilegios de acceso	95	L4	La gestión de privilegios de acceso está bien supervisada y controlada.
8.3	Restricción del acceso a la información	90	L3	Las acciones para restringir el acceso a la información están formalizadas y se aplican consistentemente.
8.4	Acceso al código fuente			
8.5	Autenticación segura	90	L3	Se ha implementado un sistema de autenticación segura formal y completamente desarrollado.
8.6	Gestión de capacidades	95	L4	La gestión de capacidades se realiza de manera estandarizada y consistente.
8.7	Protección contra el código dañino	90	L3	Las medidas contra el código dañino están implementadas de manera sistemática.
8.8	Gestión de las vulnerabilidades técnicas	90	L3	La gestión de vulnerabilidades técnicas se realiza de manera formal y documentada.
8.9	Gestión de la configuración	95	L4	La gestión de la configuración está bien documentada y se gestionan los cambios de manera efectiva.
8.10	Eliminación de la información	95	L4	La eliminación de datos se realiza de manera segura y estandarizada.
8.11	Enmascaramiento de datos	90	L3	Las medidas para el enmascaramiento de datos están formalizadas y se aplican consistentemente.
8.12	Prevención de la fuga de datos	90	L3	Se ha implementado un enfoque formal para la prevención de la fuga de datos.
8.13	Copia de seguridad de la información	100	L5	Las copias de seguridad se realizan siguiendo un proceso formal de restauración y verificación.
8.14	Redundancia recursos de tratamiento de la información	95	L4	La redundancia de recursos está planificada y mantenida de manera óptima.

8.15	Registros de eventos			
8.16	Seguimiento de actividades			
8.17	Sincronización del reloj	90	L3	Se ha implementado un sistema de sincronización automática, asegurando la precisión de los registros y la detección de incidentes.
8.18	Uso de programas de utilidad con privilegios	90	L3	Se ha implementado una política formal para limitar y supervisar el uso de herramientas con privilegios.
8.19	Instalación de software en sistemas en producción	90	L3	Se han implementado procesos formales de revisión y aprobación para la instalación de software.
8.20	Seguridad de redes	90	L3	La seguridad de las redes está gestionada de manera integral y sistemática.
8.21	Seguridad de los servicios de red	95	L4	Los servicios de red cuentan con medidas de seguridad robustas y consistentes.
8.22	Segregación de redes	90	L3	La segregación de redes está plenamente implementada y verificada.
8.23	Filtrado webs	100	L5	El filtrado web está altamente implementado, gestionado y revisado regularmente para asegurar su eficacia.
8.24	Uso de la criptografía	95	L4	La criptografía se gestiona y audita de manera efectiva y periódica.
8.25	Seguridad en el ciclo de vida de desarrollo			
8.26	Requisitos de seguridad de las aplicaciones			
8.27	Arquitectura segura de sistemas y principios de ingeniería			
8.28	Codificación segura			
8.29	Pruebas de seguridad en desarrollo y la aceptación			
8.30	Externalización del desarrollo			
8.31	Separación de los entornos de desarrollo, prueba y producción			
8.32	Gestión de cambios			
8.33	Datos de pruebas			
8.34	Protección de los sistemas de información durante las pruebas de auditoría			

Tabla 6-2. Evaluación de la madurez de los controles de la ISO 27002:2022.
Fuente: Elaboración propia.

A continuación, la Tabla 6-3, muestra las NO CONFORMIDADES con la norma ISO/IEC 27001:2022 encontradas durante la realización de la auditoría de cumplimiento junto con las acciones correctivas recomendadas para que se pueda mejorar el estado de los controles que poseen no conformidades.

N.º	REQUERIMIENTO	TIPO DE NO CONFORMIDAD	DESCRIPCIÓN	ACCIÓN CORRECTIVA
7.2	Competencia	Menor	La organización reconoce la importancia de la competencia; sin embargo, no hay una documentación adecuada que demuestre que las competencias necesarias para los roles que afectan a la seguridad de la información han sido determinadas y aseguradas.	Realizar un análisis de las competencias del personal necesarias y evaluar las actuales. Documentar y mantener actualizadas esas competencias de cada rol, así como, revisar periódicamente asegurando la alineación con los objetivos de seguridad.

Tabla 6-3. No Conformidades (NC) con la ISO/IEC 27001:2022 y las acciones correctivas.
Fuente: Elaboración propia.

Las NO CONFORMIDADES encontradas durante la auditoría de cumplimiento con la norma ISO 27002:2022, junto con las acciones correctivas se muestran en la Tabla 6-4:

N.º	CONTROL	TIPO DE NO CONFORMIDAD	DESCRIPCIÓN	ACCIÓN CORRECTIVA
6.5	Responsabilidades ante la finalización o cambio	Menor	Las responsabilidades ante la finalización o cambio de empleo están formalizadas y se gestionan adecuadamente, pero se podrían mejorar.	Desarrollar y documentar procedimientos adicionales para gestionar la finalización o cambio de empleo y asegurar su cumplimiento.
6.8	Notificación de eventos de seguridad de la información	Menor	Existe un proceso estandarizado y formal para la notificación de eventos de seguridad de la información, pero necesita fortalecerse.	Mejorar el proceso de notificación de eventos de seguridad de la información mediante la capacitación regular y la revisión periódica de los procedimientos.
7.7	Puesto de trabajo despejado y pantalla limpia	Menor	Se han implementado políticas y prácticas para mantener los puestos de trabajo despejados y las pantallas limpias, pero pueden ser más estrictas.	Realizar auditorías regulares y proporcionar formación adicional a los empleados sobre la importancia de mantener un puesto de trabajo despejado y una pantalla limpia.
7.8	Emplazamiento y protección de equipos	Menor	Se realizan auditorías regulares de seguridad de los equipos, asegurando su protección adecuada, pero pueden ser más exhaustivas.	Mejorar los procedimientos de auditoría y protección de equipos mediante la implementación de controles más estrictos y auditorías más frecuentes.

7.10	Soportes de almacenamiento	Menor	Se han formalizado las acciones para la protección de los soportes de almacenamiento, pero podrían fortalecerse.	Revisar y actualizar las políticas de protección de soportes de almacenamiento, asegurando su cumplimiento a través de auditorías regulares.
7.11	Instalaciones de suministro	Menor	La comunicación con el proveedor de servicios es fluida, asegurando la continuidad de los servicios esenciales, pero puede mejorarse.	Implementar un sistema de comunicación y monitoreo más robusto con los proveedores de servicios para asegurar una continuidad aún más sólida.
7.12	Seguridad del cableado	Menor	Se realizan revisiones regulares del cableado, asegurando su seguridad y funcionalidad, pero pueden ser más rigurosas.	Establecer un calendario de revisiones más frecuente y detallado del cableado para asegurar su seguridad y funcionalidad óptima.
8.3	Restricción del acceso a la información	Menor	Las acciones para restringir el acceso a la información están formalizadas y se aplican consistentemente, pero pueden fortalecerse.	Revisar y mejorar las políticas y procedimientos para la restricción del acceso a la información, asegurando su cumplimiento a través de auditorías regulares.
8.5	Autenticación segura	Menor	Se ha implementado un sistema de autenticación segura formal y completamente desarrollado, pero podría mejorarse.	Implementar tecnologías más avanzadas de autenticación y realizar revisiones periódicas para asegurar la efectividad del sistema de autenticación.
8.7	Protección contra el código dañino	Menor	Las medidas contra el código dañino están implementadas de manera sistemática, pero podrían fortalecerse.	Mejorar las medidas de protección contra el código dañino mediante la implementación de herramientas más avanzadas y la capacitación continua del personal.
8.8	Gestión de las vulnerabilidades técnicas	Menor	La gestión de vulnerabilidades técnicas se realiza de manera formal y documentada, pero puede mejorarse.	Fortalecer los procedimientos de gestión de vulnerabilidades técnicas mediante la implementación de evaluaciones más frecuentes y detalladas.
8.11	Enmascaramiento de datos	Menor	Las medidas para el enmascaramiento de datos están formalizadas y se aplican consistentemente, pero pueden ser más estrictas.	Revisar y mejorar las políticas y procedimientos de enmascaramiento de datos, asegurando su cumplimiento mediante auditorías regulares.
8.12	Prevención de la fuga de datos	Menor	Se ha implementado un enfoque formal para la prevención de la fuga de datos, pero podría fortalecerse.	Implementar herramientas y procedimientos más avanzados para la prevención de la fuga de datos, incluyendo la capacitación

				regular del personal y revisiones periódicas de las políticas.
8.17	Sincronización del reloj	Menor	Se ha implementado un sistema de sincronización automática, asegurando la precisión de los registros y la detección de incidentes, pero puede mejorarse.	Revisar y mejorar el sistema de sincronización del reloj, asegurando su precisión mediante pruebas y auditorías regulares.
8.18	Uso de programas de utilidad con privilegios	Menor	Se ha implementado una política formal para limitar y supervisar el uso de herramientas con privilegios, pero puede mejorarse.	Fortalecer la política y los procedimientos de supervisión para el uso de programas de utilidad con privilegios, asegurando su cumplimiento mediante auditorías regulares.
8.19	Instalación de software en sistemas en producción	Menor	Se han implementado procesos formales de revisión y aprobación para la instalación de software, pero pueden mejorarse.	Mejorar los procesos de revisión y aprobación para la instalación de software mediante la implementación de controles más estrictos y auditorías más frecuentes.
8.20	Seguridad de redes	Menor	La seguridad de las redes está gestionada de manera integral y sistemática, pero puede mejorarse.	Revisar y mejorar las políticas y procedimientos de seguridad de redes, asegurando su cumplimiento mediante auditorías regulares y la implementación de tecnologías avanzadas de seguridad de redes.
8.22	Segregación de redes	Menor	La segregación de redes está plenamente implementada y verificada, pero puede mejorarse.	Fortalecer los procedimientos de segregación de redes mediante la implementación de controles más estrictos y auditorías más frecuentes para asegurar su efectividad.

Tabla 6-4. No Conformidades (NC) con la ISO/IEC 27002:2022 y las acciones correctivas.
Fuente: Elaboración propia.

6.5. Resultados

Antes de abordar el último capítulo, se mostrarán los resultados donde se puede ver el nivel de cumplimiento en las secciones de la ISO 27001:2022 (Tabla 6-5).

Nivel de madurez CMM ISO 27001:2022	Inicio	Actual
L0. Inexistente	3	0
L1. Inicial / Ad-hoc	4	0
L2. Repetible	0	0
L3. Definido	0	7
L4. Administrado	0	0
L5. Optimizado	0	0

Tabla 6-5. Resumen Nivel de Madurez ISO 27001:2022.
Fuente: Elaboración propia.

En los siguientes gráficos se compara la situación inicial de TRADUX antes de iniciar el proceso de implantación del SGSI y la situación actual. En ellos se puede observar una variación muy significativa respecto a los resultados con respecto al análisis inicial (Figura 6-1) (Figura 6-2).

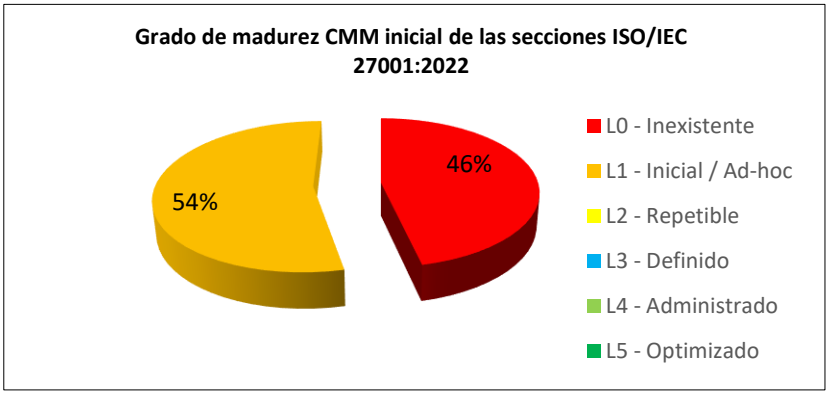

Figura 6-1. Grado de madurez inicial de la ISO/IEC 27001:2022.
Fuente: Elaboración propia.

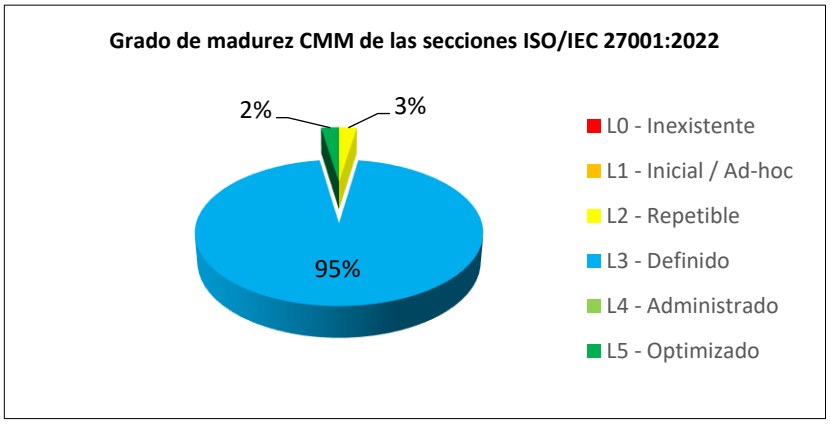

Figura 6-2. Grado de madurez actual de la ISO/IEC 27001:2022.
Fuente: Elaboración propia.

Todos esto resultados referidos a cada una de las secciones de la ISO 27001:2022 se muestran en la siguiente gráfica radial (Figura 6-3).

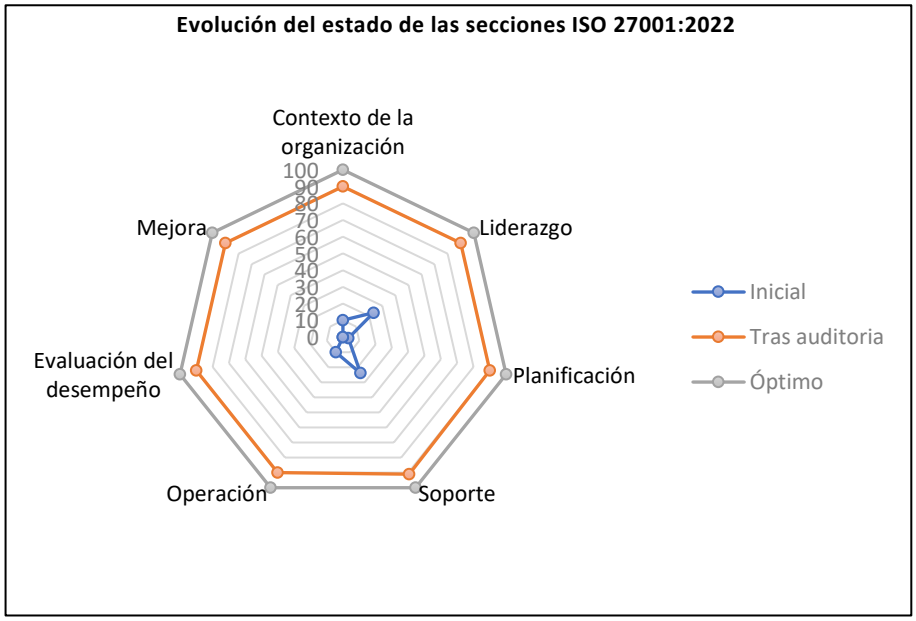

Figura 6-3. Evolución del estado de las secciones ISO 27001:2022.
Fuente: Elaboración propia.

A continuación, también se expondrán los resultados en los que se puede ver el nivel de cumplimiento de los controles de la ISO 27002:2022 (Tabla 6-6).

Nivel de madurez CMM ISO 27002:2022	Inicio	Actual
L0. Inexistente	0	0
L1. Inicial / Ad-hoc	4	0
L2. Repetible	0	0
L3. Definido	0	3
L4. Administrado	0	1
L5. Optimizado	0	0

Tabla 6-6. Resumen Nivel de Madurez ISO 27002:2022.
Fuente: Elaboración propia.

En los siguientes gráficos se compara la situación inicial de TRADUX antes de iniciar el proceso de implantación del SGSI y la situación actual. En ellos se puede observar una variación muy considerable respecto a los resultados con respecto al análisis inicial (Figura 6-4) y (Figura 6-5).

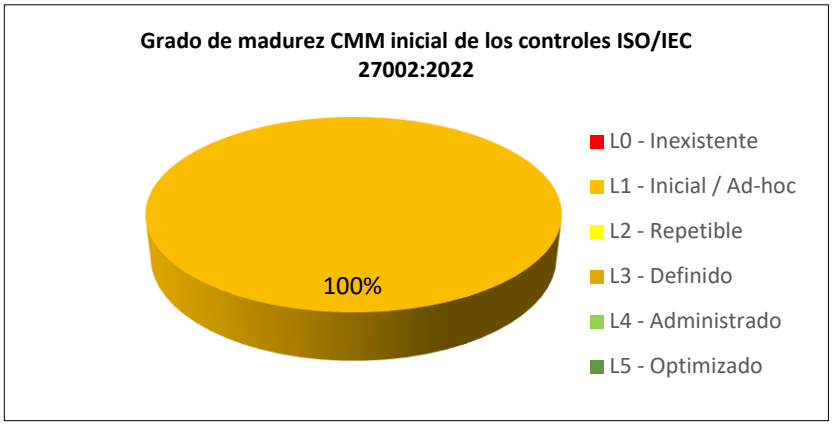

Figura 6-4. Grado de madurez inicial CMM de los controles de la ISO/IEC 27002:2022. Fuente: Elaboración propia.

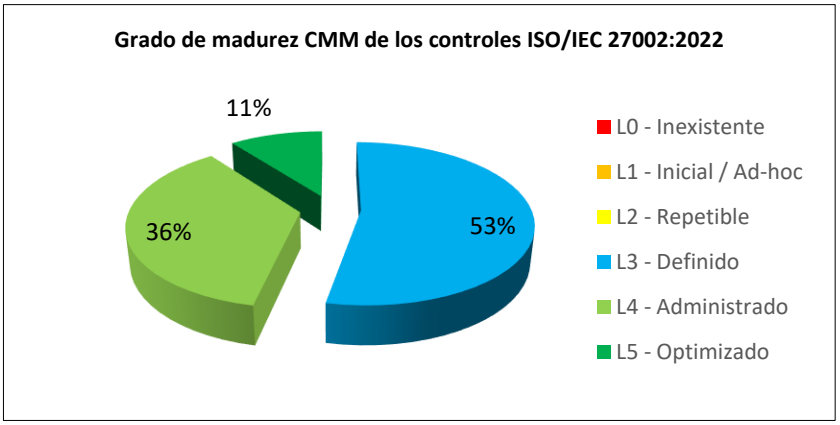

Figura 6-5. Grado de madurez actual CMM de los controles de la ISO/IEC 27002:2022. Fuente: Elaboración propia.

Una vez más, todos estos resultados, en este caso referidos a los controles de la ISO 27002:2022 se muestran en la siguiente gráfica radial (Figura 6-6).

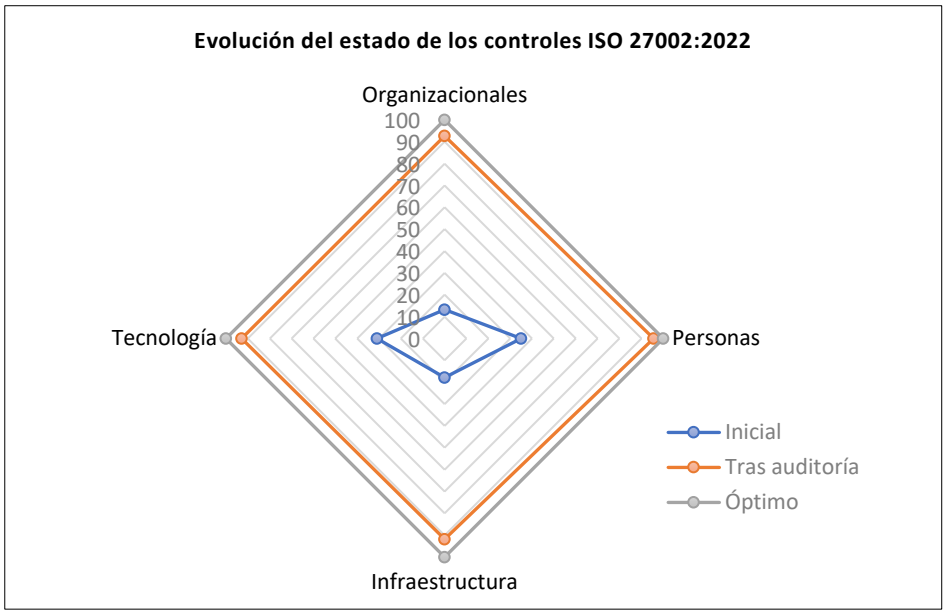

Figura 6-6. Evolución del estado de los controles ISO 27002:2022.
Fuente: Elaboración propia.

Una vez expuestos todos los resultados obtenidos y aun dada por finalizada la implementación del SGSI, tal y como se anticipó cuando se definió el alcance de este proyecto, se observa claramente cómo es prácticamente imposible alcanzar un nivel de seguridad del 100% debido principalmente a las limitaciones de personal, tiempo y recursos económicos.

Por tanto, nos encontramos con un grado de cumplimiento con posibilidades de mejora. Este escenario resulta habitual en empresas que, como TRADUX, implementan un SGSI y se enfrentan a su primera auditoría de cumplimiento. Por ello, será a través de la metodología PDCA como este nivel de madurez y cumplimento podrá ser optimizado.

7. CONCLUSIONES

7.1. Conclusiones

El presente proyecto ha permitido elaborar, desarrollar e implementar el SGSI en TRADUX, empresa ficticia de Traducción e Interpretación, basado en los estándares ISO 27001:2022 e ISO 27002:2022 y utilizando la metodología de análisis de riesgos ligera basada en MAGERIT.

Sin duda alguna, la conclusión más relevante a la que se ha llegado al finalizar este proyecto es la importancia de implantar un SGSI en una organización para conocer y gestionar los riesgos a los que se enfrenta el negocio al manejar su información en el día a día.

Además, conviene resaltar la importancia de crear una buena política de seguridad de la información, ya que estas políticas son las que dictan qué puede o no hacer un empleado con la información, uno de los principales activos que posee una organización, como ya se indicó al comienzo de este proyecto.

7.2. Objetivos superados

Antes de conseguir el objetivo del presente proyecto, ha habido que superar algunas **dificultades** tenidas en su elaboración, como se indican a continuación:

- La principal dificultad que destacar fue cómo comenzar a contextualizar una empresa ficticia en el ámbito lingüístico.

  No fue tarea fácil conseguir información relacionada directamente con el objetivo principal de este proyecto. Aunque es cierto que existe información sobre el SGSI, resulta complicado adaptarla a una empresa inexistente y muchísimo más complejo aún, que haga referencia al ámbito elegido ya que una gran parte de ella se remonta, principalmente, a organizaciones de soluciones informáticas.

- El proceso de selección de la información fue cuestión de dedicar tiempo a su lectura para no confiarnos en lo primero que se publica. No toda información es fiable, hay que comprobar su fuente porque hay mucha "basura" y se debe tener mucha precaución a la hora de seleccionarla.

Además, cuando se requiere información más específica, muchas veces se mezcla con otros ámbitos; otras, resulta demasiado repetitiva, y a menudo, se desvía del objetivo que se quiere conseguir.

No obstante, el haber cursado asignaturas relacionadas con la Ciberseguridad durante el Grado de Ingeniería Informática como, por ejemplo, “Redes y Seguridad” y “Auditoría Informática” o en el propio Máster en Ciberseguridad “Fundamentos de Ciberseguridad”, “Sistemas de Gestión de Seguridad de la Información” y “Auditoría Informática”, entre otras, ha facilitado la comprensión de la información obtenida para llevar a cabo este proyecto.

Una vez superadas las dificultades señaladas anteriormente, se puede afirmar que se ha cumplido tanto el objetivo general como todos los objetivos específicos propuestos al comienzo del TFM y, en definitiva, se ha mejorado la seguridad de la información de la organización gracias a la implementación de un Plan de Seguridad:

- Se ha establecido el estado inicial de la seguridad de la información de TRADUX teniendo en cuenta el Modelo de Madurez de las Capacidades (CMM) en base a las disposiciones o cláusulas de ISO 27001:2022 y de los controles descritos en la ISO 27002:2022.

- Se ha definido y desarrollado el esquema documental necesario para el cumplimiento normativo de la ISO 27001:2022.

- Se ha realizado el análisis de riesgos ligero basado en la metodología MAGERIT, obteniendo el listado de todos los activos de TRADUX, las amenazas posibles a las que está expuesta la organización, así como el impacto y el riesgo de todos los activos de la empresa que ha permitido identificar los activos más prioritarios en cuanto a seguridad de la información.

- Se han definido y completado con éxito las propuestas de proyectos para implementar mejoras y medidas de control adecuadas que permitan mitigar los riesgos encontrados.

- Se ha realizado una auditoría de cumplimiento para evaluar el grado de madurez de los controles realizados en torno al cumplimiento de la ISO 27002:2022.

- Se ha evaluado el nivel de madurez de la seguridad de la información de TRADUX respecto a la norma ISO 27002:2022.

- Se ha creado un plan de concienciación y formación para todo el personal de TRADUX encaminado a conseguir una mejor seguridad de los activos de la información.

En definitiva, tras la realización de todas las fases:

- Se ha conseguido mejorar significativamente el estado inicial de la seguridad de la información de la organización y reducir el riesgo de los activos de la organización, pese a no alcanzar el nivel de seguridad del 100% deseado debido principalmente a las limitaciones de personal, tiempo y recursos económicos.

Por tanto, nos encontramos con un grado de cumplimiento con posibilidades de mejora. Este escenario resulta habitual en empresas, que como TRADUX, implementan un SGSI y se enfrentan a su primera auditoría de cumplimiento. Por tanto, será a través de la metodología PDCA, como este nivel de madurez y cumplimento podrá ser optimizado.

- Se ha logrado la concienciación y colaboración de los empleados en materia de seguridad de la información, así como el compromiso de revisar y mejorar el estado de la seguridad de la información de la organización de manera periódica.

La implementación del SGSI ha logrado cumplir con los objetivos planteados para la gestión de riesgos en TRADUX consiguiendo aplicar los controles necesarios para la mitigación y reducción de los riesgos referentes a la seguridad de la información.

7.3. Futuro trabajo

Si nos parásemos a reflexionar sobre **posibles líneas futuras** de actuación basadas en este TFM, mencionaré algunas de ellas para tener en cuenta:

- Implantar las mejoras propuestas en la fase de auditoría de cumplimiento.

- Una vez implantadas las mejoras propuestas, se deberá intentar conseguir la certificación ISO 27001:2022 como se planteó al inicio del proyecto.

- Continuar trabajando en la mejora del estado de la seguridad de la información de TRADUX con el objetivo de alcanzar el estado óptimo. Para ello, se deberán plantear nuevos proyectos y, así, mejorar aquellos controles que lo precisen.

- Realizar revisiones periódicas al sistema de seguridad de la información de la organización, como se ha indicado en el Plan de Seguridad.

- Insistir en el plan de formación para todo el personal de la organización encaminado a conseguir una mejor seguridad de los activos de la información insistiendo en la importancia de la concienciación y sensibilización de todo el personal relacionado con TRADUX.

Ha llegado el momento de finalizar este documento dando por alcanzados todos los objetivos propuestos al comienzo del presente TFM, mencionando un futuro proyecto como la extensión de este y la utilización de la información expuesta en el aquí presente.

GLOSARIO DE TÉRMINOS

Como se ha visto a lo largo de este proyecto, la importancia de la Seguridad de la Información ha hecho que tengamos que incluir en nuestro vocabulario habitual diferentes términos en los que conviene insistir para su mejor comprensión. Todos ellos han sido seleccionados y ordenados alfabéticamente con el fin de agilizar su búsqueda (Tabla 0-1) [25]:

GLOSARIO DE TÉRMINOS	
TÉRMINO	**DEFINICIÓN**
Activo	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
Alcance	Ámbito de la organización que queda sometido al SGSI.
Amenaza	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Análisis de riesgos	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Autenticación	Provisión de una garantía de que una característica afirmada por una entidad es correcta.
BSI	British Standards Institution, la entidad de normalización del Reino Unido, responsable en su día de la publicación de la norma BS 7799, origen de ISO 27001. Su función como entidad de normalización es comparable a la de AENOR en España.
Competencia	Capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.
Compromiso de la Dirección	Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Control	Medida por la que se modifica el riesgo.
Declaración de aplicabilidad	Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Estimación de riesgos	Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. La estimación de riesgos ayuda en la decisión sobre el tratamiento de riesgos.
Evaluación de riesgos	Proceso global de identificación, análisis y estimación de riesgos.
Fiabilidad	Propiedad del comportamiento y de unos resultados consistentes previstos.

Gestión de incidentes de seguridad de la información	Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
Identificación de riesgos	Proceso de encontrar, reconocer y describir riesgos. La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.
IEC	International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.
Incidente de seguridad de la información	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Indicador	Medida que proporciona una estimación o evaluación.
Integridad	Propiedad de la información relativa a su exactitud y completitud.
ISO	Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).
Mejora continua	Actividad recurrente para aumentar el rendimiento.
Organización	Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos. El concepto de organización incluye pero no se limita a un comerciante individual, compañía, corporación, agencia, empresa, autoridad, sociedad, organización benéfica o institución, o parte o combinación de las anteriores, ya sea sociedad anónima o no, pública o privada.
PDCA	Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.
Plan de continuidad del negocio	Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
Plan Director de Seguridad (PDS)	Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial. Para realizar un buen PDS es fundamental que se alinee con los objetivos estratégicos de la empresa, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización, así como terceros que colaboren con ésta.
Riesgo	Efecto de la incertidumbre sobre los objetivos.
Riesgo residual	El riesgo que permanece tras el tratamiento del riesgo. El riesgo residual puede contener un riesgo no identificado. El riesgo residual también puede denominarse "riesgo retenido".
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.
Sistema de Gestión de la Seguridad de la Información	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza

	una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Tabla 7-1. Glosario de términos.
Fuente: Elaboración propia a partir de ISO 27000.es. Glosario (2005). Obtenido a partir de https://www.iso27000.es/glosario.html

BIBLIOGRAFÍA

Todas las direcciones URL que aparecen a continuación, han sido comprobadas y validadas a fecha de 4 de junio de 2024**:**

[1] NACIONES UNIDAS. *Objetivos de desarrollo sostenible, 2030.* (S. D.)

https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

[2] METODOLOGÍA. *Concepto*. (2013-2023) Enciclopedia. Etecé. (S. D.)

https://concepto.de/metodologia/

[3] QuestionPro. *Tipos de investigación y sus características.* (2023)

https://www.questionpro.com/blog/es/tipos-de-investigacion-de-mercados/

[4] *Qué es la gestión de riesgos y cómo aplicarla a tu proyecto en solo 6 pasos* (2023, febrero).

https://asana.com/es/resources/project-risk-management-process

[5] HERRERO, P. *Riesgos que se deben dominar al gestionar un proyecto*. Sage Group. (2023)

https://www.sage.com/es-es/blog/riesgos-que-se-deben-dominar-al-gestionar-un-proyecto/

[6] Garre S., Segovia, A. J. y Tortajada, A. *Implantación de un sistema de gestión de la seguridad de la información (SGSI).* Universitat Oberta de Catalunya (UOC) (2020, septiembre).

https://www.studocu.com/ca-es/document/universitat-oberta-de-catalunya/sistema-de-gestion-de-la-seguridad/modulo-3-implantacion-de-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/13824650

[7] INGERTEC. *Nueva versión ISO 27001:2022*

https://ingertec.com/nueva-version-iso-27001-2022/

[8] APPLUS CERTIFICATION. *Guía de transición a la nueva ISO/IEC 27001:2022* (2023, 18 de mayo).

https://www.appluscertification.com/global/es/news/publications/guia-transici%C3%B3n-nueva-iso-iec-27001-2022

[9] FEEL AGILE *¿Qué es la ISO 27002?* (2022, 29 de marzo)

https://feelagile.com/es/iso-27002-2022-quest-ce-qui-a-change/#:~:text=La%20historia%20de%20la%20norma,pas%C3%B3%20a%20denominarse%20ISO%2027002.

[10] UNE ISO/IEC 27001:2013. *Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información Requisitos.*

[11] SEGU-INFO. *Cambios en la nueva ISO/IEC 27002:2022*. (2022, 25 de enero).

https://blog.segu-info.com.ar/2022/01/cambios-en-la-nueva-isoiec-270022022.html?m=0

[12] UNE ISO/IEC 27001:2022. *Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de la Seguridad de la Información Requisitos.*

[13] UNE ISO/IEC 27002:2022. *Seguridad de la información, ciberseguridad y protección de la privacidad*

Control de la seguridad de la información.

[14] BENAYAS VALDÉS, A. *Traducción en el entorno digital.* (2011, 6 de noviembre)

https://anabenayasvaldes.wordpress.com/2011/11/06/modelo-de-negocio-para-una-empresa-de-traduccion-e-interpretacion/

[15] INTAREX. *Qué es la infraestructura digital y cómo impacta en la transformación*

https://www.intarex.com/que-es-la-infraestructura-digital/

[16] ISOTools. PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA. *ISO 27001: Los requisitos básicos para aumentar la seguridad de las TIC.* (S. D.)

https://pe.isotools.us/iso-27001-requisitos-basicos-para-aumentar-seguridad-tic/

[17] Jørgensen, S. *La importancia de la seguridad de los datos en el sector lingüístico.* (2024)

https://www.languagewire.com/es-es/blog/seguridad-de-los-datos-en-el-sector-linguistico

[18] IDISC Making comunication easy. *ISO-18587 Posedición del resultado de traducción automática*. (S. D.)

https://www.idisc.com/es/porque-idisc/certificaciones/iso-18587-posedicion-traduccion-automatica

[19] CHAUI. AUDITORÍA INFORMÁTICA. *Niveles de capacidad del Modelo de Madurez de Capacidades (CCM).*

https://chaui1701023085.wordpress.com/2018/02/01/cubo-cobit-4-1/

[20] SAFETY CULTURE. Introducción a la norma ISO 19011:2018 (2024, 15 de enero)

https://safetyculture.com/es/temas/iso-19011/

[21] COMPETENCIAS Y HABILIDADES QUE DEBE TENER UN AUDITOR ISO 27001 (2021, 22 de octubre)

https://www.cynthus.com.mx/competencias-y-habilidades-auditor-iso-27001/

[22] UNIR. *¿Qué es una auditoría interna y qué objetivo tiene?* (2021, 7 de octubre)

https://www.unir.net/empresa/revista/auditoria-interna/

[23] Análisis de riesgos, Universitat Oberta de Catalunya (UOC) (2020, septiembre)

https://materials.campus.uoc.edu/daisy/Materials/PID_00275346/html5/PID_00275346.html#w31aab7c17b9

[24] MAGERIT – versión 3.0 "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" Ministerio de Hacienda y Administraciones Públicas (2012, octubre)

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

Libro I: Método

Libro II: Catálogo de Elementos

Libro III: Guía de Técnicas

[25] ISO 27000.es. Glosario (2005)
https://www.iso27000.es/glosario.html

ANEXOS

Anexo I. ISO/IEC 27001:2022

1. Origen y evolución

A continuación, se indicará el origen y la evolución de la norma a lo largo de estas dos últimas décadas, tal y como se muestra en la Tabla 0-1 [6]:

1901 - Normas "BS". La British Standards Institution publica normas con el prefijo "BS" con carácter internacional.

1995 - Primera publicación oficial de BS 7799-1:1995. Código de buenas prácticas en seguridad de la información. Se trataba de recomendaciones que no permitían la certificación.

1998 - Publicación oficial de la BS 7799-2:1999. Especificaciones de los sistemas de gestión de la seguridad de la información.

1999 - Publicación oficial de la BS 7799. Partes 1 y 2.

2000 - Publicación de la primera versión de la norma ISO/IEC 17799:2000 - Código de buenas prácticas en seguridad de la información.

2002 - Publicación de la nueva versión de la BS7799:2 y publicación oficial por parte de AENOR de la norma UNE-ISO/IEC 17799 - Código de buenas prácticas en seguridad de la información.

2004 - Publicación oficial de la UNE 71502 - Especificaciones de los sistemas de gestión de seguridad de la información.

2005 - Publicación oficial de la ISO/IEC 17799:2005 - Código de buenas prácticas en seguridad de la información y la ISO/IEC 27001:2005 - Especificaciones de los sistemas de gestión de la seguridad de la información.

2007 - Publicación de la ISO/IEC 27006:2007. La ISO 17799:2005 se convierte en la ISO 27002:2005. Publicación de la ISO 27001 en España como UNE-ISO/IEC 27001:2007 AENOR).

2008 - Publicación de la ISO/IEC 27005:2008.

2009 - Publicación de la ISO/IEC 27000:2009 y la ISO/IEC 27004:2009.

2010 - Publicación de la ISO/IEC 27003.

2013 - Publicación de la nueva versión de la ISO 27001:2013, esta versión presenta cambios importantes en su estructura, evaluación y tratamiento de los riesgos.

2022 - Se publica la nueva versión de la ISO 27001:2022

1995	BS 7799-1:1995
1998	BS 7799-2:1998
1999	BS 7799-1 BS 7799-2
2000	ISO 17799:2000
2002	BS 7799-2:2002 UNE-ISO 17799:2000
2004	UNE 71502
2005	ISO/IEC 17799:2005 ISO/IEC 27001:2005
2007	ISO 27001:2007 ISO 17799:2005 se convierte en ISO 27002:2005 UNE-ISO/IEC 27001:2007 (AENOR)
2009	ISO 27000:2009 ISO 27004:2009
2013	ISO 27001:2013
2022	ISO 27001:2022

Tabla 0-1. Evolución de la Norma ISO 27001.
Fuente: Elaboración propia a partir de Implantación de un sistema de gestión de la seguridad de la información (SGSI). Garre S., Segovia, A. J. y Tortajada, A. Fundació Universitat Oberta de Catalunya (FUOC) (2020, septiembre).

Aunque ISO 27001:2013 ya nació bajo la estructura de ISO, estas normas han ido evolucionando en claridad y simplicidad aportando un conjunto de mejores prácticas a aplicar en el desarrollo de nuevos estándares. Nueve años en los que nuestra forma de vivir y trabajar ha cambiado, sobre todo desde la pandemia. Estas nuevas maneras de trabajar no solo han tenido un impacto positivo gracias al trabajo remoto y la democratización de la nube, sino también nuevos riesgos que el SGSI debe tener en cuenta: el perímetro de seguridad de las empresas se ha extendido a los hogares de las personas que trabajan en ellas. Debido a la creciente necesidad de implantar medidas eficaces de ciberseguridad en las organizaciones como consecuencia de numerosos ataques de seguridad existentes, la introducción de las normas ISO en las compañías es una realidad [7].

El 22 de octubre de 2022 se publicó la nueva versión de la norma ISO/IEC 27001:2022 y renombrada como *"Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión*

de la seguridad de la información. Requisitos". Esta nueva versión reemplaza la versión actual ISO/IEC 27001:2013.

2. Transición

El período de transición para ejecutar el cambio es de un plazo máximo de tres años. Las organizaciones que deseen seguir certificadas según la norma ISO/IEC 27001 tendrán que ajustar el cambio a la versión del 2022 dentro del período establecido. Seguidamente, se muestra (Figura 0-1) el calendario de transición de la ISO/IEC 27001:2013 a ISO/IEC 27001:2022 [8]:

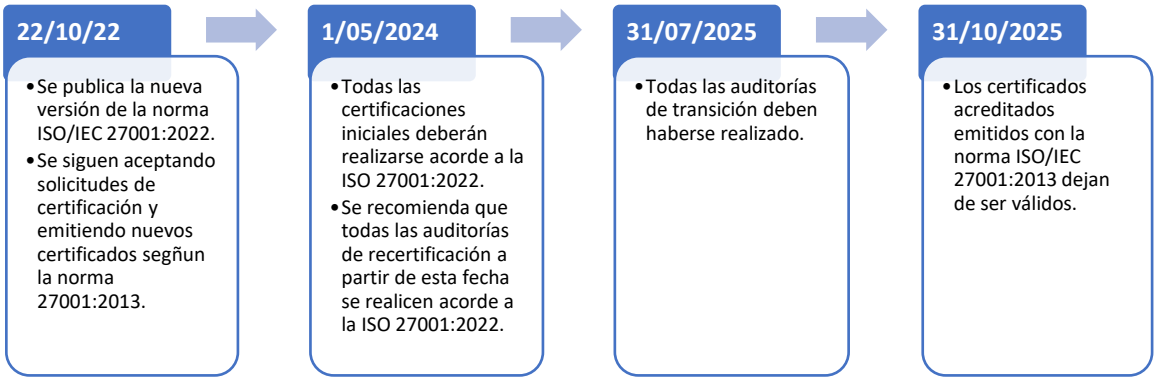

Figura 0-1. Transición a la nueva ISO 27001:2022.
Fuente: Elaboración propia. Obtenido de https://www.appluscertification.com/global/es/news/publications/guia-transici%C3%B3n-nueva-iso-iec-27001-2022

3. Novedades de ISO/IEC 27001:2022

Cambio de nombre

El nombre de la norma cambia de llamarse *"Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos"* a denominarse *"Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos".*

Cambios en el cuerpo de la norma

Aunque no son muy significativos, esta versión ha traído los siguientes cambios [7]:

- Reestructuración de la numeración para acercarla a la estructura de alto nivel.

- En la cláusula 4.4. hay un requisito explícito para definir los procesos y sus interacciones. Esto lo alinea con las mejores prácticas de los sistemas de gestión que indican que estos deben de construirse alrededor de los procesos y de sus interacciones.

- En la cláusula 5.3. se explicita la necesidad de comunicar los roles relevantes en seguridad de la información en toda la organización.

- En la cláusula 6.2. se hace referencia explícita a la monitorización de los objetivos de Seguridad de la Información.

- La cláusula 6.3. nos indica que hay que planificar los cambios del sistema de gestión y que estos se realicen de manera controlada, existiendo un plan de cómo estos se van a implementar y validar.

- En el capítulo 8 se insiste en la gestión por procesos del sistema de gestión de seguridad de la información. En la cláusula 8.1. especifica: "establecer criterios para los procesos y aplicar el control de estos."

- Respecto a la cláusula 9.3, en la revisión por la dirección se deben de tener en cuenta los cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI.

Como vemos los cambios en el cuerpo de la nueva versión ISO 27001 son menores y hacen especialmente hincapié en que los procesos estén claramente definidos junto con sus interacciones.

No obstante, los cambios más importantes de la ISO 27001:2022 se encuentran en su Anexo A, los cuales se corresponden directamente con los que figuran en la ISO/IEC 27002:2022, capítulos 5 a 8, y deben ser empleados en el contexto del apartado 6.1.3.

---

4. Estructura de la Norma ISO/IEC 27001:2022

Estándar publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC). Actualmente es la única norma aceptada a nivel internacional para la gestión de la Seguridad de la Información y se complementa con las mejores prácticas ISO 27002 [9].

La Norma ISO/IEC 27001:2022 se divide en dos partes [10]:

a) La primera parte está compuesta por 11 apartados, del 0 al 3 de carácter introductorios, no obligados para la implementación y del 4 al 10 obligatorios, deben ser efectuados todos sus requerimientos para cumplir con la norma. De hecho, son los que forman parte de las 4 fases del ciclo de Deming o PDCA (Plan-Do-Check-Act), como muestra en la Tabla 0-2. Esta metodología se basa en la mejora continua, ya que un proceso no podrá ser nunca implantado al 100% de efectividad y precisión.

ISO 27001:2022	PDCA (Plan-Do-Check-Act)
0. Introducción 1. Alcance 2. Referencias normativas 4. Términos y definiciones	

4. Contexto de la organización **5. Liderazgo** **6. Planificación** **7. Soporte**	**PLAN (PLANIFICAR)**
8. Operación	**DO (HACER)**
9. Evaluación del Desempeño.	**CHECK (VERIFICAR)**
10. Mejora	**ACT (ACTUAR)**

Tabla 0-2. Apartados de la ISO 27001:2022 que forman parte del PDCA.
Fuente: Elaboración propia.

b) La segunda parte, está conformada por el Anexo A, el cual establece los objetivos de control y los controles de referencia. El Anexo A es un documento normativo que sirve como guía para implementar los controles de seguridad específicos de ISO 27001. La norma ISO 27002, que ya tiene su versión de 2022, desarrolla la guía de implementación de este Anexo.

A continuación, se enumeran sus apartados con una breve explicación sobre cada uno de ellos [10]:

0. Introducción: explica el objetivo de la norma y su compatibilidad con otras normas.

1. Objeto y campo de aplicación: aporta unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.

2. Normas para consulta: recomienda la ISO/IEC 27000 como norma para consulta indispensable para la aplicación de este documento

3. Términos y definiciones: referencia a la Norma ISO/IEC 27000 como estándar.

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

4.1. Comprensión de la organización y de su contexto.
4.2. Comprensión de las necesidades y expectativas de las partes interesadas.
4.3. Determinación del alcance del sistema de gestión de la seguridad de la información.
4.4. Sistema de gestión de la seguridad de la información.

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

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

6. Planificación: define las acciones para tratar los riesgos y oportunidades; y la manera de integrar e implementar las acciones en los procesos del SGSI, y evaluar la eficacia de estas acciones.

6.1. Acciones para tratar los riesgos y oportunidades.
6.2. Objetivos de seguridad de la información y planificación para su consecución.
6.3. Planificación de cambios.

7. Soporte: define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de la información documentada que la organización determine para necesaria para la eficacia del SGSI.

7.1. Recursos.
7.2. Competencia.
7.3. Concienciación.
7.4. Comunicación.
7.5. Información documentada.

8. Operación: la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos, así como evaluar los riesgos en materia de seguridad de la información y su tratamiento.

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

9. Evaluación del desempeño: determina el seguimiento mediante el monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la Dirección antes de proceder con la auditoría externa de certificación.

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

10. Mejora: realiza el proceso de mejora continua del SGSI y la gestión de las no conformidades detectadas en el sistema a través de auditorías internas/externas o empleados.

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

Anexo A: controles de la seguridad de la información de referencia.

Anexo II. ISO/IEC 27002:2022

1. Origen y evolución

Aunque cada versión tiene sus propios cambios, todas ellas tienen en común la misma temática: las buenas prácticas en seguridad de la información. A continuación, se indicará el origen y la evolución de la norma a lo largo de estos últimos veinte años (Tabla 0-3) [9]:

- 1995 - Publicación del estándar ISO/IEC 17799 con origen en el British Standard BS 7799-1.
- 2000 - Publicación del estándar ISO/IEC 17799:2000 por la International Organization for Standardization y la Comisión Electrotécnica Internacional, con el título de Information technology - Security techniques - Code of practice for information security management.
- 2005 - Tras un período de revisión y actualización de los contenidos del estándar, se publica el documento modificado ISO/IEC 17799:2005.
- 2007 - Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007.
- 2013 - Publicación de la norma ISO/IEC 27002:2013 con novedades asociadas al ANEXO A.
- 2022 - Se publica la nueva versión de la ISO 27001:2022

1995	BS 7799-1:1995
2000	ISO 17799:2000
2005	ISO/IEC 17799:2005
2007	ISO 27001:2007
2013	ISO 27001:2013
2022	ISO 27001:2022

Tabla 0-3. Evolución de la norma ISO/IEC 27001:2022.
Fuente: Elaboración propia. Obtenido de https://feelagile.com/es/iso-27002-2022-quest-ce-qui-a-change/#:~:text=La%20historia%20de%20la%20norma,pas%C3%B3%20a%20denominarse%20ISO%2027002.

2. Novedades de ISO/IEC 27002:2022

La nueva versión de la ISO 27002, publicada el pasado 16 de febrero de 2022, trae consigo cambios importantes, siendo los más representativos:

Cambio de nombre

El nombre de la norma cambia de llamarse *"Tecnología de la Información. Técnicas de seguridad. Códigos de Prácticas para los controles de seguridad de la información"* a denominarse *"Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información".*

Nueva estructura de temas y controles

El principal cambio con respecto a la versión anterior se centra en los **controles de seguridad**. A diferencia de los 114 controles organizados en 14 dominios o categorías de la ISO 27002:2013 (Tabla 0-4), la ISO 27002:2022 tiene 93 controles organizados en 4 grupos (Tabla 0-5) [10].

DOMINIOS ISO 27002:2013	CONTROLES
A.5 Políticas de Seguridad de la Información	2
A.6 Organización de la Seguridad de la información	7
A.7 Seguridad de los Recursos Humanos	6
A.8 Gestión de activos	10
A.9 Control de acceso	14
A.10 Criptografía	2
A.11 Seguridad Física y del Entorno	15
A.12 Seguridad de las Operaciones	14
A.13 Seguridad de las Comunicaciones	7
A.14 Adquisición, desarrollo y mantenimiento de sistemas	13
A.15 Relaciones con los proveedores	5
A.16 Gestión de incidentes de seguridad de la información	7
A.17 Aspectos de Seguridad de la información de la Gestión de Continuidad de Negocio	4
A.18 Cumplimiento	8
TOTAL	114

Tabla 0-4. Dominios de Control ISO 27002:2013
Fuente: Elaboración propia a partir de la ISO 27002:2013

TEMAS ISO 27002:2022	CONTROLES
A.5 Organización	37
A.6 Personas	8
A.7 Infraestructura	14
A.8 Tecnología	34
TOTAL	93

Tabla 0-5. Temas ISO 27002:2022
Fuente: Elaboración propia a partir de la ISO 27002:2022

Cambios en los controles desde la ISO 27002:2013

Nuevos controles

El objetivo de esta nueva reestructuración ha sido minimizarlos y agruparlos de una forma más fácil de entender. Estos **11 nuevos controles** (Tabla 0-6) quedan agrupados de la siguiente manera [11]:

- Controles Organizacionales: 37 controles (34 son existentes y 3 nuevos).

- Controles de Personas: 8 controles (sin cambios respecto a la versión anterior).
- Controles de Infraestructura: 14 controles (13 existentes y 1 nuevo).
- Controles Tecnológicos: 34 controles (27 controles existentes y 7 nuevos).

5	ORGANIZATIVOS	CONTROL
5.7	Inteligencia de amenazas	La información relativa a las amenazas a la seguridad de la información debe recopilarse y analizarse para producir información sobre amenazas.
5.23	Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y finalización de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.
5.30	Preparación para las TIC para la continuidad del negocio	La resiliencia de las TIC debe planificarse, implantarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
7	**INFRAESTRUCTURA**	**CONTROL**
7.4	Monitorización de la seguridad física	Las instalaciones deben ser monitorizadas continuamente para detectar cualquier acceso físico no autorizado.
8	**TECNOLOGÍA**	**CONTROL**
8.9	Gestión de la configuración	Se debe ser establecer, documentar, implementar, monitorizar y revisar las configuraciones de hardware, software, servicios y redes, incluyendo sus configuraciones de seguridad.
8.10	Eliminación de la información	La información almacenada en los sistemas de información, en los dispositivos y cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria.
8.11	Enmascaramiento de datos	El enmascaramiento de datos debe utilizarse de acuerdo con la política específica del tema de la organización sobre el control de acceso, con otras políticas temáticas relacionadas, así como con los requisitos de negocio, teniendo en cuenta los requisitos legales aplicables.
8.12	Prevención de fugas de datos	Se deben aplicar medidas de prevención de fugas de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.
8.16	Seguimiento de actividades	Las redes, los sistemas y las aplicaciones deben monitorizarse en busca de comportamientos anómalos y se deben tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.
8.23	Filtrado de webs	El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.
8.28	Codificación segura	Principios de codificación segura deben aplicarse al desarrollo de software.

Tabla 0-6. Nuevos controles de la Seguridad de la Información ISO 27002:2022.
Fuente: Elaboración propia.

Controles que se fusionan con otros controles desde la ISO 27002:2013

Algunos controles procedentes de la ISO 27002:2013 han sido reordenados o fusionados, generando otros nuevos que aparecen en la nueva versión ISO 27002:2022 (Tabla 0-7) [11]:

Controles procedentes de la ISO 27002:2013	Nuevos controles de la ISO 27002:2022
5.1.1 Políticas para la seguridad de la información. **5.1.2 Revisión de las políticas para la seguridad de la información.**	5.1 Políticas de seguridad de la información.
6.2.1 Política de dispositivos móviles. **11.2.8 Equipo de usuario desatendido.**	8.1 Dispositivos de punto final del usuario.
8.1.1 Inventario de activos. **8.1.2 Propiedad de los activos.**	5.9 Inventario de información y otros activos asociados.
8.1.3 Uso aceptable de los activos. **8.2.3 Manipulado de la información.**	5.10 Uso aceptable de la información y activos asociados.
8.3.1 Gestión de soportes extraíbles. **8.3.2 Eliminación de soportes.** **8.3.3 Soportes físicos en tránsito.**	7.10 Medios de Almacenamiento.
9.1.1 Política de control de acceso. **9.1.2 Acceso a las redes y a los servicios de red.**	5.15 Control de Accesos.
9.2.4 Gestión de la información secreta de autenticación de los usuarios. **9.3.1 Uso de la información secreta de autenticación.** **9.4.3 Restricción del acceso a la información.**	5.17 Autenticación de información.
9.2.2 Provisión de acceso de usuario. **9.2.5 Revisión de los derechos de acceso de usuario.** **9.2.6 Retirada o reasignación de los derechos de acceso.**	5.18 Derechos de Acceso
10.1.1 Política de uso de los controles criptográficos. **10.1.2 Gestión de claves.**	8.24 Uso de Criptografía.
11.1.2 Controles físicos de entrada. **11.1.6 Áreas de carga y descarga.**	7.2 Controles de entrada física.
12.1.4 Separación de los recursos de desarrollo, prueba y operación. **14.2.6 Entorno de desarrollo seguro.**	8.31 Separación de ambientes de desarrollo, prueba y producción.
12.4.1 Registro de eventos. **12.4.2 Protección de la información del registro.** **12.4.3 Registros de administración y operación.**	8.15 Inicio de Sesión.
12.5.1 Instalación del software en explotación. **12.6.2 Restricción en la instalación de software.**	8.19 Instalación de software en sistemas operativos.
12.6.1 Gestión de las vulnerabilidades técnicas. **18.2.3 Comprobación del cumplimiento técnico.**	8.8 Gestión de vulnerabilidades técnicas.
12.1.2 Gestión de cambios. **14.2.2 Procedimiento de control de cambios en sistemas.**	8.32 Gestión del Cambio.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. **14.2.4 Restricciones a los cambios en los paquetes de software.**	
13.2.1 Políticas y procedimientos de intercambio de información. **13.2.2 Acuerdos de intercambio de información.** **13.2.3 Mensajería electrónica.**	5.14 Transferencia de información.
14.1.2 Asegurar los servicios de aplicaciones en redes públicas. **14.1.3 Protección de las transacciones de servicios de aplicaciones.**	8.26 Requerimientos de seguridad en aplicaciones.
14.2.8 Pruebas funcionales de seguridad de sistemas. **14.2.9 Pruebas de aceptación de sistemas.**	8.29 de Pruebas de seguridad en el desarrollo y aceptación.
15.2.1 Control y revisión de la provisión de servicios del proveedor. **15.2.2 Gestión de cambios en la provisión del servicio del proveedor.**	5.22 Monitoreo, revisión y gestión del cambio con proveedores de servicios.
16.1.2 Notificación de los eventos de seguridad de la información. **16.1.3 Notificación de puntos débiles de la seguridad.**	6.8 Reporte de eventos de seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información. **17.1.2 Implementar la continuidad de la seguridad de la información.** **17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.**	5.29 Disrupción durante la seguridad de la información.
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales. **18.1.5 Regulación de los controles criptográficos.**	5.31 Identificación de requerimientos legales, estatutarios, regulatorios y contractuales.
18.2.2 Cumplimiento de las políticas y normas de seguridad. **18.2.3 Comprobación del cumplimiento técnico.**	5.36 Cumplimiento con políticas y estándares para la seguridad de la información.

Tabla 0-7. Controles que se fusionan con otros controles de la ISO 27002:2013.
Fuente: Elaboración propia.

Controles que se eliminan desde la ISO 27002:2013

Solo un control fue eliminado desde la versión 2013, el cual corresponde a [11]:

11.2.5 Retirada de materiales propiedad de la empresa.

Nueva estructura de atributos de los controles

El nuevo enfoque de la ISO 27002 conlleva la desaparición del concepto "objetivo de control" y la aparición de cinco atributos para cada control que pueden ayudarnos en la categorización y en el monitoreo de estos. Estos aparecen definidos como se indican a continuación [11]:

Tipo de Control. Cuando o cómo el control impacta en la gestión de riesgos con respecto a la ocurrencia de un incidente de seguridad de la información. Los posibles valores son: #Preventivo (el control actúa

antes de que la amenaza actué), # Detectivo (el control actúa cuando la amenaza ocurre) y #Correctivo (el control actúa después de que la amenaza ocurre).

Propiedades de Seguridad de la Información. Ver los controles desde la perspectiva de qué características de la información contribuirá a preservar la seguridad de la información: #Confidencialidad, #Integridad y #Disponibilidad.

Conceptos de Ciberseguridad. Ver los controles desde la perspectiva de la asociación de controles a conceptos de ciberseguridad descritos en ISO/IEC TS 27110: #Identificar, #Proteger, #Detectar, #Responder y #Recuperar.

Capacidades operacionales. Ver los controles desde la perspectiva profesional de las capacidades de seguridad de la información: #Gobernanza, #Gestión de Activos, #Protección de la Información, #Seguridad en los Recursos Humanos, #Seguridad Física, #Seguridad en sistemas y Redes, #Seguridad en Aplicaciones, #Seguridad en la Configuración, #Gestión de Accesos e Identidades, #Gestión de Amenazas y Vulnerabilidades, #Continuidad, #Seguridad en Relaciones con Proveedores, #Legalidad y Cumplimiento normativo, #Gestión de Eventos de seguridad de la información y #Garantía de seguridad de la información.

Dominios de Seguridad. Permite ver los controles desde la perspectiva de cuatro dominios de seguridad de la información: #Gobernanza y ecosistema, #Protección, #Defensa, #Resiliencia.

Estos atributos establecen subclasificaciones que permiten caracterizar al control. La Figura 0-2 muestra los primeros tres controles del tema de controles organizacionales definidos en la nueva versión de la norma.

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience
5.2	Information security roles and responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience
5.3	Segregation of duties	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance	#Governance_and_Ecosystem

Figura 0-2. Ejemplo de atributos de controles.
Fuente: SEGU-INFO. Cambios en la nueva ISO/IEC 27002:2022. (2022, 25 de enero). Obtenido de https://blog.segu-info.com.ar/2022/01/cambios-en-la-nueva-isoiec-270022022.html?m=0

3. Correspondencia de la ISO/IEC 27002:2022 con la ISO/IEC 27002:2013

El propósito de esta correspondencia es proporcionar compatibilidad con versiones anteriores de la norma ISO/IEC 27002:2013 para organizaciones que actualmente utilizan esa norma y ahora desean hacer la transición a esta edición.

A continuación, se muestra la correspondencia de los controles especificados en los capítulos 5 a 8 de la nueva ISO/IEC 27002:2022 con los de la versión anterior ISO/IEC 27002:2013 (Tabla 0-8) [12]:

Identificador de control UNE-EN ISO/IEC 27002:2022	Identificador de control UNE-EN ISO/IEC 27002:2013	Nombre de control
5		**Controles organizativos**
5.1	05.1.1, 05.1.2	Políticas para la seguridad de la información
5.2	06.1.1	Roles y responsabilidades en seguridad de la información
5.3	06.1.2	Segregación de tareas
5.4	07.2.1	Responsabilidades de la dirección
5.5	06.1.3	Contacto con las autoridades
5.6	06.1.4	Contacto con grupos de interés especial
5.7	Nuevo	Inteligencia de amenazas
5.8	06.1.5, 14.1.1	Seguridad de la información en la gestión de proyectos
5.9	08.1.1, 08.1.2	Inventario de información y otros activos asociados
5.10	08.1.3, 08.2.3	Uso aceptable de la información y otros activos asociados
5.11	08.1.4	Devolución de activos
5.12	08.2.1	Clasificación de la información
5.13	08.2.2	Etiquetado de la información
5.14	13.2.1, 13.2.2, 13.2.3	Transferencia de la información
5.15	09.1.1, 09.1.2	Control de acceso
5.16	09.2.1	Gestión de la identidad.
5.17	09.2.4, 09.3.1, 09.4.3	Información de autenticación
5.18	09.2.2, 09.2.5, 09.2.6	Derechos de acceso
5.19	15.1.1	Seguridad de la información en las relaciones con proveedores
5.20	15.1.2	Abordar la seguridad de la información dentro de los acuerdos de proveedores
5.21	15.1.3	Gestión de información de la información la cadena de suministro TIC

5.22	15.2.1, 15.2.2	Seguimiento, revisión y gestión del cambio de los servicios de proveedores
5.23	Nuevo	Seguridad de la información para el uso de servicios en la nube
5.24	16.1.1	Planificación y preparación para la gestión de incidentes de seguridad de información
5.25	16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información
5.26	16.1.5	Respuesta a incidentes de seguridad de la información
5.27	16.1.6	Aprender de los incidentes de seguridad de la información
5.28	16.1.7	Recopilación de evidencias
5.29	17.1.1, 17.1.2, 17.1.3	Seguridad de la información durante la interrupción
5.30	Nuevo	Preparación de las TIC para la continuidad del negocio
5.31	18.1.1, 18.1.5	Identificación de requisitos legales, reglamentarios y contractuales
5.32	18.1.2	Derechos de propiedad intelectual (DPI)
5.33	18.1.3	Protección de los registros
5.34	18.1.4	Privacidad y protección de datos de carácter personal (DCP)
5.35	18.2.1	Revisión independiente de la seguridad de la información
5.36	18.2.2, 18.2.3	Conformidad con las políticas, reglas y estándares de seguridad de la información
5.37	12.1.1	Documentación de procedimientos operacionales
6		**Personas**
6.1	07.1.1	Comprobación
6.2	07.1.2	Términos y condiciones de contratación
6.3	07.2.2	Concienciación, educación y formación en seguridad de la información
6.4	07.2.3	Proceso disciplinario
6.5	07.3.1	Responsabilidades ante la finalización o cambio
6.6	13.2.4	Acuerdos de confidencialidad o no divulgación
6.7	06.2.2	Teletrabajo
6.8	16.1.2, 16.1.3	Notificación de eventos de seguridad de la información
7		**Infraestructura**
7.1	11.1.1	Perímetro de seguridad física
7.2	11.1.2, 11.1.6	Controles físicos de entrada
7.3	11.1.3	Seguridad de oficinas, despachos y recursos
7.4	Nuevo	Monitorización de la seguridad física
7.5	11.1.4	Protección contra las amenazas externas y ambientales
7.6	11.1.5	Trabajo en áreas seguras
7.7	11.2.9	Puesto de trabajo despejado y pantalla limpia

7.8	11.2.1	Emplazamiento y protección de equipos
7.9	11.2.6	Seguridad de los equipos fuera de las instalaciones
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Soportes de almacenamiento
7.11	11.2.2	Instalaciones de suministro
7.12	11.2.3	Seguridad del cableado
7.13	11.2.4	Mantenimiento de los equipos
7.14	11.2.7	Eliminación o reutilización segura de equipos
8		**Tecnología**
8.1	06.2.1, 11.2.8	Dispositivos de punto final de los usuarios
8.2	09.2.3	Gestión de privilegios de acceso
8.3	09.4.1	Restricción del acceso a la información
8.4	09.4.5	Acceso al código fuente
8.5	09.4.2	Autenticación segura
8.6	12.1.3	Gestión de capacidades
8.7	12.2.1	Protección contra el código dañino
8.8	12.6.1, 18.2.3	Gestión de las vulnerabilidades técnicas
8.9	Nuevo	Gestión de la configuración
8.10	Nuevo	Eliminación de la información
8.11	Nuevo	Enmascaramiento de datos
8.12	Nuevo	Prevención de la fuga de datos
8.13	12.3.1	Copia de seguridad de la información
8.14	17.2.1	Redundancia recursos de tratamiento de la información
8.15	12.4.1, 12.4.2, 12.4.3	Registros de eventos
8.16	Nuevo	Seguimiento de actividades
8.17	12.4.4	Sincronización del reloj
8.18	09.4.4	Uso de programas de utilidad con privilegios
8.19	12.5.1, 12.6.2	Instalación de software en sistemas en producción
8.20	13.1.1	Seguridad de redes
8.21	13.1.2	Seguridad de los servicios de red
8.22	13.1.3	Segregación de redes
8.23	Nuevo	Filtrado webs
8.24	10.1.1, 10.1.2	Uso de la criptografía
8.25	14.2.1	Seguridad en el ciclo de vida de desarrollo
8.26	14.1.2, 14.1.3	Requisitos de seguridad de las aplicaciones
8.27	14.2.5	Arquitectura segura de sistemas y principios de ingeniería

8.28	Nuevo	Codificación segura
8.29	14.2.8, 14.2.9	Pruebas de seguridad en desarrollo y la aceptación
8.30	14.2.7	Externalización del desarrollo
8.31	12.1.4, 14.2.6	Separación de los entornos de desarrollo, prueba y producción
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestión de cambios
8.33	14.3.1	Datos de pruebas
8.34	12.7.1	Protección de los sistemas de información durante las pruebas de auditoría

Tabla 0-8. Correspondencia de ISO/IEC 27002:2022 con ISO/IEC 27002:2013.
Fuente: Elaboración propia a partir de la ISO/IEC 27002:2013 e ISO/IEC 27002:2022

4. Estructura de la Norma ISO/IEC 27002:2022

Estándar para la seguridad de la información publicada por International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC). Su versión más reciente es la norma ISO 27002:2022.

El 15 de febrero de 2022 se publicó una nueva actualización del estándar ISO 27002 que ayuda a implementar las mejores prácticas y controles más eficaces de seguridad de la información, ciberseguridad y protección de la privacidad. Esta nueva versión de la norma ISO 27002:2022 tiene la siguiente estructura [13]:

0. **Introducción**: contextualiza el valor de la información para las organizaciones, cómo es alcanzada la seguridad de la información a través de la implementación de un conjunto de controles de seguridad, los requerimientos de seguridad de la información que debe determinar una organización, la determinación de controles para proteger la información, consideraciones del ciclo de vida de la información (desde su creación hasta su eliminación) y la relación de esta norma con otras normas (especialmente de la familia ISO/IEC 2700).

1. **Alcance**: documento diseñado en el contexto de un sistema de gestión de la seguridad de la información (SGSI) basado en la Norma ISO/IEC 27001, para la implementar controles y desarrollar directrices de gestión de la seguridad en el proceso de implantación de un SGSI basado en la ISO/IEC 27001.

2. **Referencias normativas**: no hay referencias normativas en esta norma.

3. **Términos, definiciones y términos abreviados**: relaciona un conjunto de términos, definiciones y abreviaturas que aplican en el contexto de esta norma.

4. **Estructura del documento**: determina los capítulos, los cuatro temas y los cinco atributos de cada control y el panel de cada control.
5. **Controles organizativos.**
6. **Controles de personas.**
7. **Controles físicos.**
8. **Controles tecnológicos.**

Establece el título del control, tabla de atributos, tipo de control, propósito (por qué implementarse), orientación (cómo implementarse) e información adicional (si aplica) para controles de seguridad.

Anexo A: Este anexo proporciona dos tablas: la primera para explicar el uso de los cinco atributos como forma de crear diferentes vistas de los controles; la segunda muestra un ejemplo de cómo crear una vista filtrando por un valor de atributo particular, en este caso #Correctivo.

Anexo B: Correspondencia de ISO/IEC 27002:2022 con ISO/IEC 27002:2013

Bibliografía: Relación de otras normas y documentos usados en la norma objeto de estudio.

Anexo III. Beneficios de la implantación del SGSI

Los beneficios que obtiene una organización al implantar un SGSI, Figura 0-3, son [6]:

- **Visión común**: permite definir y divulgar unas directrices básicas en materia de seguridad aprobadas por la Dirección, básicas de cualquier acción relacionada con el tratamiento de la información.

- **Implicación de la organización**: define la estructura organizativa para gestionar la seguridad de la información, identificando funciones y responsabilidades desde la alta Dirección hasta el usuario final, estableciendo los niveles de decisión necesarios, y los procedimientos de divulgación / concienciación para implicar a toda la organización.

- **Gestión global y activa**: permite gestionar la seguridad de la información según criterios comunes, procedimientos homogéneos y un vocabulario compartido, y establece los mecanismos para garantizar la vigencia del sistema de gestión, sin quedar obsoleto una vez implantado.

- **Control y seguimiento**: permite disponer de una metodología de medida y evaluación de indicadores, con el fin de valorar los resultados frente a los objetivos establecidos y mantener informada a la Dirección para que pueda tomar decisiones. Asimismo, establece los mecanismos para autoevaluarse y facilita la realización de auditorías de seguridad de la información.

- **Mejora continua**: permite establecer un proceso alcanzar los objetivos en diferentes iteraciones, de forma que el sistema de gestión se va ampliando gradualmente, y permite tener en marcha un proceso de revisión para asegurar que los problemas se detectan y corrigen, que se incorporan las lecciones aprendidas y que se implantan mejoras justificadas, permitiendo evolucionar paso a paso.

- **Optimización de los recursos:**

    - Uso racional y más controlado de la información.
    - Presupuesto justificado, ajustado al riesgo real.
    - Personal concienciado y formado en sus responsabilidades.
    - Ahorro de tiempo, dado que los procedimientos y criterios están definidos y comunicados.
    - Infraestructura ajustada a las necesidades reales del negocio.

Figura 0-3. Beneficios de la implantación del SGSI.
Fuente: Elaboración propia a partir de https://www.studocu.com/ca-es/document/universitat-oberta-de-catalunya/sistema-de-gestion-de-la-seguridad/modulo-3-implantacion-de-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/13824650

El desarrollo de un SGSI se basa en la ISO 27001 y la ISO 27002, así como en el Ciclo de Deming, para garantizar la actualización del sistema y la mejora continua, como se describe en la Figura 0-4 [6]:

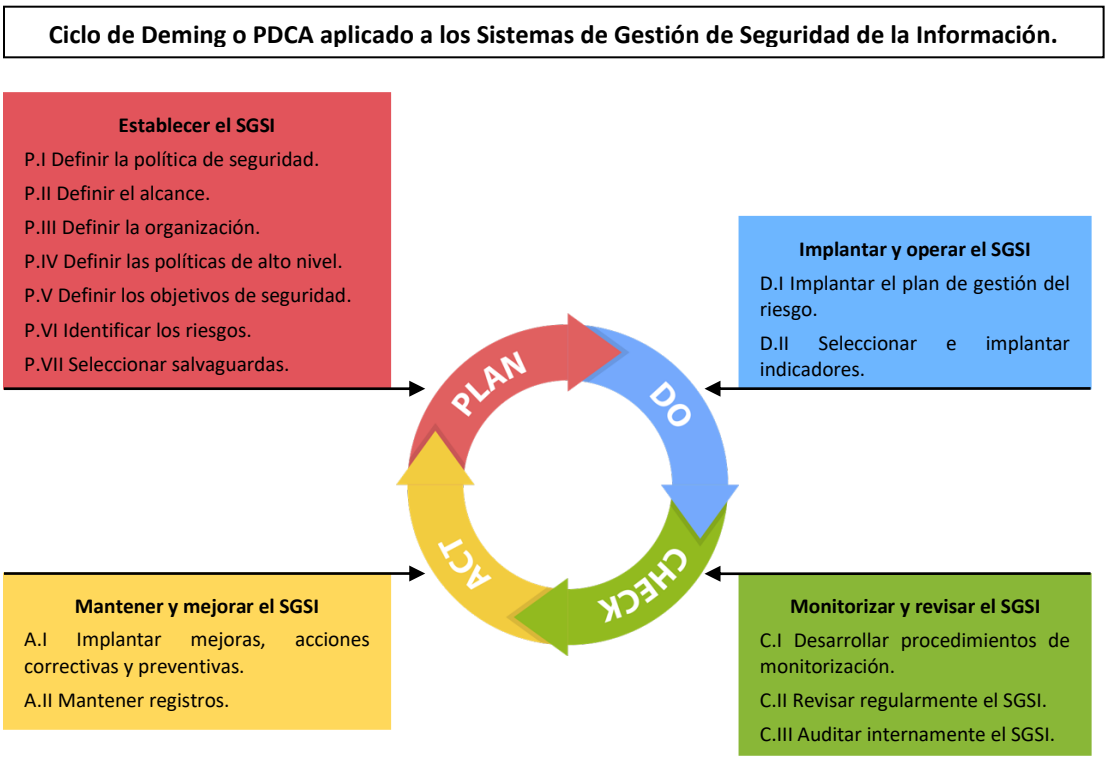

Figura 0-4. Ciclo de Deming aplicado a los sistemas de gestión de seguridad de la información.
Fuente: Elaboración propia a partir de Implantación de un sistema de gestión de la seguridad de la información (SGSI). Garre S., Segovia, A. J. y Tortajada, A. Fundació Universitat Oberta de Catalunya (FUOC) (2020, septiembre). Obtenido de https://www.studocu.com/ca-es/document/universitat-oberta-de-catalunya/sistema-de-gestion-de-la-seguridad/modulo-3-implantacion-de-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/13824650

El ciclo PDCA o Ciclo de Deming consta de cuatro fases:

1ª FASE
PLAN / PLANIFICAR: establecer el SGSI

Previamente a emprender acciones se debe **planificar**, es decir, ver dónde estamos, hacia dónde queremos ir, con qué recursos o medios contamos y sobre qué entorno queremos trabajar.

A continuación, se indican tanto las distintas etapas de esta fase de planificación como las principales características de cada una de ellas [6]:

P. I. Definir la política de seguridad de la información. Establece los principios y líneas de actuación globales en cuestiones de seguridad de la información, alineados con los objetivos del negocio. La política debe demostrar el compromiso de la Dirección con la seguridad de la información y se debe dar a conocer a todos los usuarios.

P. II. Definir el alcance. El primer paso pasa por establecer el alcance del sistema de gestión en términos de procesos, áreas organizativas, emplazamientos y activos.

P. III. Definir la organización de la seguridad de la información. Cada organización deberá crear su propio esquema organizativo interno, asegurando que todas las responsabilidades y funciones en materia de seguridad de la información están correctamente asignadas y garantizando, siempre que sea posible, el principio de segregación de funciones.

P. IV. Definir las políticas de alto nivel. Las políticas de alto nivel contemplan todas las áreas de seguridad de la información.

P. V. Definición de objetivos de seguridad de la información. Establecer objetivos concretos de seguridad de la información, que garanticen que todas las iniciativas en seguridad de la información estén coordinadas y orientadas en una misma dirección, y alineadas con los objetivos del negocio. Los objetivos de seguridad se suelen definir con carácter anual.

P. VI. Identificación de los riesgos. Identificar los activos de información y establecer el riesgo al que están sometidos, indicando cuál sería el impacto para la organización en caso de que se produjera una situación de falta de confidencialidad / privacidad, integridad o disponibilidad de dichos activos.

P. VII. Selección de salvaguardas. Una vez identificados los riesgos que hay que mitigar (riesgos no asumibles) y los objetivos de seguridad que se desea alcanzar, se deberán seleccionar los controles o salvaguardas necesarias.

La selección de controles se puede hacer a partir de la ISO 27002 u otro tipo de controles que se consideren útiles para la organización, aun no estando incluidos en la citada norma.

2ª FASE
DO / HACER: implantar y operar el SGSI.

Una vez finalizada la fase de planificación del SGSI, se entra en la segunda fase del SGSI, compuesta de dos actividades, mostradas en la Figura 0-4 y, sobre las que, a continuación, se indicarán sus principales características [6]:

D.I. Implantación del plan de gestión del riesgo. El Plan de gestión del riesgo determina cómo y cuándo implantar los controles seleccionados y se concreta en el **Plan de seguridad de la información** o **Plan director de seguridad de la información**, que agrupa las acciones en proyectos, las prioriza definiendo acciones a corto y medio plazo (unos 3 años) y realiza una estimación de costes. Dicho Plan de seguridad debe ser presentado a la Dirección para conseguir su aprobación y la dotación presupuestaria necesaria, paso previo al arranque de cualquier proyecto.

D.II. Selección e implantación de indicadores. Para que el sistema se mantenga vivo y actualizado, es necesario evaluar su eficacia de forma continuada. Se deben establecer indicadores que permitan controlar el funcionamiento de las medidas de seguridad de la información implantadas, así como su eficacia y eficiencia, y definir los mecanismos y la periodicidad de medida de dichos indicadores.

3ª FASE
CHECK / VERIFICAR: monitorizar y revisar el SGSI

Esta tercera fase del SGSI se compone de 3 actividades, mostradas en la Figura 0-4 y, sobre las que, seguidamente, se indicarán sus características más importantes [6]:

C.I. Desarrollar procedimientos de monitorización. Resulta imprescindible realizar un seguimiento periódico de los indicadores de seguridad de la información, conocer su estado y evolución y, en definitiva, su eficacia.

C.II. Revisar regularmente el SGSI. La Dirección debe revisar el SGSI a intervalos planificados, para ratificar su conveniencia, adecuación y eficacia. Esta revisión debe ser como mínimo anual, aunque inicialmente se recomienda una periodicidad menor.

C.III. Auditar internamente el SGSI. La comprobación de la idoneidad del diseño e implantación del SGSI se realiza a través de auditorías internas y/o externas, pero siempre adecuadamente planificadas para poder contar con la implicación de todas las personas necesarias.

4ª FASE
ACT / ACTUAR: mantener y mejorar el SGSI

La cuarta y última fase del ciclo del SGSI se compone de dos actividades, mostradas en la Figura 0-4 y, sobre las que, se indicarán sus características principales [6]:

A. I. Implantar mejoras y acciones correctivas. De la monitorización y la revisión del SGSI y de los resultados de las auditorías se obtendrán propuestas de mejora y acciones correctivas y preventivas, que se deberán planificar dentro del Plan de seguridad de la información.

A. II. Mantener registros. Conservar un conjunto de evidencias que prueben que políticas, procedimientos, controles e indicadores no son definiciones teóricas, sino que se están llevando a la práctica tal y como especifica el sistema. Estas evidencias / registros deben ser legibles, identificables y trazables. Cuando no existen requerimientos legales específicos, los registros se suelen guardar unos tres años.

Anexo IV. Análisis diferencial completo con respecto a la ISO 27001:2022

El análisis diferencial detallado de las medidas de seguridad que TRADUX tiene implantadas respecto a las cláusulas de la ISO 27001:2022 frente al Modelo de Madurez de Capacidades (CMM) se muestra en la Tabla 0-9:

N.º	REQUERIMIENTOS ISO 27001:2022	Valoración %	Nivel CMM	JUSTIFICACIÓN DE LA VALORACIÓN
4.	**Contexto de la organización**	**10**	**L1**	
4.1	Comprensión de la organización y de su contexto	10		Aunque hay conciencia sobre la seguridad de la información, la falta de un plan de acción estructurado indica que la comprensión de la organización y su contexto es superficial.
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	10		La organización es consciente de las necesidades y expectativas de las partes interesadas, pero no ha implementado medidas para gestionarlas adecuadamente.
4.3	Determinación del alcance del sistema de gestión de la seguridad de la información	10		La organización está desarrollando el alcance del SGSI.
4.4	Sistema de gestión de la seguridad de la información	10		El SGSI no está establecido ni implementado, por lo que no se realizan revisiones planificadas ni actualizaciones.
5.	**Liderazgo**	**23,3**	**L1**	
5.1	Liderazgo y compromiso	10		La dirección muestra apoyo a la seguridad de la información, pero no ha demostrado un liderazgo efectivo al no establecer un plan de acción estructurado.
5.2	Política	10		Se reconoce la necesidad de una política de seguridad de la información, pero su desarrollo e implementación son insuficientes. Además, no existe el documento de la Política de Seguridad de la Información.
5.3	Roles, responsabilidades y autoridades en la organización	50		Existe una conciencia de los roles y responsabilidades, pero no están documentadas ni registradas.
6.	**Planificación**	**3,3**	**L0**	
6.1	Acciones para tratar los riesgos y oportunidades	10		La organización entiende la importancia de abordar los riesgos y oportunidades, pero la falta de un análisis de riesgos formal y un plan de tratamiento indica que la comprensión y la acción son limitadas.
6.1.1	Consideraciones generales	10		A pesar de haberse considerado los riesgos y oportunidades, no existe un enfoque sistemático.
6.1.2	Evaluación de los riesgos de seguridad de la información	10		No existe un inventario detallado de activos y un análisis de riesgos formal limita la efectividad de la evaluación de riesgos.
6.1.3	Tratamiento de los riesgos de seguridad de la información	10		No se ha implementado un plan de tratamiento de riesgos.

6.2	Objetivos de seguridad de la información y planificación para su consecución	0		No se han establecido objetivos claros ni planificaciones para la consecución de objetivos.
6.3	Planificación de cambios	0		No existe una planificación de cambios.
7.	**Soporte**	**24**	**L1**	
7.1	Recursos	50		Se han identificado y asignado los recursos para la seguridad de la información.
7.2	Competencia	10		Aunque la organización reconoce la importancia de la competencia, hay una falta de documentación.
7.3	Concienciación	50		Existe un nivel de concienciación sobre la seguridad de la información, pero no existe un programa formal de concienciación.
7.4	Comunicación	10		La comunicación sobre la seguridad de la información es limitada y no está formalizada.
7.5	Información documentada	0		Existe una carencia total de procesos parala creación, actualización y control de la información documentada.
7.5.1	Consideraciones generales	0		La organización no ha implementado ningún proceso para la gestión de la información documentada, lo que indica que no se ha reconocido la necesidad de controlar los documentos como parte de la seguridad de la información.
7.5.2	Creación y actualización	0		La ausencia de procesos para la creación y actualización de documentos indica una carencia total.
7.5.3	Control de la información documentada	0		Existe una ausencia de control sobre la información documentada.
8.	**Operación**	**10**	**L1**	
8.1	Planificación y control operacional	20		La organización ha realizado esfuerzos ad hoc para planificar y controlar las operaciones relacionadas con la seguridad de la información. Estos esfuerzos iniciales indican reconocimiento del problema y algunos intentos de abordarlo.
8.2	Evaluación de los riesgos de seguridad de la información	0		No se ha realizado una evaluación formal de los riesgos de seguridad de la información. No hay evidencia de reconocimiento del problema o intentos por resolverlo.
8.3	Tratamiento de los riesgos de seguridad de la información	10		Se han tomado medidas iniciales para tratar los riesgos de seguridad de la información. Aunque no están formalizadas, muestran que la organización ha reconocido el problema y ha comenzado a abordarlo de manera ad hoc.
9.	**Evaluación del desempeño**	**0**	**L0**	
9.1	Seguimiento, medición, análisis y evaluación	0		Existe una ausencia de seguimiento y medición de la seguridad de la información.
9.2	Auditoría interna	0		No se han realizado auditorías internas, lo que indica una falta de reconocimiento de su importancia para el SGSI.

9.2.1	Consideraciones generales	0		Existe una falta de un enfoque general para la auditoría interna.
9.2.2	Programa de auditoría interna	0		No existe un programa de auditoría interna.
9.3	Revisión por la Dirección	0		No existe una revisión por la dirección.
9.3.1	Consideraciones generales	0		No hay un enfoque reconocible para la revisión por la dirección.
9.3.2	Entradas de la revisión por la dirección	0		Existe una ausencia total de entradas para la revisión por la dirección.
9.3.3	Resultados de la revisión por la dirección	0		No existen las revisiones por la dirección por falta de resultados.
10	**Mejora**	**0**	**L0**	
10.1	Mejora continua	0		No existen procesos implementados para garantizar la mejora continua del SGSI.
10.2	No conformidad y acciones correctivas	0		No existen documentos para la mejora continua, ni para registrar las no conformidades ni el tratamiento recomendado de las mismas.

Tabla 0-9. Análisis diferencial completo con respecto a la ISO 27001:2022
Fuente: Elaboración propia a partir de la ISO 27001:2022

Anexo V. Análisis diferencial completo con respecto a la ISO 27002:2022

A continuación, se valorarán los controles indicados en la ISO 27002, a partir del modelo CMM (Tabla 0-10):

N.º	CONTROL	Valoración %	Nivel CMM	JUSTIFICACIÓN DE LA VALORACIÓN
5	**Controles organizacionales**	**13,23**	**L1**	
5.1	Políticas para la seguridad de la información	10		Existe una política para la seguridad de la información documentada, pero es de muy baja calidad, la organización ha reconocido la necesidad de mejorarla.
5.2	Roles y responsabilidades en seguridad de la información	0		Existe una carencia total de los roles y su asignación y responsabilidades en seguridad de la información.
5.3	Segregación de tareas	10		A pesar de que existen esfuerzos iniciales para la segregación de tareas, no hay procedimientos documentados o consistentes.
5.4	Responsabilidades de la dirección	50		La dirección ha empezado a asumir responsabilidades, pero la falta de comunicación formal y dependencia del conocimiento individual limite la valoración.
5.5	Contacto con las autoridades	10		Existe un reconocimiento de la necesidad de contacto con las autoridades, sin embargo, esta acción no está formalizada y es limitada.
5.6	Contacto con grupos de interés especial	0		La organización ha indicado que no se ha establecido contacto, lo que indica una carencia total.
5.7	Inteligencia de amenazas			
5.8	Seguridad de la información en la gestión de proyectos	20		Existe un sistema de seguridad en la gestión de proyectos, pero se reconocen áreas de mejora para fortalecer la protección de la información.
5.9	Inventario de información y otros activos asociados	10		Aunque la empresa tiene conocimiento de sus equipos, no ha realizado un inventario detallado de activos ni un análisis de riesgos. Se carece de una documentación adecuada de los activos y recursos críticos de la organización.
5.10	Uso aceptable de la información y otros activos asociados	10		Aun reconociendo la importancia de establecer normas, procedimientos y reglas claras, actualmente no existe una política formalizada ni comunicada para el uso adecuado de los activos de la organización.
5.11	Devolución de activos	10		A pesar de que existen medidas de devolución de los activos, no están formalizadas.
5.12	Clasificación de la información	10		La organización ha empezado a clasificar la información, pero sin procedimientos formales.
5.13	Etiquetado de la información	10		Existe un etiquetado inicial de la información, pero no está estandarizado.
5.14	Transferencia de la información	0		No existen controles para la transferencia de la información.
5.15	Control de acceso	10		Existe un control de acceso implementado de manera ad hoc.
5.16	Gestión de la identidad	0		Existe una carencia total en la gestión de identidades.
5.17	Información de autenticación	10		Se han tomado medidas iniciales para manejar la información de autenticación.
5.18	Derechos de acceso	10		Los derechos de acceso están definidos, sin embargo, carecen de un proceso formal.

5.19	Seguridad de la información en las relaciones con proveedores	50		Los procesos se encuentran parcialmente establecidos.
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	10		La organización ha reconocido la necesidad, pero no posee acciones formalizadas.
5.21	Gestión de información de la información la cadena de suministro TIC	10		Existen esfuerzos iniciales para la gestión de información de la información la cadena de suministro TIC, pero no están estandarizados.
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	10		Existe un seguimiento y revisión ad hoc de los servicios de proveedores.
5.23	Seguridad de la información para el uso de servicios en la nube	10		Existen medidas iniciales para la seguridad de la información en la nube, pero no hay ningún enfoque formal.
5.24	Planificación y preparación para la gestión de incidentes de seguridad de información	20		Existe un plan de gestión de incidentes de seguridad, sin embargo, su implementación y coordinación con servicios externos no están formalizadas, lo que podría afectar la capacidad de la empresa para responder de manera efectiva ante amenazas de seguridad.
5.25	Evaluación y decisión sobre los eventos de seguridad de la información	20		A pesar de que se cuenta con un trabajador externo responsable de la evaluación y toma de decisiones sobre eventos de seguridad, no se han establecido procesos formales ni se realiza una evaluación continua de su desempeño, lo que podría comprometer la capacidad de respuesta de la empresa ante incidentes de seguridad.
5.26	Respuesta a incidentes de seguridad de la información	20		Aunque se ha designado un trabajador externo para la respuesta a incidentes de seguridad, no se han establecido procedimientos formales ni se realizan revisiones posts-incidentes para identificar áreas de mejora en la respuesta, lo que limita la capacidad de la empresa para gestionar eficazmente los incidentes de seguridad.
5.27	Aprender de los incidentes de seguridad de la información	20		No se ha implementado un proceso formal para aprender de los incidentes de seguridad, lo que dificulta la maximización del aprendizaje y la mejora continua de las prácticas de seguridad de la empresa.
5.28	Recopilación de evidencias			
5.29	Seguridad de la información durante la interrupción	20		Se reconoce la importancia de garantizar la seguridad de los datos durante una interrupción, no se han realizado ejercicios de recuperación ante desastres para mejorar la resiliencia de la empresa, lo que la deja vulnerable ante posibles amenazas.
5.30	Preparación de las TIC para la continuidad del negocio			
5.31	Identificación de requisitos legales, reglamentarios y contractuales	20		Se reconoce la importancia de identificar y mantener actualizados los requisitos legales, regulatorios y contractuales, actualmente no se lleva a cabo un seguimiento adecuado de los cambios normativos, lo que podría afectar el cumplimiento continuo de la empresa.
5.32	Derechos de propiedad intelectual (DPI)	10		A pesar de que existen esfuerzos para proteger el DPI, estos no están formalizados.
5.33	Protección de los registros	10		Se protegen los registros, pero no existen políticas ni procedimientos estandarizados.
5.34	Privacidad y protección de datos de carácter personal (DCP)	10		Se toman medidas para la protección de los datos de carácter personal, pero sin un enfoque sistemático.
5.35	Revisión independiente de la seguridad de la información	10		Se hacen revisiones independientes, pero estas son de manera inconsciente.

5.36	Conformidad con las políticas, reglas y estándares de seguridad de la información	10		Existe un reconocimiento de las políticas, pero sin seguimiento adecuado.
5.37	Documentación de procedimientos operacionales	10		Los procedimientos operacionales están documentados, sin embargo, no se revisan ni actualizan de manera periódica.
6	**Personas**	**35**	**L1**	
6.1	Comprobación	50		Se realizan comprobaciones de los antecedentes de las personas, sin embargo, la metodología no está estandarizada completamente.
6.2	Términos y condiciones de contratación	50		A pesar de que los términos y condiciones estén establecidos, su aplicación puede ser inconsistente.
6.3	Concienciación, educación y formación en seguridad de la información	50		Existen programas de formación, pero no están plenamente integrados en la cultura de la organización.
6.4	Proceso disciplinario	10		Existe el proceso disciplinario, pero no se aplica uniformemente ni de forma efectiva.
6.5	Responsabilidades ante la finalización o cambio	10		Existe conciencia de la importancia de las responsabilidades ante la finalización o cambio de empleo, sin embargo, las acciones no están formalizadas.
6.6	Acuerdos de confidencialidad o no divulgación	50		Los acuerdos de confidencialidad están parcialmente implementados, aunque pueden carecer de seguimiento y aplicación formal.
6.7	Teletrabajo	50		Existen políticas de teletrabajo, pero la supervisión y el control de su cumplimiento son incompletos.
6.8	Notificación de eventos de seguridad de la información	10		Se reconocen los eventos de seguridad de la información, pero no existe un proceso estandarizado para su notificación.
7	**Infraestructura**	**17,85**	**L1**	
7.1	Perímetro de seguridad física	20		Se tiene el control del perímetro de seguridad física, la falta de controles de acceso adecuados y registros de visitantes deja a la empresa vulnerable a posibles intrusiones no autorizadas, lo que requiere una mejora en la vigilancia y seguridad del perímetro físico.
7.2	Controles físicos de entrada	20		Aunque se cuenta con controles físicos de entrada, la falta de revisiones regulares de la eficacia de estos controles puede comprometer la seguridad de las instalaciones, lo que requiere una mejora en la evaluación y el mantenimiento de los controles de acceso físico implementados.
7.3	Seguridad de oficinas, despachos y recursos	10		La gestión de la seguridad de las oficinas y recursos está externalizada, la falta de auditorías periódicas de seguridad física puede dejar a la empresa expuesta a vulnerabilidades, por lo que se requiere una mejora en la realización de auditorías para identificar posibles mejoras.
7.4	Monitorización de la seguridad física	10		Se cuenta con un servicio de monitorización de la seguridad física, la falta de sistemas avanzados de monitorización puede limitar la detección de amenazas, por lo que se requiere una mejora en la implementación de sistemas de monitorización avanzados para mejorar la detección de amenazas.
7.5	Protección contra las amenazas externas y ambientales	10		Aunque se han implementado medidas contra amenazas externas y ambientales, no se han implementado de manera sistemática.
7.6	Trabajo en áreas seguras	50		Existen medidas implementadas para trabajar en áreas seguras, sin embargo, pueden no estar integradas en la operación diaria.

7.7	Puesto de trabajo despejado y pantalla limpia	0		No existen políticas o prácticas para mantener los puestos de trabajo despejados y las pantallas limpias.
7.8	Emplazamiento y protección de equipos	10		Se cuenta con la responsabilidad externalizada del emplazamiento y la protección de equipos, la falta de auditorías regulares de seguridad de los equipos puede dejar a la empresa expuesta a riesgos, por lo que se requiere una mejora en la realización de auditorías de seguridad de los equipos.
7.9	Seguridad de los equipos fuera de las instalaciones	50		Existen políticas para la seguridad de los equipos fuera de las instalaciones, aunque la aplicación y el seguimiento de estas políticas pueden ser inconsistentes.
7.10	Soportes de almacenamiento	10		La organización ha reconocido de la necesidad de proteger los soportes de almacenamiento, pero las acciones son limitadas y no están formalizadas.
7.11	Instalaciones de suministro	10		Se asegura la continuidad de los servicios esenciales, la falta de una comunicación fluida con el proveedor de servicios puede afectar la capacidad de la empresa para garantizar la continuidad de las operaciones, por lo que se requiere una mejora en la comunicación con el proveedor de servicios.
7.12	Seguridad del cableado	10		Se asegura la continuidad de los servicios esenciales, la falta de revisiones regulares del cableado puede dejar a la empresa vulnerable a fallos de seguridad, por lo que se requiere una mejora en la realización de revisiones regulares del cableado.
7.13	Mantenimiento de los equipos	50		Existe y se realiza mantenimiento de los equipos, pero los procedimientos podrían no estar estandarizados ni ser consistentes.
7.14	Eliminación o reutilización segura de equipos	50		Aunque existen procesos para la eliminación o reutilización segura de equipos, pero podrían mejorar en cuanto a seguimiento y verificación.
8	**Tecnología**	**30,95**	**L1**	
8.1	Dispositivos de punto final de los usuarios	50		Se han tomado medidas para asegurar los dispositivos de punto final de los usuarios, sin embargo, la consistencia y la cobertura pueden estar incompletas.
8.2	Gestión de privilegios de acceso	50		A pesar de que los privilegios están gestionados, la supervisión y el control podrían mejorar.
8.3	Restricción del acceso a la información	10		Existe conciencia sobre la necesidad de restringir el acceso, aunque las acciones no están formalizadas y son limitadas.
8.4	Acceso al código fuente			
8.5	Autenticación segura	10		Existen esfuerzos para implementar la autenticación segura, aunque no están completamente desarrollados.
8.6	Gestión de capacidades	50		Las capacidades están gestionadas, sin embargo, la metodología y la aplicación pueden ser inconsistentes
8.7	Protección contra el código dañino	10		Se han implementado medidas contra el código dañino, pero no de manera sistemática.
8.8	Gestión de las vulnerabilidades técnicas	10		Existe un reconocimiento de las vulnerabilidades técnicas, aunque la gestión es ad hoc.
8.9	Gestión de la configuración	50		Existe una gestión de la configuración, pero puede haber carencias en la documentación y en la gestión de cambio.
8.10	Eliminación de la información	50		Se eliminan los datos de manera segura, sin embargo, los procedimientos no están estandarizados.
8.11	Enmascaramiento de datos	10		Se toman medidas para el enmascaramiento de datos, pero no están formalizadas.

8.12	Prevención de la fuga de datos	10		Se reconocen los riesgos de fuga de datos, pero no hay un enfoque para su prevención.
8.13	Copia de seguridad de la información	10		Aunque se realizan copias de seguridad, pero no hay un proceso formal de restauración ni verificación.
8.14	Redundancia recursos de tratamiento de la información	50		Existe la redundancia de recursos, aunque la planificación y el mantenimiento podrían no ser óptimos.
8.15	Registros de eventos			
8.16	Seguimiento de actividades			
8.17	Sincronización del reloj	10		La empresa reconoce la importancia de la sincronización del reloj, la falta de implementación de un sistema de sincronización automática puede afectar la precisión de los registros y la detección de incidentes de seguridad, por lo que se requiere una mejora en la implementación de un sistema de sincronización automática.
8.18	Uso de programas de utilidad con privilegios	10		Se reconoce la importancia de limitar y supervisar el uso de herramientas con privilegios, la falta de una política formal puede dejar a la empresa expuesta a riesgos de seguridad, por lo que se requiere una mejora en la implementación de una política de acceso a herramientas de utilidad basada en privilegios.
8.19	Instalación de software en sistemas en producción	20		Se cuenta con un informático interno para gestionar la instalación de software, la falta de procesos formales de revisión y aprobación puede dejar a la empresa vulnerable a la instalación de aplicaciones no autorizadas, por lo que se requiere una mejora en la implementación de procesos de revisión y aprobación de instalaciones de software.
8.20	Seguridad de redes	50		Las redes se encuentran protegidas en un nivel básico, sin embargo, falta una gestión integral y sistemática.
8.21	Seguridad de los servicios de red	50		Los servicios de red tienen medidas de seguridad, aunque podrían mejorar respecto a la cobertura y la consistencia.
8.22	Segregación de redes	50		Existe segregación de redes, pero la implementación no es completa ni está plenamente verificada.
8.23	Filtrado webs	90		El filtrado web está altamente implementado y gestionado.
8.24	Uso de la criptografía	20		Se cuenta con un informático interno para gestionar el uso de la criptografía, la falta de auditorías periódicas de configuración puede dejar a la empresa vulnerable a vulnerabilidades de seguridad, por lo que se requiere una mejora en la realización de auditorías periódicas de configuración de criptografía.
8.25	Seguridad en el ciclo de vida de desarrollo			
8.26	Requisitos de seguridad de las aplicaciones			
8.27	Arquitectura segura de sistemas y principios de ingeniería			
8.28	Codificación segura			
8.29	Pruebas de seguridad en desarrollo y la aceptación			
8.30	Externalización del desarrollo			
8.31	Separación de los entornos de desarrollo, prueba y producción			
8.32	Gestión de cambios			

8.33	Datos de pruebas			
8.34	Protección de los sistemas de información durante las pruebas de auditoría			

Tabla 0-10. Análisis diferencial completo con respecto a la ISO 27002:2022
Fuente: Elaboración propia a partir de la ISO 27002:2022

Anexo VI. Política de Seguridad de la Información

TRADUX TRADUCCIÓN E INTERPRETACIÓN	POLÍTICA DE SEGURIDAD	Código	SGSI-1
		Versión	1
		Fecha de aprobación	Abril 2024
		Nº páginas	5

Objetivo

El objetivo de esta política consiste en establecer las directrices en seguridad de la información de la empresa TRADUX que permitan preservar la información garantizando la integridad, confidencialidad y disponibilidad de la información y de los activos.

Alcance

La política de seguridad está dirigida y aplicada a todos los servicios de la empresa, así como a todo el personal interno o externo que tenga relación con los activos de la esta. Incluye a empleados, contratistas, proveedores y colaboradores.

Marco normativo

Norma ISO/IEC 27001:2022.

Recursos

En TRADUX, la preservación de la seguridad de la información es considerada como un objetivo común para todo el personal contratado. El equipo humano es fundamental para mantener esta seguridad. Por lo tanto, es crucial que todos los empleados sean conscientes de su responsabilidad.

Se utiliza una tecnología avanzada implementando herramientas y sistemas seguros para proteger los activos digitales. Al mismo tiempo, los procesos internos son sólidos y están diseñados para gestionar riesgos y garantizar la seguridad de la información. Estos procesos son el pilar fundamental para mantener la integridad, confidencialidad y disponibilidad de todos los datos.

Asimismo, la Dirección adquiere el compromiso de dotar a la función de seguridad con los roles necesarios para asegurar su buen hacer, eficiencia, y progresión respecto a la madurez en la implantación de las medidas de seguridad pertinentes.

Descripción de políticas

Se han definido las siguientes políticas que deben ser cumplidas por todo el personal de la empresa:

Política 1. Cumplimiento y sanciones

Todo el personal, tanto interno como externo, debe cumplir rigurosamente las políticas y los procedimientos en cuestión de protección y seguridad de la información. La alta dirección asume la responsabilidad de supervisar y garantizar el cumplimiento adecuado de estas políticas.

El incumplimiento de una política de seguridad es motivo suficiente para iniciar acciones disciplinarias y, dependiendo de su gravedad, puede llegar hasta el cese laboral. La seguridad de la información es un asunto crucial para nuestra organización, y todos debemos asumir nuestra parte en su protección.

Política 2. Personal externo

En TRADUX, se reconoce la importancia de involucrar al personal externo en las prácticas de seguridad de la información. Por lo tanto, el personal externo relacionado con nuestra empresa debe estar plenamente informado sobre sus responsabilidades y obligaciones en relación con la seguridad de la información. Estas responsabilidades deben estar reflejadas en los contratos establecidas con ellos. Es fundamental que comprendan su papel en la protección de los activos.

Además, los acuerdos relacionados con el tratamiento de la información por parte de terceros deben incluir cláusulas específicas que aborden la confidencialidad y privacidad de los datos. Esto garantiza que la información compartida con terceros se maneje de forma segura y se proteja adecuadamente.

Política 3. Acceso físico

En TRADUX, se establecen rigurosas medidas para garantizar el acceso físico seguro a las instalaciones. A continuación, se detallan las directrices:

- El acceso físico de los trabajadores a las diferentes zonas de la empresa debe ser realizado mediante una tarjeta de identificación. En caso de pérdida, el trabajador debe notificarlo de inmediato para tomar las medidas necesarias.

- El personal externo que desee acceder a las instalaciones deberá rellenar sus datos en una lista de control de visitas, siendo el empleado interno del Dpto. TI el responsable de dicha lista. Cada jefe de departamento será el responsable del tiempo que permanezca dicha visita en TRADUX. Al salir de las instalaciones, el visitante deberá firmar en dicha lista para verificar su partida.

- El acceso a los despachos de los jefes de departamento y dirección se realizará utilizando una llave que sólo tendrán las personas que ocupen dichos cargos. El jefe de cada departamento dispondrá de las llaves de todas las salas y su control. El resto de los trabajadores podrá solicitar acceso a las llaves según sus necesidades.

- El acceso a las salas de servidores estará restringido al jefe de TI y al empleado interno de dicho departamento.

Política 4. Uso del servicio de Internet

- Todos los trabajadores deben realizar un uso responsable de internet y en línea con sus tareas laborales, siendo su uso de carácter exclusivo para realizar las actividades profesionales.

- Queda terminantemente prohibido visitar páginas web con contenido ilícito o ilegal, el acceso, uso o instalación de servicios de mensajería instantánea que no sean los utilizados por TRADUX, así como la descarga, uso o instalación de cualquier programa de descarga, juegos o software no aprobados por el Dpto. TI de TRADUX.

Política 5. Uso del correo electrónico

- Cada empleado de TRADUX dispone de una cuenta de correo personal e intransferible que sólo podrá ser utilizada para temas relacionados con el trabajo que desempeñan dentro de la empresa.

- Se prohíbe el uso del correo electrónico con fines personales y que vulnere los derechos fundamentales de las personas.

- Los trabajadores de TRADUX deben rechazar y abstenerse de abrir el correo SPAM. Si se recibiera un correo electrónico sospechoso, debe seguirse el procedimiento definido por la empresa para comprobar su seguridad.

Política 6. Software

- Todos los equipos deben de tener instalado el antivirus utilizado por TRADUX y mantenerlo habilitado en todo momento. Es crucial que el antivirus esté actualizado con la última versión disponible para garantizar una protección efectiva.

- Queda prohibida la instalación de software no aprobado por TRADUX y ningún equipo podrá tener instalado software que no disponga de licencia o no cumpla con los requisitos legales.

- Para la instalación o actualización de nuevo software es imprescindible comunicarlo al empleado interno del Dpto. TI. Previo a la instalación, se consultará con el jefe de TI para determinar si procede o no la instalación.

Política 7. Equipos y hardware

- Todos los equipos deben estar protegidos por contraseña siendo cada trabajador el responsable de su equipo asignado. Cualquier comportamiento anómalo observado en algún equipo debe informarse de manera inmediata al empleado interno del Dpto. TI.

- El equipo debe bloquearse cada vez que el trabajador deje de utilizarlo durante cinco minutos consecutivos o cuando libere su puesto. Esto garantiza la seguridad en caso de ausencia temporal.

- Los sistemas de almacenamiento utilizados deben ser extraídos siempre de manera segura. Esto evita pérdida de datos o daños.

- Los dispositivos de almacenamiento que no se vayan a usar deberán ser entregados al empleado interno del Dpto. TI, quien decidirá si se reutiliza o se retira definitivamente. En cualquier caso, deberá realizar un formateo completo del dispositivo.

- Los ordenadores portátiles dispondrán de un sistema de seguridad para evitar que puedan ser llevados fuera de las instalaciones.

  Si algún trabajador necesita sacar un equipo fuera de las instalaciones, debe comunicárselo al empleado interno del Dpto. TI. Tras consultar al jefe de TI, se procederá a su aprobación. Una vez fuera de las instalaciones, el trabajador será responsable de lo que le suceda tanto al equipo como a la información que contenga.

Política 8. Información

- Queda prohibido sacar fuera de las instalaciones cualquier información restringida o confidencial sin haber obtenido un permiso previo. El empleado interno del Dpto. TI, tras consultar al jefe de TI, evaluará y aprobará o denegará la solicitud de permiso.

- Todos los trabajadores deben recoger los documentos impresos inmediatamente después de enviarlos a imprimir. Es responsabilidad de cada empleado mantener su puesto de trabajo limpio de documentos restringidos o confidenciales. Para la destrucción segura de documentos, se debe utilizar la trituradora de papel.

Política 9. Identificación y Autorización

- Las contraseñas deben ser personales, confidenciales e intransferibles. Cada usuario es responsable de mantener su contraseña de forma segura.

- En ninguna circunstancia se deben anotar las contraseñas en agendas u otros lugares accesibles a otros trabajadores. Esto se aplica tanto a los nombres de usuario como a las contraseñas utilizadas en los diferentes departamentos de la empresa.

- Las contraseñas deben tener entre 8 y 15 caracteres. Deben incluir una combinación de mayúsculas, minúsculas, números y símbolos para aumentar su seguridad.

- Las contraseñas deben cambiarse cada 3 meses. Además, no se puede reutilizar ninguna de las tres contraseñas anteriores.

Política 10. Gestión de copias y recuperación de información

- Las copias de seguridad de la información, el software y los sistemas deben mantenerse y probarse periódicamente. Esto garantiza que la información almacenada esté en buen estado y sea recuperable en caso de necesidad.

- Todos los trabajadores de TRADUX deben realizar copias de seguridad de sus equipos de manera regular. Esto incluye tanto los equipos de oficina como los portátiles utilizados para teletrabajo.

- Se deben realizar copias de seguridad diarias de todos los servidores de TRADUX. El empleado interno del Dpto. TI es responsable de asegurar que las copias de los servidores a su cargo se realicen correctamente.

Política 11. Concienciación y formación de los trabajadores

En TRADUX, la concienciación y la formación en seguridad de la información está considerada como un pilar fundamental para proteger los activos. Todo el personal de la organización y las partes interesadas pertinentes debe recibir una adecuada formación sobre seguridad de la información. Esto incluye comprender los riesgos, las mejores prácticas y la importancia de salvaguardar nuestros datos.

Por ello, se proporciona una formación específica según el puesto de trabajo de cada empleado, abarcando desde el uso correcto de contraseñas hasta la identificación de posibles amenazas y ataques. Además, se realizan actualizaciones periódicas de la política de seguridad de la información y de los procedimientos específicos para mantener a todos informados sobre los cambios y las mejores prácticas.

En definitiva, la concienciación y la formación son herramientas poderosas para fortalecer la seguridad en TRADUX.

Medios de divulgación

Este documento será divulgado mediante el correo electrónico asignado por la propia empresa. Esta vía de comunicación permite llegar de manera efectiva a todos los destinatarios y garantizar que estén informados sobre la política de seguridad de la información en TRADUX.

Anexo VII. Procedimiento de Auditorías Internas

TRADUX TRADUCCIÓN E INTERPRETACIÓN	AUDITORÍAS INTERNAS	Código	SGSI-2
		Versión	1
		Fecha de aprobación	Abril 2024
		Nº páginas	6

Objetivo

El objetivo de este procedimiento es evaluar y conocer el nivel de cumplimiento del SGSI en la empresa TRADUX.

Alcance

Se llevarán a cabo auditorías internas que abarcarán los controles establecidos en la norma ISO/IEC 27002:2022. Estos controles se refieren a aspectos relacionados con la organización, las personas, las infraestructuras y la tecnología.

Marco normativo

Norma ISO/IEC 27001:2022.

Descripción

Las auditorías internas se llevan a cabo con el objetivo de evaluar y asegurar la efectividad del SGSI implementado en TRADUX. Estas auditorías proporcionan una revisión imparcial y objetiva del cumplimiento de los requisitos de la norma y de las mejores prácticas en materia de seguridad de la información. Además, permiten a la empresa identificar los puntos débiles de sus procesos y mejorar continuamente sus sistemas de gestión.

Teniendo en cuenta que TRADUX quiere formar un equipo para realizar auditorías internas al SGSI implantado con el personal que trabaja en la empresa, el equipo auditor estará formado por el Director Ejecutivo (CEO), el Jefe de Tecnologías de la Información (TI), el Jefe Administrativo y Financiero, el Jefe de Traducción y el Jefe de Interpretación.

Cada miembro del equipo desempeñará un rol específico:

- Jefe Auditor: coordinará y liderará la auditoría.
- Auditores de Apoyo: participarán activamente en la evaluación.
- Expertos Técnicos: asesorarán a los auditores en áreas específicas.

El equipo de auditoría realizará las siguientes funciones [20]:

- Observar y analizar las tendencias: identificar patrones recurrentes en los hallazgos.
- Evaluar la eficacia de soluciones: determinar la efectividad de las soluciones para abordar problemas.

- Examinar registros: revisar los registros del programa de auditoría.
- Verificar conformidad: asegurar la conformidad con los procedimientos establecidos.
- Garantizar seguridad y confidencialidad: proteger la información durante todo el proceso.

Al mismo tiempo, los requisitos que deben cumplir los miembros del equipo auditor son:

- No pertenecer al departamento auditado.
- Conocimiento de la norma ISO 27001:2022 e ISO 27002:2022.
- Capacidad para elaborar informes basados en documentos de referencia del proceso.
- Experiencia profesional en el ámbito de las tecnologías de la información y en la realización auditorías de seguridad de la información.

El auditor jefe en las auditorías internas será el Jefe de Tecnologías de la Información (TI) ya que posee el Certificado de Auditor de Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001 y amplia experiencia como auditor jefe. Las habilidades técnicas del auditor jefe son esenciales a la hora de llevar a cabo exitosamente la auditoría dentro de la empresa [21]:

- El auditor jefe debe conocer y comprender el contenido de la norma ISO/IEC 27001:2022 sobre Gestión de la Seguridad de la Información.
- Esto garantiza que las auditorías se realicen conforme a los estándares establecidos.
- Debe saber aplicar sus conocimientos sobre auditorías de seguridad de la información.
- Proporcionará recomendaciones para la prevención y evaluación continuas de las amenazas dentro de la organización.
- El auditor jefe debe estar preparado para asumir responsabilidades en cualquier etapa del proceso de auditoría.
- Su liderazgo es fundamental para el éxito de las evaluaciones.

Además, el auditor jefe debe poseer ciertas características específicas:

- Capacidad para proporcionar información relevante basada en análisis sólidos.
- Mantenerse actualizado en las tendencias y novedades del campo.
- Comunicarse de forma transparente, concisa y directa con los miembros de la organización.
- Transmitir confianza y respeto durante todo el proceso de auditoría.
- Mantener una postura de integridad sin negociar con el auditado.
- Ser objetivo al dictaminar y comunicar riesgos que puedan comprometer la información de la organización.

Cronograma de la auditoría

La planificación de las auditorías internas, mostrada en Tabla 0-11, se llevará a cabo cada 3 años durante los cuatro trimestres (T):

- En el primer año, se llevarán a cabo auditorías sobre los 37 controles organizativos.
- Durante el segundo año, se realizarán auditorías sobre los 8 controles de personas y 14 controles de infraestructuras.
- En el tercer año, se llevarán a cabo auditorías sobre los 34 controles de tecnología.

Nº	CONTROL	1er año				2º año				3er año			
		T 1	T 2	T 3	T 4	T 1	T 2	T 3	T 4	T 1	T 2	T 3	T 4
5	**Controles organizativos**												
5.1	Políticas para la seguridad de la información	x											
5.2	Roles y responsabilidades en seguridad de la información	x											
5.3	Segregación de tareas	x											
5.4	Responsabilidades de la dirección	x											
5.5	Contacto con las autoridades	x											
5.6	Contacto con grupos de interés especial	x											
5.7	Inteligencia de amenazas	x											
5.8	Seguridad de la información en la gestión de proyectos	x											
5.9	Inventario de información y otros activos asociados		x										
5.10	Uso aceptable de la información y otros activos asociados		x										
5.11	Devolución de activos		x										
5.12	Clasificación de la información		x										
5.13	Etiquetado de la información		x										
5.14	Transferencia de la información		x										
5.15	Control de acceso		x										
5.16	Gestión de la identidad		x										
5.17	Información de autenticación		x										
5.18	Derechos de acceso		x										
5.19	Seguridad de la información en las relaciones con proveedores			x									
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores			x									
5.21	Gestión de información de la cadena de suministro TIC			x									
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores			x									
5.23	Seguridad de la información para el uso de servicios en la nube			x									
5.24	Planificación y preparación para la gestión de incidentes de seguridad de información			x									
5.25	Evaluación y decisión sobre los eventos de seguridad de la información			x									
5.26	Respuesta a incidentes de seguridad de la información			x									
5.27	Aprender de los incidentes de seguridad de la información			x									
5.28	Recopilación de evidencias			x									
5.29	Seguridad de la información durante la interrupción			x									
5.30	Preparación de las TIC para la continuidad del negocio				x								
5.31	Identificación de requisitos legales, reglamentarios y contractuales				x								
5.32	Derechos de propiedad intelectual (DPI)				x								
5.33	Protección de los registros				x								
5.34	Privacidad y protección de datos de carácter personal (DCP)				x								
5.35	Revisión independiente de la seguridad de la información				x								

5.36	Conformidad con las políticas, reglas y estándares de seguridad de la información				x								
5.37	Documentación de procedimientos operacionales				x								
6	**Personas**												
6.1	Comprobación					x							
6.2	Términos y condiciones de contratación					x							
6.3	Concienciación, educación y formación en seguridad de la información					x							
6.4	Proceso disciplinario						x						
6.5	Responsabilidades ante la finalización o cambio						x						
6.6	Acuerdos de confidencialidad o no divulgación						x						
6.7	Teletrabajo						x						
6.8	Notificación de eventos de seguridad de la información						x						
7	**Infraestructura**												
7.1	Perímetro de seguridad física							x					
7.2	Controles físicos de entrada							x					
7.3	Seguridad de oficinas, despachos y recursos							x					
7.4	Monitorización de la seguridad física							x					
7.5	Protección contra las amenazas externas y ambientales							x					
7.6	Trabajo en áreas seguras							x					
7.7	Puesto de trabajo despejado y pantalla limpia							x					
7.8	Emplazamiento y protección de equipos								x				
7.9	Seguridad de los equipos fuera de las instalaciones								x				
7.10	Soportes de almacenamiento								x				
7.11	Instalaciones de suministro								x				
7.12	Seguridad del cableado								x				
7.13	Mantenimiento de los equipos								x				
7.14	Eliminación o reutilización segura de equipos								x				
8	**Tecnología**												
8.1	Dispositivos de punto final de los usuarios									x			
8.2	Gestión de privilegios de acceso									x			
8.3	Restricción del acceso a la información									x			
8.4	Acceso al código fuente									x			
8.5	Autenticación segura									x			
8.6	Gestión de capacidades									x			
8.7	Protección contra el código dañino										x		
8.8	Gestión de las vulnerabilidades técnicas										x		
8.9	Gestión de la configuración										x		
8.10	Eliminación de la información										x		
8.11	Enmascaramiento de datos										x		
8.12	Prevención de la fuga de datos										x		
8.13	Copia de seguridad de la información										x		
8.14	Redundancia recursos de tratamiento de la información										x		
8.15	Registros de eventos										x		
8.16	Seguimiento de actividades										x		
8.17	Sincronización del reloj										x		

8.18	Uso de programas de utilidad con privilegios										x	
8.19	Instalación de software en sistemas en producción										x	
8.20	Seguridad de redes										x	
8.21	Seguridad de los servicios de red										x	
8.22	Segregación de redes										x	
8.23	Filtrado webs										x	
8.24	Uso de la criptografía										x	
8.25	Seguridad en el ciclo de vida de desarrollo										x	
8.26	Requisitos de seguridad de las aplicaciones											x
8.27	Arquitectura segura de sistemas y principios de ingeniería											x
8.28	Codificación segura											x
8.29	Pruebas de seguridad en desarrollo y la aceptación											x
8.30	Externalización del desarrollo											x
8.31	Separación de los entornos de desarrollo, prueba y producción											x
8.32	Gestión de cambios											x
8.33	Datos de pruebas											x
8.34	Protección de los sistemas de información durante las pruebas de auditoría											x

Tabla 0-11. Planificación de la Auditoría Interna.
Fuente: Elaboración propia

Fases de la auditoría interna

Los pasos de la auditoría interna son los mostrados a continuación (Figura 0-5) [22]:

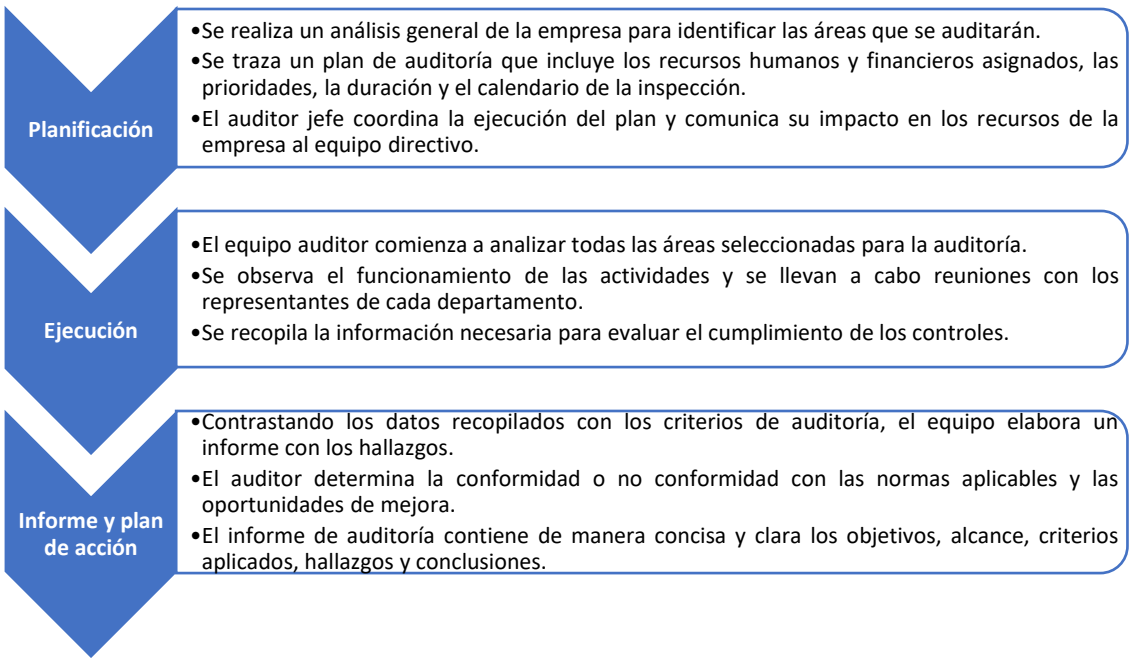

Figura 0-5. Fases de una auditoría interna.
Fuente: Elaboración propia a partir de https://www.unir.net/empresa/revista/auditoria-interna/

Control de cambios

Una vez que el equipo auditor redacte el informe de auditoría con los hallazgos, las no conformidades detectadas y las recomendaciones pertinentes, dicho informe deberá ser actualizado, revisado y aprobado, como se muestra en la Tabla 0-12:

Versión	Fecha	Actualizado	Revisado	Aprobado
1	12/04/24	Firma Nombre y apellidos Cargo que ocupa	Firma Nombre y apellidos Cargo que ocupa	Firma Nombre y apellidos Cargo que ocupa
2				

Tabla 0-12. Modelo del control de cambios de auditoría interna.
Fuente: Elaboración propia.

Medios de divulgación

El medio de comunicación por el cual se divulgará este documento será exclusivamente a través del correo electrónico asignado por la propia empresa.

Anexo VIII. Gestión de Indicadores

TRADUX TRADUCCIÓN E INTERPRETACIÓN	GESTIÓN DE INDICADORES	Código	SGSI-3
		Versión	1
		Fecha de aprobación	Abril 2024
		Nº páginas	2

Objetivo

El objetivo de este procedimiento es establecer un marco para la gestión de indicadores de seguridad de la información en TRADUX asegurando la monitorización, medición, análisis y evaluación efectivos del desempeño del SGSI.

Alcance

Este anexo se aplica a todos los empleados, directivos y partes interesadas involucradas en la gestión de la seguridad de la información en TRADUX.

Marco normativo

Norma ISO/IEC 27001:2022.

Descripción

Este procedimiento establece un marco para la gestión de indicadores de seguridad de la información en TRADUX, conforme a ISO/IEC 27001:2022. Se aplica a la identificación, seguimiento, medición, análisis y evaluación de indicadores donde:

- la alta dirección aprueba KPIs y proporciona recursos;
- el responsable de seguridad coordina la gestión;
- los departamentos suministran datos;
- se identifican KPIs según ISO/IEC 27001:2022, se establecen métodos, calendario y responsabilidades. Se analizan resultados y se documenta evidencia.

Este procedimiento será revisado periódicamente para garantizar su adecuación y mejora continua.

A continuación, en la Tabla 0-10, se muestran los indicadores que se tendrán en cuenta para medir la eficacia de los controles de seguridad implantados por TRADUX:

- **ID**. Nomenclatura establecida por TRADUX para identificar el indicador.
- **Descripción del indicador**. Explicación del objetivo de medida de dicho indicador.
- **Control**. Definido en la ISO 27002:2022.

- **Periodicidad**. Cada cuánto tiempo se debe recoger la medición.

- **Valor objetivo y valor umbral**. Cuál es el valor que sería correcto para la empresa y cuál es el valor por debajo del cual se debiera levantar una alarma.

- **Responsable de la medida**. Sobre qué cargo recae la responsabilidad de proporcionar el resultado de la medida.

ID	Nombre	Descripción	Control	Periodicidad	Valor objetivo/ Valor umbral	Responsable
IN1	Políticas para la seguridad de la información	Verificar que se realiza la revisión de las políticas de seguridad por parte de la Dirección.	5.1	Anual	2 / 1	Comité de Seguridad
IN2	Roles y responsabilidades en seguridad de la información	Verificar si los roles y responsabilidades en cuanto a seguridad de la información están definidos.	5.2	Anual	100% / 90%	Comité de Seguridad
IN3	Segregación de tareas	Verificar que se implementa la segregación de tareas para limitar el acceso a la información y evitar conflictos de interés.	5.3	Semestral	100% / 95%	Comité de Seguridad
IN5	Inventario de información y otros activos asociados	Verificar la existencia y actualización del inventario de información y activos asociados.	5.9	Trimestral	100% / 90%	Comité de Seguridad
IN6	Control de acceso	Verificar la efectividad de los controles de acceso implementados para proteger la información.	5.15	Mensual	100% / 95%	Comité de Seguridad
IN8	Seguridad de la información en las relaciones con proveedores	Verificar que se cumplen los requisitos de seguridad de la información en las relaciones con proveedores.	5.19	Semestral	100% / 90%	Comité de Seguridad
IN9	Identificación de requisitos legales, reglamentarios y contractuales	Verificar la identificación y cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con la seguridad de la información.	5.31	Anual	100% / 95%	Comité de Seguridad
IN12	Copia de seguridad de la información	Verificar la realización y efectividad de las copias de seguridad de la información.	8.13	Semanal	100% / 95%	Dpto. TI
IN13	Redundancia recursos de tratamiento de la información	Verificar la implementación y operatividad de la redundancia de recursos para asegurar la	8.14	Mensual	100% / 95%	Dpto. TI

		disponibilidad de la información.				
IN14	Seguridad de redes	Verificar la efectividad de los controles de seguridad implementados en las redes de la empresa.	8.20	Trimestral	100% / 95%	Dpto. TI
IN15	Seguridad de los servicios de red	Verificar la seguridad de los servicios críticos de red contra amenazas como el acceso no autorizado y el malware.	8.21	Mensual	100% / 95%	Dpto. TI
IN16	Segregación de redes	Verificar la implementación y efectividad de la segregación de redes para limitar la exposición a amenazas.	8.22	Semestral	100% / 95%	Dpto. TI
IN17	Filtrado webs	Verificar la implementación y operatividad del filtrado web para controlar y proteger el acceso a sitios potencialmente maliciosos o inseguros.	8.23	Mensual	100% / 95%	Dpto. TI

Tabla 0-13. Gestión de Indicadores.
Fuente: Elaboración propia.

Medios de divulgación

El medio de comunicación por el cual se divulgará este documento será exclusivamente a través del correo electrónico asignado por la propia empresa.

Anexo IX. Procedimiento de Revisión por la Dirección

TRADUX TRADUCCIÓN E INTERPRETACIÓN	PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN	**Código**	SGSI-4
		Versión	1
		Fecha de aprobación	Abril 2024
		Nº páginas	2

Objetivo

El objetivo de este procedimiento es establecer un marco para la revisión periódica del SGSI en TRADUX. Esta revisión tiene como finalidad garantizar la conveniencia, adecuación y eficacia continuas del SGSI.

Alcance

Este anexo se aplica a todos los empleados, directivos y partes interesadas involucradas en la gestión de la seguridad de la información en TRADUX.

Marco normativo

Norma ISO/IEC 27001:2022.

Descripción

La revisión del Sistema de Gestión de Seguridad de la Información (SGSI) es una actividad esencial para garantizar su conveniencia, adecuación y eficacia. Este proceso debe ser llevado a cabo por la dirección de la compañía en colaboración con el Comité de Seguridad.

A continuación, se detallan los aspectos clave de esta revisión anual:

1. Estado de acciones anteriores:

- Se evalúa el progreso de las acciones derivadas de revisiones previas.
- Se analiza cómo han evolucionado desde la última revisión.

2. Cambios en la organización:

- Se consideran modificaciones relevantes que puedan afectar al SGSI, como, por ejemplo, la incorporación de nuevos procesos de negocio o activos.

3. Informes y cumplimiento:

- Se revisan informes sobre no conformidades, acciones correctivas y el cumplimiento con el sistema.

- Se analizan indicadores relacionados con los objetivos de seguridad.
- Se toma en cuenta el resultado de auditorías internas y externas.

4. Apreciaciones del Comité de Seguridad:

- Se recopilan las opiniones y comentarios del Comité.

5. Evolución del plan de tratamiento de riesgos:

- Se verifica el estado del plan de tratamiento de riesgos.

6. Oportunidades de mejora:

- Se identifican áreas donde se puede mejorar el SGSI.

Dado que este proceso es cíclico, el informe de revisión incluirá una sección de conclusiones. Estas conclusiones, estarán, principalmente relacionadas con cambios en el SGSI o posibles mejoras y serán objeto de seguimiento en futuras revisiones. Además, se almacenará una copia firmada por la dirección y los miembros del Comité de Seguridad como evidencia para futuras auditorías.

Medios de divulgación

El medio de comunicación por el cual se divulgará este documento será exclusivamente a través del correo electrónico asignado por la propia empresa.

Anexo X. Gestión de Roles y Responsabilidades

TRADUX TRADUCCIÓN E INTERPRETACIÓN	GESTIÓN DE ROLES Y RESPONSABILIDADES	**Código**	SGSI-5
		Versión	1
		Fecha de aprobación	Abril 2024
		Nº páginas	1

Objetivo

Este anexo tiene como objetivo establecer y comunicar las responsabilidades y autoridades relacionadas con la seguridad de la información en TRADUX, conforme a los requisitos de la norma ISO/IEC 27001:2022.

Alcance

Este anexo se aplica a todos los empleados, directivos y partes interesadas involucradas en la gestión de la seguridad de la información en TRADUX.

Marco normativo

Norma ISO/IEC 27001:2022

Descripción

A continuación, se definen los roles y responsabilidades clave relacionados con la seguridad de la información. Estos roles incluyen, pero no se limitan a:

- Comité de Seguridad: es el responsable de supervisar y revisar el SGSI. Debe asegurarse de que se cumplan los objetivos y políticas de seguridad.

- Responsable de Seguridad de la Información: coordinará y ejecutará las actividades relacionadas con la seguridad. Además, será el punto focal para la gestión de incidentes y la implementación de controles.

- Usuarios y personal: Deben cumplir con las políticas y controles de seguridad establecidos. Reportar cualquier incidente o vulnerabilidad al Responsable de Seguridad de la Información.

Seguimiento y revisión

Se establecerá un mecanismo de seguimiento y revisión periódica de los roles y responsabilidades definidos en este anexo para garantizar su eficacia y relevancia continua.

Medios de divulgación

El medio de comunicación por el cual se divulgará este documento será exclusivamente a través del correo electrónico asignado por la propia empresa.

Anexo XI. Metodología de Gestión de Riesgos

TRADUX TRADUCCIÓN E INTERPRETACIÓN	METODOLOGÍA DE GESTIÓN DE RIESGOS	Código	SGSI-6
		Versión	1
		Fecha de aprobación	Abril 2024
		Nº páginas	3

Objetivo

Establecer y comunicar la metodología para la gestión de riesgos de seguridad de la información en TRADUX, basada en el estándar MAGERIT versión 3.0: Metodología de Análisis y Gestión de los Sistemas de Información y en los requisitos de la norma ISO/IEC 27001:2022.

Alcance

Se aplica a todas las actividades relacionadas con la evaluación de riesgos de seguridad de la información en TRADUX. Cubre la definición de criterios de riesgo, la identificación, análisis y evaluación de riesgos, así como la priorización y tratamiento de estos.

Marco normativo

Norma ISO/IEC 27001:2022 y MAGERIT como referencia para la metodología de gestión de riesgos.

Descripción

La estrategia de TRADUX para gestionar los riesgos de seguridad de la información se fundamenta en MAGERIT la cual es una metodología española para mejorar aspectos organizativos, adaptable internacionalmente. Su tercera versión fue lanzada en 2012. Las herramientas de análisis de riesgos (EAR) la respaldan, financiadas parcialmente por el CCN. MAGERIT se distingue por expresar los riesgos en valores económicos, lo que facilita decisiones fundamentadas y defendibles para la dirección. Sin embargo, esta ventaja se contrarresta con el costo de traducir todas las valoraciones a valores económicos, lo que puede hacer que su aplicación resulte costosa.

Los pasos de la metodología MAGERIT se indican a continuación y se muestran en la Figura 0-6 [23]:

1. Toma de datos y procesos de información: esta fase es crucial para comprender el alcance del análisis de riesgos. Se identifican los procesos críticos de la organización y se delimita el ámbito de estudio. Determinar el nivel de detalle necesario es fundamental, ya que influirá en la cantidad de riesgos que se puedan identificar y analizar.

2. Establecimiento de parámetros: se definen valores económicos para activos, vulnerabilidades, impactos y efectividad de controles de seguridad. Estos parámetros servirán como base para cuantificar los riesgos y tomar decisiones fundamentadas durante todo el proceso de análisis.

3. Análisis de activos: se identifican y clasifican todos los activos de la organización, incluyendo tanto los tangibles (como hardware y software) como los intangibles (como la reputación de la empresa).

Este paso es esencial para entender qué recursos deben protegerse y qué impacto tendría su pérdida o compromiso.

4. Análisis de amenazas: las amenazas potenciales se clasifican en categorías como accidentes, errores y amenazas intencionales. Este análisis ayuda a comprender los diferentes tipos de riesgos a los que se enfrenta la organización, desde desastres naturales hasta ciberataques.

5. Establecimiento de vulnerabilidades: se identifican las debilidades o fallos en la seguridad que podrían ser explotados por las amenazas para causar daños a los activos de la organización. Estas vulnerabilidades se consideran puntos críticos que necesitan ser abordados para reducir el riesgo.

6. Valoración de impactos: se evalúa el posible impacto que tendrían las amenazas sobre los activos de la organización en términos económicos o de otro tipo. Esto ayuda a priorizar qué riesgos deben ser abordados primero y a asignar recursos de manera eficiente.

7. Análisis de riesgos intrínseco: se calcula el riesgo inicial, sin tener en cuenta ninguna medida de seguridad implementada. Esto proporciona una comprensión clara de la exposición de la organización a los riesgos antes de aplicar cualquier control o salvaguarda.

8. Influencia de las salvaguardas: se examina cómo diferentes medidas de seguridad pueden reducir las vulnerabilidades y mitigar los impactos de las amenazas. Esto ayuda a determinar qué controles son más efectivos para proteger los activos de la organización.

9. Análisis de riesgos efectivos: se calcula el riesgo final considerando las medidas de seguridad implementadas. Esto permite evaluar el éxito de las acciones tomadas para mitigar los riesgos y proporciona una visión clara de la situación de seguridad de la organización.

10. Gestión de riesgos: se toman decisiones para reducir, transferir o aceptar los riesgos identificados. Se elabora un plan de acción que incluye la asignación de responsabilidades y la implementación de controles de seguridad adecuados para garantizar la protección de los activos de la organización.

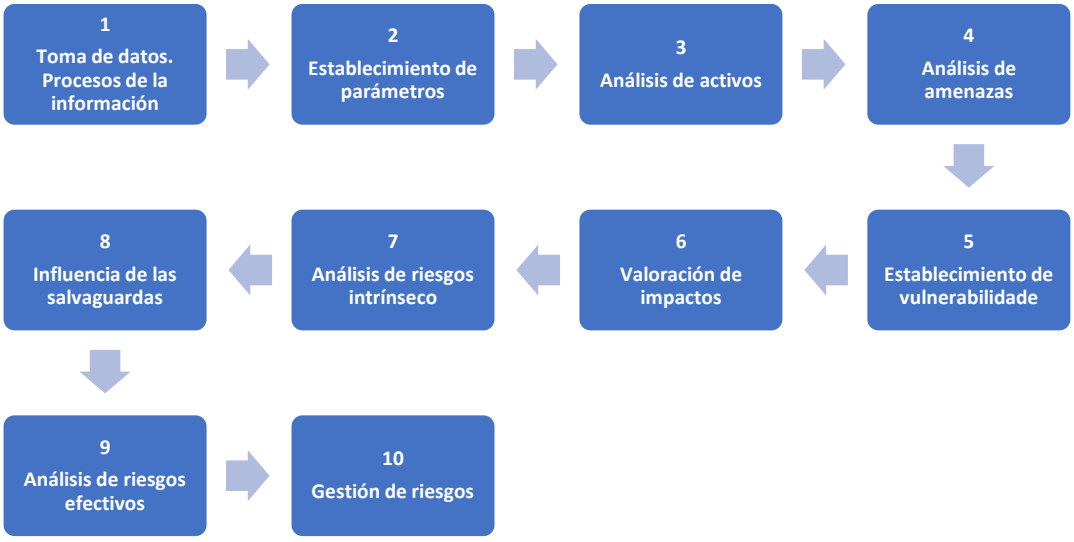

Figura 0-6. Fases de la metodología MAGERIT.
Fuente: Elaboración propia.

Medios de divulgación

El medio de comunicación por el cual se divulgará este documento será exclusivamente a través del correo electrónico asignado por la propia empresa.

Anexo XII. Declaración de Aplicabilidad

TRADUX TRADUCCIÓN E INTERPRETACIÓN	DECLARACIÓN DE APLICABILIDAD	Código	SGSI-7
		Versión	1
		Fecha de aprobación	Abril 2024
		Nº páginas	13

Objetivo

El objetivo de este anexo es establecer y comunicar los controles necesarios para implementar las opciones seleccionadas de tratamiento de riesgos de seguridad de la información en TRADUX, en cumplimiento con los requisitos de la norma ISO/IEC 27001:2022.

Alcance

Este anexo se aplica a todas las actividades relacionadas con la identificación, evaluación y tratamiento de riesgos de seguridad de la información en TRADUX, con el fin de elaborar una Declaración de Aplicabilidad completa y precisa.

Marco normativo

Norma ISO/IEC 27001:2022 y ISO/IEC 27002:2022.

Descripción

La Declaración de Aplicabilidad detalla los controles necesarios para implementar las opciones seleccionadas de tratamiento de riesgos de seguridad de la información en TRADUX. Incluye la identificación de los controles, la justificación de su inclusión, el estado de su implementación y la justificación de cualquier exclusión. Este documento garantiza una comprensión clara de los controles aplicables y su efectividad en la gestión de riesgos de seguridad de la información en TRADUX.

La Tabla 0-14 muestra la valoración de los controles indicados en la ISO 27002, a partir del modelo CMM:

Nº	CONTROL	APLICA (SÍ/NO)	JUSTIFICACIÓN / DESCRIPCIÓN	ESTADO ACTUAL
5	**Controles organizacionales**			
5.1	Políticas para la seguridad de la información	Sí	Control esencial de la norma ISO/IEC 27001. Es necesario que la alta dirección defina una política de seguridad de la información, la cual debe ser divulgada y comunicada de manera efectiva a todos los empleados de la organización.	Existe una política para la seguridad de la información documentada, pero es de muy baja calidad, la organización ha reconocido la necesidad de mejorarla.
5.2	Roles y responsabilidades en seguridad de la información	Sí	Es necesario establecer y asignar claramente las responsabilidades dentro de la organización.	Existe una carencia total de los roles y su asignación y responsabilidades en seguridad de la información.

5.3	Segregación de tareas	Sí	Es imprescindible separar las funciones y responsabilidades para disminuir la posibilidad de que una sola persona o rol tenga la capacidad de comprometer sistemas o información, ya sea de manera accidental o intencionada.	A pesar de que existen esfuerzos iniciales para la segregación de tareas, no hay procedimientos documentados o consistentes.
5.4	Responsabilidades de la dirección	Sí	Es necesario establecer y asignar claramente las responsabilidades de la dirección.	La dirección ha empezado a asumir responsabilidades, pero la falta de comunicación formal y dependencia del conocimiento individual limite la valoración.
5.5	Contacto con las autoridades	Sí	Es fundamental mantener una comunicación constante con las autoridades pertinentes, como las unidades de delitos telemáticos de los cuerpos y fuerzas de seguridad del estado, la AEPD y el INCIBE. Esta comunicación debe abarcar tanto la prevención como la mitigación y respuesta a incidentes, así como facilitar posteriores denuncias e investigaciones.	Existe un reconocimiento de la necesidad de contacto con las autoridades, sin embargo, esta acción no está formalizada y es limitada.
5.6	Contacto con grupos de interés especial	Sí	Es de suma importancia participar activamente en foros o asociaciones relacionadas con la ciberseguridad y privacidad. Esto permite mantener sistemas de información alerta, estar al día en cuanto a las ciberamenazas, así como recibir información sobre nuevas vulnerabilidades y las estrategias para mitigarlas y contenerlas. El intercambio de información juega un papel fundamental en la seguridad de la información.	La organización ha indicado que no se ha establecido contacto, lo que indica una carencia total.
5.7	Inteligencia de amenazas	No	La empresa no está directamente involucrada en la recopilación y análisis de inteligencia de amenazas.	
5.8	Seguridad de la información en la gestión de proyectos	Sí	La seguridad de la información en la gestión de proyectos es relevante para la empresa, ya que garantiza la protección de la información confidencial de los clientes durante la ejecución de proyectos de traducción e interpretación.	Existe un sistema de seguridad en la gestión de proyectos, pero se reconocen áreas de mejora para fortalecer la protección de la información.
5.9	Inventario de información y otros activos asociados	Sí	Es imprescindible mantener un inventario actualizado de activos. Todo sistema de gestión de riesgos se fundamenta en tres pilares fundamentales: activos, amenazas y vulnerabilidades. Este inventario de activos proporciona una base sólida para identificar y evaluar los riesgos asociados con los sistemas de información y otros recursos críticos de la organización.	Aunque la empresa tiene conocimiento de sus equipos, no ha realizado un inventario detallado de activos ni un análisis de riesgos. Se carece de una documentación adecuada de los activos y recursos críticos de la organización.
5.10	Uso aceptable de la información y otros activos asociados	Sí	Es esencial establecer normas, procedimientos y reglas claras para el uso de los activos y recursos relacionados con el tratamiento de la información. Estas directrices proporcionan un marco para garantizar el uso adecuado, seguro y	Aun reconociendo la importancia de establecer normas, procedimientos y reglas claras, actualmente no existe una política formalizada ni comunicada para el uso

			eficiente de los activos de la organización, lo que contribuye a proteger la confidencialidad, integridad y disponibilidad de la información.	adecuado de los activos de la organización.
5.11	Devolución de activos	Sí	Es necesario establecer el protocolo para la devolución de los activos una vez finalizada la relación contractual, tanto con empleados como con terceros. Todos los activos en posesión de la persona u organización deben ser devueltos de manera oportuna y completa. Esto garantiza que los recursos de la organización no sean utilizados indebidamente y contribuye a mantener la seguridad y el control sobre los activos de la empresa.	A pesar de que existen medidas de devolución de los activos, no están formalizadas.
5.12	Clasificación de la información	Sí	Es fundamental clasificar la información en función de su importancia con respecto a la divulgación frente a requisitos legales, su valor, sensibilidad y criticidad frente a revelaciones o modificaciones no autorizadas. Esta clasificación ayuda a priorizar y aplicar medidas de seguridad adecuadas según el nivel de riesgo asociado con cada tipo de información, asegurando así su protección y manejo adecuado.	La organización ha empezado a clasificar la información, pero sin procedimientos formales.
5.13	Etiquetado de la información	Sí	Una vez que la información ha sido clasificada, es necesario etiquetarla según su valor o relevancia. Esta etiquetación facilita la identificación rápida y precisa de la información, asegurando que se apliquen las medidas de seguridad correspondientes de acuerdo con su importancia y sensibilidad.	Existe un etiquetado inicial de la información, pero no está estandarizado.
5.14	Transferencia de la información	Sí	La empresa maneja información sensible de clientes durante los procesos de traducción e interpretación, por lo que es crucial asegurar la seguridad durante la transferencia de esta información.	No existen controles para la transferencia de la información.
5.15	Control de acceso	Sí	Es esencial establecer, documentar y revisar una política de control de acceso que esté basada en los requisitos de negocio y de seguridad de la información. Esta política debe abordar el acceso a servidores, equipos, bases de datos, instalaciones, información y otros recursos críticos de la organización. Al hacerlo, se establece un marco claro para gestionar y controlar quién tiene acceso a qué recursos, lo que contribuye a proteger la confidencialidad, integridad y disponibilidad de la información, así como a cumplir con los objetivos y necesidades del negocio.	Existe un control de acceso implementado de manera ad hoc.
5.16	Gestión de la identidad	Sí	La gestión de la identidad es fundamental para garantizar que solo el personal autorizado de la empresa tenga acceso a los sistemas y datos relevantes para llevar a	Existe una carencia total en la gestión de identidades.

			cabo los servicios de traducción e interpretación.	
5.17	Información de autenticación	Sí	Dado que se emplea de usuario/contraseña para acceder a los sistemas, la asignación de información de autenticación confidencial debe estar sujeta a un procedimiento de gestión formal.	Se han tomado medidas iniciales para manejar la información de autenticación.
5.18	Derechos de acceso	Sí	Es importante realizar revisiones periódicas de los derechos de acceso a los sistemas para prevenir la presencia de usuarios activos cuya baja no se ha comunicado, cambios en roles, acceso de usuarios desconocidos, entre otros posibles escenarios.	Los derechos de acceso están definidos, sin embargo, carecen de un proceso formal.
5.19	Seguridad de la información en las relaciones con proveedores	Sí	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.	Los procesos se encuentran parcialmente establecidos.
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	Sí	Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de Tecnología de la Información. Este principio se aplica porque la organización colabora con terceros que gestionan información de manera independiente.	La organización ha reconocido la necesidad, pero no posee acciones formalizadas.
5.21	Gestión de información de la información la cadena de suministro TIC	Sí	Los acuerdos con los proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones, así como con la cadena de suministro de productos. Esto implica que los riesgos para la seguridad de la información también se ven influenciados por las actividades de subcontratación de nuestros proveedores. Por lo tanto, es crucial exigir proveedores de confianza y requerir que implementen controles de seguridad para sus propios proveedores.	Existen esfuerzos iniciales para la gestión de información de la información la cadena de suministro TIC, pero no están estandarizados.
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	Sí	La empresa tiene una dependencia crítica del proveedor externo para la licencia del programa de traducción, lo que impacta la calidad del servicio y la gestión de riesgos y cumplimiento.	Existe un seguimiento y revisión ad hoc de los servicios de proveedores.
5.23	Seguridad de la información para el uso de servicios en la nube	Sí	Se utilizan servicios en la nube para almacenar o procesar información de clientes, es necesario implementar controles de seguridad de la información para garantizar la protección adecuada de los datos.	Existen medidas iniciales para la seguridad de la información en la nube, pero no hay ningún enfoque formal.
5.24	Planificación y preparación para la gestión de	Sí	La planificación de incidentes de seguridad se aplica para garantizar respuestas efectivas, coordinación con servicios	Existe un plan de gestión de incidentes de seguridad, sin embargo, su implementación y

	incidentes de seguridad de información		externos y optimización de recursos ante posibles amenazas, asegurando la continuidad del negocio.	coordinación con servicios externos no están formalizadas, lo que podría afectar la capacidad de la empresa para responder de manera efectiva ante amenazas de seguridad.
5.25	Evaluación y decisión sobre los eventos de seguridad de la información	Sí	Esta responsabilidad recae en el trabajador externo, quien posee la expertise y los recursos necesarios para llevar a cabo evaluaciones efectivas y tomar decisiones rápidas y adecuadas en relación con los eventos de seguridad de la información.	A pesar de que se cuenta con un trabajador externo responsable de la evaluación y toma de decisiones sobre eventos de seguridad, no se han establecido procesos formales ni se realiza una evaluación continua de su desempeño, lo que podría comprometer la capacidad de respuesta de la empresa ante incidentes de seguridad.
5.26	Respuesta a incidentes de seguridad de la información	Sí	El trabajador externo es el encargado de la respuesta a incidentes de seguridad, lo que asegura una gestión rápida y eficiente de cualquier incidente que pueda surgir, minimizando así el impacto en la empresa.	Aunque se ha designado un trabajador externo para la respuesta a incidentes de seguridad, no se han establecido procedimientos formales ni se realizan revisiones post-incidentes para identificar áreas de mejora en la respuesta, lo que limita la capacidad de la empresa para gestionar eficazmente los incidentes de seguridad.
5.27	Aprender de los incidentes de seguridad de la información	Sí	Aunque la empresa no tiene un proceso interno para aprender de los incidentes de seguridad, su trabajador externo tiene mecanismos para mejorar continuamente sus prácticas de seguridad, lo que garantiza que se aprovechen las lecciones aprendidas de manera efectiva.	No se ha implementado un proceso formal para aprender de los incidentes de seguridad, lo que dificulta la maximización del aprendizaje y la mejora continua de las prácticas de seguridad de la empresa.
5.28	Recopilación de evidencias	No	El objetivo primario en caso de incidentes de seguridad es la recuperación de la capacidad operativa, por lo que la recopilación de evidencias no es una prioridad inmediata.	
5.29	Seguridad de la información durante la interrupción	Sí	Garantizar la seguridad de los datos en caso de interrupción, por ejemplo, ante un ataque ransomware, donde se busca prevenir el acceso no autorizado a los datos durante períodos críticos.	Se reconoce la importancia de garantizar la seguridad de los datos durante una interrupción, no se han realizado ejercicios de recuperación ante desastres para mejorar la resiliencia de la empresa, lo que la deja vulnerable ante posibles amenazas.
5.30	Preparación de las TIC para la continuidad del negocio	No	Las estrategias de continuidad de negocio no necesariamente requieren una infraestructura de tecnologías de la información redundante, especialmente cuando las operaciones de TI están externalizadas, ya que existe un empleado externo.	

5.31	Identificación de requisitos legales, reglamentarios y contractuales	Sí	Todos los requisitos legales, regulatorios o contractuales, y el enfoque de la organización para cumplirlos, deben ser definidos de manera explícita, documentados y mantenidos actualizados para cada sistema de información de la organización. Esto garantiza una comprensión clara de las obligaciones y responsabilidades de la organización en materia de seguridad de la información, así como la capacidad de adaptarse a los cambios en el entorno normativo y empresarial.	Se reconoce la importancia de identificar y mantener actualizados los requisitos legales, regulatorios y contractuales, actualmente no se lleva a cabo un seguimiento adecuado de los cambios normativos, lo que podría afectar el cumplimiento continuo de la empresa.
5.32	Derechos de propiedad intelectual (DPI)	Sí	Implementar procedimientos para cumplir requisitos legales sobre propiedad intelectual y software. Evitar uso no autorizado y asegurar protección adecuada de activos organizacionales dentro de la ley.	A pesar de que existen esfuerzos para proteger el DPI, estos no están formalizados.
5.33	Protección de los registros	Sí	Los registros deben protegerse contra pérdida, destrucción, falsificación, o acceso no autorizado, cumpliendo requisitos legales y regulatorios, como el RGPD, garantizando la integridad y confidencialidad de la información.	Se protegen los registros, pero no existen políticas ni procedimientos estandarizados.
5.34	Privacidad y protección de datos de carácter personal (DCP)	Sí	La empresa debe cumplir con las regulaciones de privacidad y protección de datos de carácter personal para garantizar la confidencialidad y el tratamiento adecuado de los datos de sus clientes.	Se toman medidas para la protección de los datos de carácter personal, pero sin un enfoque sistemático.
5.35	Revisión independiente de la seguridad de la información	Sí	Es fundamental someter los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información a una revisión independiente en intervalos planificados o cuando se produzcan cambios significativos en la implementación de la seguridad. Esta revisión independiente es crucial para garantizar la mejora continua y debe ser llevada a cabo por personas que sean independientes del área que se está revisando. Esto ayuda a identificar posibles deficiencias, riesgos o áreas de mejora, asegurando así la eficacia y eficiencia del sistema de seguridad de la información.	Se hacen revisiones independientes, pero estas son de manera inconsciente.
5.36	Conformidad con las políticas, reglas y estándares de seguridad de la información	Sí	Es responsabilidad de la dirección garantizar que todos los procedimientos de seguridad dentro de su área de responsabilidad se lleven a cabo correctamente para cumplir con las políticas, normas y cualquier otro requisito de seguridad aplicable. Esto es crucial para establecer y mantener un SGSI efectivo, que proporcione un marco sólido para proteger la confidencialidad, integridad y disponibilidad de la información de la organización.	Existe un reconocimiento de las políticas, pero sin seguimiento adecuado.

5.37	Documentación de procedimientos operacionales	Sí	Es esencial realizar verificaciones periódicas para asegurar que los sistemas de información cumplan con las políticas y normas de seguridad de la información de la organización. Esto garantiza que los sistemas estén alineados con los estándares establecidos y que se mantenga un nivel adecuado de seguridad para proteger la información sensible y los activos de la organización.	Los procedimientos operacionales están documentados, sin embargo, no se revisan ni actualizan de manera periódica.
6	**Personas**			
6.1	Comprobación	Sí	Es fundamental realizar una investigación exhaustiva o recopilar información sobre la idoneidad de los perfiles para asumir responsabilidades y funciones en el ámbito de la ciberseguridad y privacidad. Esto implica evaluar su formación, experiencia, habilidades personales y cualquier otro criterio relevante para garantizar que estén debidamente calificados y preparados para desempeñar dichas responsabilidades de manera efectiva.	Se realizan comprobaciones de los antecedentes de las personas, sin embargo, la metodología no está estandarizada completamente.
6.2	Términos y condiciones de contratación	Sí	Es necesario que todos los trabajadores acepten ciertas obligaciones en el momento de su contratación en relación con la privacidad y la seguridad de la información. Es crucial asegurar que los trabajadores cumplan con las políticas establecidas relacionadas con la seguridad de la información. Esto garantiza un ambiente laboral seguro y protege la confidencialidad, integridad y disponibilidad de los datos de la organización.	A pesar de que los términos y condiciones estén establecidos, su aplicación puede ser inconsistente.
6.3	Concienciación, educación y formación en seguridad de la información	Sí	La formación y la concienciación desempeñan un papel fundamental en la promoción de una cultura de seguridad de la información sólida en cualquier SGSI. Por ello, es crucial exigir y ofrecer formación tanto a empleados como a terceros cuando sea necesario. Esto garantiza que todos estén adecuadamente informados sobre las mejores prácticas de seguridad, los procedimientos y las políticas relevantes, lo que contribuye a fortalecer la postura de seguridad de la organización y a mitigar los riesgos asociados con la seguridad de la información.	Existen programas de formación, pero no están plenamente integrados en la cultura de la organización.
6.4	Proceso disciplinario	Sí	Es necesario establecer y comunicar de manera clara un proceso disciplinario formal en caso de incidentes de ciberseguridad cuando sea necesario. Esto asegura una respuesta adecuada y consistente ante posibles violaciones de la seguridad de la información, así como promueve la responsabilidad y la conciencia de seguridad entre los empleados.	Existe el proceso disciplinario, pero no se aplica uniformemente ni de forma efectiva.

6.5	Responsabilidades ante la finalización o cambio	Sí	Es crucial que, aunque la relación contractual haya terminado, ya sea con un empleado o un tercero que haya prestado un servicio, las responsabilidades y obligaciones establecidas en el Acuerdo de No Divulgación (NDA) se mantengan vigentes. Esto asegura la confidencialidad y protección de la información sensible de la organización incluso después de que la relación laboral o comercial haya finalizado. Es importante ajustarse a los plazos legales pertinentes y considerar la relevancia de la información para la organización al mantener estas responsabilidades y obligaciones.	Existe conciencia de la importancia de las responsabilidades ante la finalización o cambio de empleo, sin embargo, las acciones no están formalizadas.
6.6	Acuerdos de confidencialidad o no divulgación	Sí	Es fundamental identificar, documentar y revisar regularmente los requisitos de los acuerdos de confidencialidad o no divulgación. Esta práctica no solo es una buena medida de seguridad, sino que también es obligatoria por ley, según el Reglamento General de Protección de Datos (RGPD). Garantizar el cumplimiento de estos requisitos ayuda a proteger la información sensible y a mantener la confidencialidad de los datos de la organización, así como a cumplir con las obligaciones legales en materia de protección de datos.	Los acuerdos de confidencialidad están parcialmente implementados, aunque pueden carecer de seguimiento y aplicación formal.
6.7	Teletrabajo	Sí	Los empleados trabajan en la oficina o desde sus domicilios, por ello, se debe implementar una política y medidas de seguridad adecuadas para proteger la información. Estas medidas deben asegurar la confidencialidad, integridad y disponibilidad de los datos. Además, es fundamental evaluar todos los riesgos asociados a este modelo de trabajo remoto para garantizar una gestión efectiva de la seguridad de la información.	Existen políticas de teletrabajo, pero la supervisión y el control de su cumplimiento son incompletos.
6.8	Notificación de eventos de seguridad de la información	Sí	La empresa debe notificar eventos de seguridad de la información a las partes interesadas pertinentes, incluidos los clientes y las autoridades reguladoras, según sea necesario.	Se reconocen los eventos de seguridad de la información, pero no existe un proceso estandarizado para su notificación.
7	**Infraestructura**			
7.1	Perímetro de seguridad física	Sí	La empresa tiene la gestión del control sobre el perímetro de seguridad física debido a que la infraestructura está gestionada por un proveedor, ya que las oficinas están alquiladas. Esto implica que la empresa tiene la responsabilidad de garantizar la seguridad del perímetro físico de las instalaciones alquiladas.	Se tiene el control del perímetro de seguridad física, la falta de controles de acceso adecuados y registros de visitantes deja a la empresa vulnerable a posibles intrusiones no autorizadas, lo que requiere una mejora en la vigilancia y seguridad del perímetro físico.
7.2	Controles físicos de entrada	Sí	La gestión de controles físicos de entrada está a cargo del proveedor externo de la infraestructura, que se encarga de	Aunque se cuenta con controles físicos de entrada, la falta de revisiones regulares de la eficacia

			implementar y mantener los sistemas de acceso físico y de asegurar que solo personal autorizado pueda ingresar a las instalaciones, puesto que las oficinas son de alquiler.	de estos controles puede comprometer la seguridad de las instalaciones, lo que requiere una mejora en la evaluación y el mantenimiento de los controles de acceso físico implementados.
7.3	Seguridad de oficinas, despachos y recursos	Sí	La gestión de la seguridad de las oficinas y recursos está externalizada, lo que significa que el proveedor externo de la infraestructura se encarga de garantizar la seguridad de los espacios de trabajo y los recursos físicos de la empresa.	La gestión de la seguridad de las oficinas y recursos está externalizada, la falta de auditorías periódicas de seguridad física puede dejar a la empresa expuesta a vulnerabilidades, por lo que se requiere una mejora en la realización de auditorías para identificar posibles mejoras.
7.4	Monitorización de la seguridad física	Sí	La monitorización de la seguridad física está externalizada por el proveedor externo de la infraestructura, que ofrece servicios de monitorización y vigilancia para garantizar la protección continua de las instalaciones físicas contra amenazas de seguridad.	Se cuenta con un servicio de monitorización de la seguridad física, la falta de sistemas avanzados de monitorización puede limitar la detección de amenazas, por lo que se requiere una mejora en la implementación de sistemas de monitorización avanzados para mejorar la detección de amenazas.
7.5	Protección contra las amenazas externas y ambientales	Sí	La empresa debe garantizar que sus servicios de traducción e interpretación no se vean afectados por amenazas externas o ambientales que podrían comprometer la seguridad de la información.	Aunque se han implementado medidas contra amenazas externas y ambientales, no se han implementado de manera sistemática.
7.6	Trabajo en áreas seguras	Sí	La empresa debe garantizar que los empleados trabajen en entornos seguros para proteger la confidencialidad de la información de los clientes.	Existen medidas implementadas para trabajar en áreas seguras, sin embargo, pueden no estar integradas en la operación diaria.
7.7	Puesto de trabajo despejado y pantalla limpia	Sí	Es recomendable implementar una política de mantener los puestos de trabajo libres de papeles y dispositivos de almacenamiento extraíbles, así como una política de mantener las pantallas limpias en los recursos utilizados para el procesamiento de la información.	No existen políticas o prácticas para mantener los puestos de trabajo despejados y las pantallas limpias.
7.8	Emplazamiento y protección de equipos	Sí	La responsabilidad del emplazamiento y la protección de equipos está externalizada y es gestionada por el trabajador externo, quien garantiza la seguridad física de los equipos y recursos de la empresa.	Se cuenta con la responsabilidad externalizada del emplazamiento y la protección de equipos, la falta de auditorías regulares de seguridad de los equipos puede dejar a la empresa expuesta a riesgos, por lo que se requiere una mejora en la realización de auditorías de seguridad de los equipos.

7.9	Seguridad de los equipos fuera de las instalaciones	Sí	La empresa debe asegurar la seguridad de los equipos utilizados fuera de las instalaciones para proteger la información del cliente.	Existen políticas para la seguridad de los equipos fuera de las instalaciones, aunque la aplicación y el seguimiento de estas políticas pueden ser inconsistentes.
7.10	Soportes de almacenamiento	Sí	La empresa debe garantizar la seguridad de los soportes de almacenamiento utilizados para almacenar datos de clientes.	La organización ha reconocido de la necesidad de proteger los soportes de almacenamiento, pero las acciones son limitadas y no están formalizadas.
7.11	Instalaciones de suministro	Sí	Dado que las oficinas son de alquiler, se asegura la continuidad de los servicios esenciales para las operaciones de la empresa.	Se asegura la continuidad de los servicios esenciales, la falta de una comunicación fluida con el proveedor de servicios puede afectar la capacidad de la empresa para garantizar la continuidad de las operaciones, por lo que se requiere una mejora en la comunicación con el proveedor de servicios.
7.12	Seguridad del cableado	Sí	Dado que las oficinas son de alquiler, se asegura la continuidad de los servicios esenciales para las operaciones de la empresa.	Se asegura la continuidad de los servicios esenciales, la falta de revisiones regulares del cableado puede dejar a la empresa vulnerable a fallos de seguridad, por lo que se requiere una mejora en la realización de revisiones regulares del cableado.
7.13	Mantenimiento de los equipos	Sí	Los ordenadores de oficina y los ordenadores para el teletrabajo deben someterse a un mantenimiento adecuado con el objetivo de garantizar su disponibilidad e integridad continua.	Existe y se realiza mantenimiento de los equipos, pero los procedimientos podrían no estar estandarizados ni ser consistentes.
7.14	Eliminación o reutilización segura de equipos	Sí	Es imprescindible realizar una verificación en todos los medios de almacenamiento para asegurar que cualquier dato sensible y software bajo licencia se haya eliminado de manera segura antes de desecharlos.	Aunque existen procesos para la eliminación o reutilización segura de equipos, pero podrían mejorar en cuanto a seguimiento y verificación.
8	**Tecnología**			
8.1	Dispositivos de punto final de los usuarios	Sí	Los dispositivos utilizados por los usuarios, tanto los ordenadores de la oficina como los ordenadores para el teletrabajo, pueden ser vulnerables a amenazas de seguridad. Por ello, es fundamental implementar controles para proteger estos dispositivos y los datos que contienen.	Se han tomado medidas para asegurar los dispositivos de punto final de los usuarios, sin embargo, la consistencia y la cobertura pueden estar incompletas.
8.2	Gestión de privilegios de acceso	Sí		A pesar de que los privilegios están gestionados, la supervisión y el control podrían mejorar.
8.3	Restricción del acceso a la información	Sí	Limitar el acceso a la información a los usuarios autorizados es crucial para proteger la confidencialidad y la integridad de los	Existe conciencia sobre la necesidad de restringir el acceso,

			datos de los clientes que la empresa maneja en los procesos de negocio.	aunque las acciones no están formalizadas y son limitadas.
8.4	Acceso al código fuente	No	La empresa no se dedica al desarrollo de software, por ello, el acceso al código fuente no es relevante para sus operaciones de traducción e interpretación y facturación de sus servicios.	
8.5	Autenticación segura	Sí	Se asegurará la autenticación segura mediante el fortalecimiento de los mecanismos de autenticación, como la autenticación multifactorial, el control de contraseñas y la gestión de credenciales.	Existen esfuerzos para implementar la autenticación segura, aunque no están completamente desarrollados.
8.6	Gestión de capacidades	Sí	Se debe establecer una metodología coherente y consistente para la gestión de capacidades, garantizando la alineación con los objetivos del negocio y la optimización de recursos.	Las capacidades están gestionadas, sin embargo, la metodología y la aplicación pueden ser inconsistentes
8.7	Protección contra el código dañino	Sí	Se debe mejorar la implementación de medidas contra el código dañino mediante la implementación de soluciones antivirus/antimalware actualizados y la educación de los usuarios sobre las prácticas seguras de navegación y descarga de software.	Se han implementado medidas contra el código dañino, pero no de manera sistemática.
8.8	Gestión de las vulnerabilidades técnicas	Sí	Es necesario implementar un proceso formal para la gestión de vulnerabilidades técnicas, que incluya la identificación, evaluación, mitigación y seguimiento de las vulnerabilidades en los sistemas de información de la organización.	Existe un reconocimiento de las vulnerabilidades técnicas, aunque la gestión es ad hoc.
8.9	Gestión de la configuración	Sí	Se debe mejorar la documentación y la gestión de cambios en el proceso de gestión de configuración, asegurando la consistencia y la trazabilidad de los cambios realizados en los sistemas y activos de la organización.	Existe una gestión de la configuración, pero puede haber carencias en la documentación y en la gestión de cambio.
8.10	Eliminación de la información	Sí	Es necesario establecer procedimientos estandarizados para la eliminación segura de la información, incluyendo la implementación de métodos de borrado seguro y la documentación de las actividades de eliminación.	Se eliminan los datos de manera segura, sin embargo, los procedimientos no están estandarizados.
8.11	Enmascaramiento de datos	Sí	Se debe formalizar y estandarizar los procesos de enmascaramiento de datos, asegurando la consistencia y la efectividad en la protección de datos sensibles en entornos no productivos.	Se toman medidas para el enmascaramiento de datos, pero no están formalizadas.
8.12	Prevención de la fuga de datos	Sí	La prevención de la fuga de datos es esencial para proteger la información confidencial de los clientes y así garantizar el cumplimiento de las regulaciones de privacidad.	Se reconocen los riesgos de fuga de datos, pero no hay un enfoque para su prevención.
8.13	Copia de seguridad de la información	Sí	Realizar copias de seguridad de la información es crítico para garantizar la disponibilidad y la integridad de los datos de	Aunque se realizan copias de seguridad, pero no hay un

			los clientes que la empresa maneja en sus procesos de negocio.	proceso formal de restauración ni verificación.
8.14	Redundancia recursos de tratamiento de la información	Sí	Ayudar a garantizar la disponibilidad continua de los servicios, lo cual resulta fundamental para mantener la satisfacción del cliente y el cumplimiento de los compromisos contractuales.	Existe la redundancia de recursos, aunque la planificación y el mantenimiento podrían no ser óptimos.
8.15	Registros de eventos	No	No se lleva a cabo una recopilación de eventos, por lo que no se generan registros de eventos que requieran seguimiento.	
8.16	Seguimiento de actividades	No	No se está realizando un seguimiento de actividades específicas que requiera documentación o supervisión.	
8.17	Sincronización del reloj	Sí	Es fundamental que todos los sistemas estén sincronizados con el mismo servicio de tiempo para poder trazar y correlacionar todas las operaciones que se ejecuten en los diferentes sistemas. Esto asegura que se pueda mantener un registro preciso de la hora en que se realizan las acciones y eventos en toda la infraestructura, lo que facilita la detección y análisis de incidentes de seguridad, así como la generación de registros de auditoría precisos y confiables.	La empresa reconoce la importancia de la sincronización del reloj, la falta de implementación de un sistema de sincronización automática puede afectar la precisión de los registros y la detección de incidentes de seguridad, por lo que se requiere una mejora en la implementación de un sistema de sincronización automática.
8.18	Uso de programas de utilidad con privilegios	Sí	Se debe limitar y supervisar de manera estricta el uso de herramientas que podrían evadir los controles del sistema.	Se reconoce la importancia de limitar y supervisar el uso de herramientas con privilegios, la falta de una política formal puede dejar a la empresa expuesta a riesgos de seguridad, por lo que se requiere una mejora en la implementación de una política de acceso a herramientas de utilidad basada en privilegios.
8.19	Instalación de software en sistemas en producción	Sí	El informático interno se encarga de gestionar y controlar la instalación de software en los sistemas en producción para garantizar que solo se instalen aplicaciones autorizadas y seguras, lo que contribuye a mantener la integridad y la seguridad de los sistemas de información de la empresa.	Se cuenta con un informático interno para gestionar la instalación de software, la falta de procesos formales de revisión y aprobación puede dejar a la empresa vulnerable a la instalación de aplicaciones no autorizadas, por lo que se requiere una mejora en la implementación de procesos de revisión y aprobación de instalaciones de software.
8.20	Seguridad de redes	Sí	Garantizar la seguridad de las redes es esencial para proteger la confidencialidad e integridad de la información transmitida a través de las redes utilizadas en los procesos de negocio de la empresa.	Las redes se encuentran protegidas en un nivel básico, sin embargo, falta una gestión integral y sistemática.
8.21	Seguridad de los servicios de red	Sí	La seguridad de los servicios de red es fundamental para proteger los servicios	Los servicios de red tienen medidas de seguridad, aunque

			críticos de la empresa contra amenazas como el acceso no autorizado y el malware.	podrían mejorar respecto a la cobertura y la consistencia.
8.22	Segregación de redes	Sí	La segregación de redes ayuda a limitar la exposición de los sistemas de la empresa a posibles amenazas al restringir el acceso a segmentos de red específicos según las necesidades y los niveles de seguridad requeridos.	Existe segregación de redes, pero la implementación no es completa ni está plenamente verificada.
8.23	Filtrado webs	Sí	Implementar filtrado web ayuda a la empresa a controlar y proteger el acceso a los sitios web potencialmente maliciosos o inseguros, reduciendo de esta manera, el riesgo de ataques de malware y phishing.	El filtrado web está altamente implementado y gestionado.
8.24	Uso de la criptografía	Sí	El informático interno se encarga del uso de la criptografía, especialmente en aplicaciones como Office (Outlook), lo que asegura la confidencialidad y la integridad de la información sensible de la empresa.	Se cuenta con un informático interno para gestionar el uso de la criptografía, la falta de auditorías periódicas de configuración puede dejar a la empresa vulnerable a vulnerabilidades de seguridad, por lo que se requiere una mejora en la realización de auditorías periódicas de configuración de criptografía.
8.25	Seguridad en el ciclo de vida de desarrollo	No	La empresa no participa en el desarrollo de software ni en el ciclo de vida de desarrollo de aplicaciones ya que no es una operación que realice esta empresa.	
8.26	Requisitos de seguridad de las aplicaciones	No	La empresa no desarrolla ni mantiene aplicaciones propias, sino que se centra en servicios de traducción e interpretación, por tanto, no existen requisitos de seguridad de aplicaciones específicos que deban ser abordados, estas son responsabilidad del proveedor.	
8.27	Arquitectura segura de sistemas y principios de ingeniería	No	La arquitectura segura de sistemas y los principios de ingeniería de seguridad están fuera del alcance de las operaciones y la arquitectura está descentralizada.	
8.28	Codificación segura	No	La empresa no está involucrada en operaciones de por lo que no hay necesidad de implementar controles relacionados con la codificación segura.	
8.29	Pruebas de seguridad en desarrollo y la aceptación	No	La empresa no es responsable del desarrollo de software, por tanto, no se llevan a cabo pruebas de seguridad en el desarrollo ni en la fase de aceptación.	
8.30	Externalización del desarrollo	No	No se realizan actividades de desarrollo de software internamente. En lugar de eso, se externaliza al proveedor quien proporciona licencias del programa de traducción utilizado en los procesos.	

8.31	Separación de los entornos de desarrollo, prueba y producción	No	La gestión y el mantenimiento del programa de traducción se externalizan a una empresa proveedora que proporciona licencias. Por lo tanto, la empresa no opera ni mantiene entornos de desarrollo, prueba y producción en su infraestructura interna.	
8.32	Gestión de cambios	No	Debido a que la gestión del programa de traducción y las licencias asociadas son responsabilidad de una empresa externa contratada para este fin. Por lo tanto, la empresa no tiene autoridad directa sobre los cambios en el software y su gestión está cubierta por el acuerdo con el proveedor externo.	
8.33	Datos de pruebas	No	La empresa se dedica a la traducción e interpretación y no desarrolla software internamente, por lo que no se espera que maneje datos de pruebas en este contexto.	
8.34	Protección de los sistemas de información durante las pruebas de auditoría	No	La empresa no desarrolla software internamente por lo que no se espera que se realice este control.	

Tabla 0-14. Declaración de Aplicabilidad
Fuente: Elaboración propia

Medios de divulgación

El medio de comunicación por el cual se divulgará este documento será exclusivamente a través del correo electrónico asignado por la propia empresa.

Anexo XIII. Riesgo actual

IDENTIFICADOR	NOMBRE DEL ACTIVO	CATEGORÍA DEL ACTIVO	PROPIETARIO DEL ACTIVO	AMENAZA	VULNERABILIDAD	PROPIETARIO DEL RIESGO	VALOR ACTIVO	FRECUENCIA DE LA AMENAZA ACTUAL	IMPACTO DE LA AMENAZA ACTUAL	NIVEL RIESGO ACTUAL
RSK-001	Información financiera	Datos	Jefe Administrativo y Financiero	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Jefe Administrativo y Financiero	5	3	4	**60**
RSK-002	Información financiera	Datos	Jefe Administrativo y Financiero	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Jefe Administrativo y Financiero	5	2	5	**50**
RSK-003	Información financiera	Datos	Jefe Administrativo y Financiero	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Jefe Administrativo y Financiero	5	2	5	**50**
RSK-004	Información financiera	Datos	Jefe Administrativo y Financiero	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Jefe Administrativo y Financiero	5	2	4	**40**
RSK-005	Información financiera	Datos	Jefe Administrativo y Financiero	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de la misma, ya sea por acciones maliciosas o accidentales.	Jefe Administrativo y Financiero	5	2	5	**50**
RSK-006	Información financiera	Datos	Jefe Administrativo y Financiero	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Jefe Administrativo y Financiero	5	2	4	**40**
RSK-007	Propiedad intelectual	Datos	Director Ejecutivo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Director Ejecutivo	4	3	4	**48**
RSK-008	Propiedad intelectual	Datos	Director Ejecutivo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Director Ejecutivo	4	2	5	**40**

RSK-009	Propiedad intelectual	Datos	Director Ejecutivo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Director Ejecutivo	4	2	4	**32**
RSK-010	Propiedad intelectual	Datos	Director Ejecutivo	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Director Ejecutivo	4	2	4	**32**
RSK-011	Propiedad intelectual	Datos	Director Ejecutivo	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida, ya sea por acciones maliciosas o accidentales.	Director Ejecutivo	4	2	5	**40**
RSK-012	Propiedad intelectual	Datos	Director Ejecutivo	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Director Ejecutivo	4	2	4	**32**
RSK-013	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	3	4	**48**
RSK-014	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	2	5	**40**
RSK-015	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	2	4	**32**

RSK-016	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	2	4	**32**
RSK-017	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de la misma, ya sea por acciones maliciosas o accidentales.	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	2	5	**40**
RSK-018	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	2	4	**32**
RSK-019	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	3	4	**60**
RSK-020	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	5	**50**
RSK-021	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	5	**50**

RSK-022	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	4	**40**
RSK-023	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de la misma, ya sea por acciones maliciosas o accidentales.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	5	**50**
RSK-024	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	4	**40**
RSK-025	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Jefes de Proyectos de Traducción e Interpretación	5	3	4	**60**
RSK-026	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Jefes de Proyectos de Traducción e Interpretación	5	2	5	**50**
RSK-027	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Jefes de Proyectos de Traducción e Interpretación	5	2	5	**50**
RSK-028	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Jefes de Proyectos de Traducción e Interpretación	5	2	4	**40**

RSK-029	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de la misma, ya sea por acciones maliciosas o accidentales.	Jefes de Proyectos de Traducción e Interpretación	5	2	5	**50**
RSK-030	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Jefes de Proyectos de Traducción e Interpretación	5	2	4	**40**
RSK-031	Información de acceso de las visitas	Datos	Dpto. TI	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Dpto. TI	2	3	4	**24**
RSK-032	Información de acceso de las visitas	Datos	Dpto. TI	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Dpto. TI	2	2	5	**20**
RSK-033	Información de acceso de las visitas	Datos	Dpto. TI	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Dpto. TI	2	2	3	**12**
RSK-034	Información de acceso de las visitas	Datos	Dpto. TI	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Dpto. TI	2	2	4	**16**
RSK-035	Información de acceso de las visitas	Datos	Dpto. TI	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de la misma, ya sea por acciones maliciosas o accidentales.	Dpto. TI	2	2	5	**20**
RSK-036	Información de acceso de las visitas	Datos	Dpto. TI	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Dpto. TI	2	2	4	**16**
RSK-037	Proveedor informático	Proveedor	Jefe de Tecnologías de la Información	[I.9] Interrupción de otros servicios y suministros esenciales (D)	Un proveedor de servicios de infraestructura experimenta una interrupción no planificada, lo que afecta negativamente a los servicios críticos de la empresa.	Jefe de Tecnologías de la Información	5	2	3	**30**

RSK-038	Proveedor de servicios en la nube (Microsoft Azure)	Proveedor	Jefe de Tecnologías de la Información	[I.9] Interrupción de otros servicios y suministros esenciales (D)	Un proveedor de servicios de infraestructura experimenta una interrupción no planificada, lo que afecta negativamente a los servicios críticos de la empresa.	Jefe de Tecnologías de la Información	5	2	3	**30**
RSK-039	Ordenadores de escritorio	Hardware	Dpto. TI	[I.5] Avería de origen físico o lógico (D)	Posibilidad de fallos tanto físicos como lógicos en el hardware, ya sea debido a componentes electrónicos que pueden fallar o a problemas de software que afectan su funcionamiento.	Dpto. TI	4	2	5	**40**
RSK-040	Ordenadores de escritorio	Hardware	Dpto. TI	[E.2] Errores de administrador (D) (I) (C)	Fallos causados por errores en la gestión del hardware por parte de los administradores, lo que puede permitir a usuarios no autorizados realizar cambios en la configuración de los equipos, comprometiendo su seguridad.	Dpto. TI	4	2	5	**40**
RSK-041	Ordenadores de escritorio	Hardware	Dpto. TI	[E.23] Errores de mantenimiento / actualización de equipos (D)	Fallos relacionados con la falta de procedimientos adecuados de mantenimiento y actualización, lo que puede llevar a la persistencia de equipos con vulnerabilidades conocidas y aumentar el riesgo de fallos de seguridad.	Dpto. TI	4	3	2	**24**
RSK-042	Ordenadores de escritorio	Hardware	Dpto. TI	[E.24] Caída del sistema por agotamiento de recursos (D)	Ocurre cuando los recursos disponibles en el hardware no son suficientes para soportar la carga de trabajo, lo que provoca la caída del sistema. Esto puede ser resultado de una capacidad insuficiente de los recursos o de una demanda excesiva en momentos de alto uso.	Dpto. TI	4	2	2	**16**
RSK-043	Ordenadores para el teletrabajo (portátiles)	Hardware	Dpto. TI	[I.5] Avería de origen físico o lógico (D)	Posibilidad de fallos tanto físicos como lógicos en el hardware, ya sea debido a componentes electrónicos que pueden fallar o a problemas de software que afectan su funcionamiento.	Dpto. TI	4	2	2	**16**
RSK-044	Ordenadores para el teletrabajo (portátiles)	Hardware	Dpto. TI	[E.2] Errores de administrador (D) (I) (C)	Fallos causados por errores en la gestión del hardware por parte de los administradores, lo que puede permitir a usuarios no autorizados realizar cambios en la configuración de los equipos, comprometiendo su seguridad.	Dpto. TI	4	2	2	**16**
RSK-045	Ordenadores para el teletrabajo (portátiles)	Hardware	Dpto. TI	[E.23] Errores de mantenimiento / actualización de equipos (D)	Fallos relacionados con la falta de procedimientos adecuados de mantenimiento y actualización, lo que puede llevar a la persistencia de equipos con vulnerabilidades conocidas y aumentar el riesgo de fallos de seguridad.	Dpto. TI	4	2	2	**16**

RSK-046	Ordenadores para el teletrabajo (portátiles)	Hardware	Dpto. TI	[E.24] Caída del sistema por agotamiento de recursos (D)	Ocurre cuando los recursos disponibles en el hardware no son suficientes para soportar la carga de trabajo, lo que provoca la caída del sistema. Esto puede ser resultado de una capacidad insuficiente de los recursos o de una demanda excesiva en momentos de alto uso.	Dpto. TI	4	2	2	**16**
RSK-047	Enrutadores	Hardware	Dpto. TI	[I.5] Avería de origen físico o lógico (D)	Posibilidad de fallos tanto físicos como lógicos en el hardware, ya sea debido a componentes electrónicos que pueden fallar o a problemas de software que afectan su funcionamiento.	Dpto. TI	2	2	2	**8**
RSK-048	Enrutadores	Hardware	Dpto. TI	[E.2] Errores de administrador (D) (I) (C)	Fallos causados por errores en la gestión del hardware por parte de los administradores, lo que puede permitir a usuarios no autorizados realizar cambios en la configuración de los equipos, comprometiendo su seguridad.	Dpto. TI	2	2	2	**8**
RSK-049	Enrutadores	Hardware	Dpto. TI	[E.23] Errores de mantenimiento / actualización de equipos (D)	Fallos relacionados con la falta de procedimientos adecuados de mantenimiento y actualización, lo que puede llevar a la persistencia de equipos con vulnerabilidades conocidas y aumentar el riesgo de fallos de seguridad.	Dpto. TI	2	2	2	**8**
RSK-050	Enrutadores	Hardware	Dpto. TI	[E.24] Caída del sistema por agotamiento de recursos (D)	Ocurre cuando los recursos disponibles en el hardware no son suficientes para soportar la carga de trabajo, lo que provoca la caída del sistema. Esto puede ser resultado de una capacidad insuficiente de los recursos o de una demanda excesiva en momentos de alto uso.	Dpto. TI	2	2	2	**8**
RSK-051	Conmutadores	Hardware	Dpto. TI	[I.5] Avería de origen físico o lógico (D)	Posibilidad de fallos tanto físicos como lógicos en el hardware, ya sea debido a componentes electrónicos que pueden fallar o a problemas de software que afectan su funcionamiento.	Dpto. TI	2	2	2	**8**
RSK-052	Conmutadores	Hardware	Dpto. TI	[E.2] Errores de administrador (D) (I) (C)	Fallos causados por errores en la gestión del hardware por parte de los administradores, lo que puede permitir a usuarios no autorizados realizar cambios en la configuración de los equipos, comprometiendo su seguridad.	Dpto. TI	2	2	2	**8**

RSK-053	Conmutadores	Hardware	Dpto. TI	[E.23] Errores de mantenimiento / actualización de equipos (D)	Fallos relacionados con la falta de procedimientos adecuados de mantenimiento y actualización, lo que puede llevar a la persistencia de equipos con vulnerabilidades conocidas y aumentar el riesgo de fallos de seguridad.	Dpto. TI	2	2	3	**12**
RSK-054	Conmutadores	Hardware	Dpto. TI	[E.24] Caída del sistema por agotamiento de recursos (D)	Ocurre cuando los recursos disponibles en el hardware no son suficientes para soportar la carga de trabajo, lo que provoca la caída del sistema. Esto puede ser resultado de una capacidad insuficiente de los recursos o de una demanda excesiva en momentos de alto uso.	Dpto. TI	2	2	2	**8**
RSK-055	Firewall	Hardware	Dpto. TI	[I.5] Avería de origen físico o lógico (D)	Posibilidad de fallos tanto físicos como lógicos en el hardware, ya sea debido a componentes electrónicos que pueden fallar o a problemas de software que afectan su funcionamiento.	Dpto. TI	3	2	2	**12**
RSK-056	Firewall	Hardware	Dpto. TI	[E.2] Errores de administrador (D) (I) (C)	Fallos causados por errores en la gestión del hardware por parte de los administradores, lo que puede permitir a usuarios no autorizados realizar cambios en la configuración de los equipos, comprometiendo su seguridad.	Dpto. TI	3	2	2	**12**
RSK-057	Firewall	Hardware	Dpto. TI	[E.23] Errores de mantenimiento / actualización de equipos (D)	Fallos relacionados con la falta de procedimientos adecuados de mantenimiento y actualización, lo que puede llevar a la persistencia de equipos con vulnerabilidades conocidas y aumentar el riesgo de fallos de seguridad.	Dpto. TI	3	2	2	**12**
RSK-058	Firewall	Hardware	Dpto. TI	[E.24] Caída del sistema por agotamiento de recursos (D)	Ocurre cuando los recursos disponibles en el hardware no son suficientes para soportar la carga de trabajo, lo que provoca la caída del sistema. Esto puede ser resultado de una capacidad insuficiente de los recursos o de una demanda excesiva en momentos de alto uso.	Dpto. TI	3	2	2	**12**
RSK-059	Impresora	Hardware	Dpto. TI	[I.5] Avería de origen físico o lógico (D)	Posibilidad de fallos tanto físicos como lógicos en el hardware, ya sea debido a componentes electrónicos que pueden fallar o a problemas de software que afectan su funcionamiento.	Dpto. TI	2	2	2	**8**

RSK-060	Impresora	Hardware	Dpto. TI	[E.2] Errores de administrador (D) (I) (C)	Fallos causados por errores en la gestión del hardware por parte de los administradores, lo que puede permitir a usuarios no autorizados realizar cambios en la configuración de los equipos, comprometiendo su seguridad.	Dpto. TI	2	2	2	**8**
RSK-061	Impresora	Hardware	Dpto. TI	[E.23] Errores de mantenimiento / actualización de equipos (D)	Fallos relacionados con la falta de procedimientos adecuados de mantenimiento y actualización, lo que puede llevar a la persistencia de equipos con vulnerabilidades conocidas y aumentar el riesgo de fallos de seguridad.	Dpto. TI	2	2	2	**8**
RSK-062	Impresora	Hardware	Dpto. TI	[E.24] Caída del sistema por agotamiento de recursos (D)	Ocurre cuando los recursos disponibles en el hardware no son suficientes para soportar la carga de trabajo, lo que provoca la caída del sistema. Esto puede ser resultado de una capacidad insuficiente de los recursos o de una demanda excesiva en momentos de alto uso.	Dpto. TI	2	2	2	**8**
RSK-063	Sistema operativo	Software	Dpto. TI	[E.1] Errores de los usuarios (D) (I) (C)	Desaciertos cometidos por los usuarios al interactuar con los servicios o los datos, lo que puede provocar incidentes de diversa índole.	Dpto. TI	5	2	3	**30**
RSK-064	Sistema operativo	Software	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	5	2	3	**30**
RSK-065	Sistema operativo	Software	Dpto. TI	[E.4] Errores de configuración (D) (I) (C)	Configuraciones incorrectas o mal gestionadas que causan el deterioro del software, ya sea debido a defectos originales o a problemas surgidos durante la operación del sistema.	Dpto. TI	5	2	4	**40**
RSK-066	Sistema operativo	Software	Dpto. TI	[E.20] Vulnerabilidades de los programas (D) (I) (C)	Defectos en el código de los programas que generan un funcionamiento incorrecto sin intervención intencionada por parte del usuario, afectando la integridad de los datos o la capacidad de operación.	Dpto. TI	5	2	3	**30**
RSK-067	Sistema operativo	Software	Dpto. TI	[E.21] Errores de mantenimiento /actualización (D) (I) (C)	Defectos en los procesos o controles de actualización del código, lo que permite que se sigan utilizando programas con fallos conocidos y corregidos por el fabricante.	Dpto. TI	5	2	3	**30**

RSK-068	Sistema operativo	Software	Dpto. TI	[A.5] Suplantación de la identidad del usuario (I) (C)	Cuando un atacante logra hacerse pasar por un usuario autorizado, obteniendo acceso a sus privilegios y utilizándolos para sus propios fines. Este tipo de amenaza puede ser ejecutada por personal interno, externo a la organización o contratado temporalmente.	Dpto. TI	5	3	3	**45**
RSK-069	Sistema operativo	Software	Dpto. TI	[A.6] Abuso de privilegios de acceso (D) (I) (C)	Cuando un usuario utiliza sus privilegios de acceso de manera inadecuada, realizando acciones que están fuera de su ámbito de competencia.	Dpto. TI	5	2	3	**30**
RSK-070	Sistema operativo	Software	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	5	3	3	**45**
RSK-071	Antivirus	Software	Dpto. TI	[E.1] Errores de los usuarios (D) (I) (C)	Desaciertos cometidos por los usuarios al interactuar con los servicios o los datos, lo que puede provocar incidentes de diversa índole.	Dpto. TI	4	2	3	**24**
RSK-072	Antivirus	Software	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	4	2	3	**24**
RSK-073	Antivirus	Software	Dpto. TI	[E.4] Errores de configuración (D) (I) (C)	Configuraciones incorrectas o mal gestionadas que causan el deterioro del software, ya sea debido a defectos originales o a problemas surgidos durante la operación del sistema.	Dpto. TI	4	2	3	**24**
RSK-074	Antivirus	Software	Dpto. TI	[E.20] Vulnerabilidades de los programas (D) (I) (C)	Defectos en el código de los programas que generan un funcionamiento incorrecto sin intervención intencionada por parte del usuario, afectando la integridad de los datos o la capacidad de operación.	Dpto. TI	4	2	3	**24**
RSK-075	Antivirus	Software	Dpto. TI	[E.21] Errores de mantenimiento /actualización (D) (I) (C)	Defectos en los procesos o controles de actualización del código, lo que permite que se sigan utilizando programas con fallos conocidos y corregidos por el fabricante.	Dpto. TI	4	2	3	**24**

RSK-076	Antivirus	Software	Dpto. TI	[A.5] Suplantación de la identidad del usuario (I) (C)	Cuando un atacante logra hacerse pasar por un usuario autorizado, obteniendo acceso a sus privilegios y utilizándolos para sus propios fines. Este tipo de amenaza puede ser ejecutada por personal interno, externo a la organización o contratado temporalmente.	Dpto. TI	4	3	3	**36**
RSK-077	Antivirus	Software	Dpto. TI	[A.6] Abuso de privilegios de acceso (D) (I) (C)	Cuando un usuario utiliza sus privilegios de acceso de manera inadecuada, realizando acciones que están fuera de su ámbito de competencia.	Dpto. TI	4	2	3	**24**
RSK-078	Antivirus	Software	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	4	3	3	**36**
RSK-079	Adobe Acrobat Professional	Software	Dpto. TI	[E.1] Errores de los usuarios (D) (I) (C)	Desaciertos cometidos por los usuarios al interactuar con los servicios o los datos, lo que puede provocar incidentes de diversa índole.	Dpto. TI	4	2	3	**24**
RSK-080	Adobe Acrobat Professional	Software	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	4	2	3	**24**
RSK-081	Adobe Acrobat Professional	Software	Dpto. TI	[E.4] Errores de configuración (D) (I) (C)	Configuraciones incorrectas o mal gestionadas que causan el deterioro del software, ya sea debido a defectos originales o a problemas surgidos durante la operación del sistema.	Dpto. TI	4	2	3	**24**
RSK-082	Adobe Acrobat Professional	Software	Dpto. TI	[E.20] Vulnerabilidades de los programas (D) (I) (C)	Defectos en el código de los programas que generan un funcionamiento incorrecto sin intervención intencionada por parte del usuario, afectando la integridad de los datos o la capacidad de operación.	Dpto. TI	4	2	3	**24**
RSK-083	Adobe Acrobat Professional	Software	Dpto. TI	[E.21] Errores de mantenimiento /actualización (D) (I) (C)	Defectos en los procesos o controles de actualización del código, lo que permite que se sigan utilizando programas con fallos conocidos y corregidos por el fabricante.	Dpto. TI	4	2	3	**24**

RSK-084	Adobe Acrobat Professional	Software	Dpto. TI	[A.5] Suplantación de la identidad del usuario (I) (C)	Cuando un atacante logra hacerse pasar por un usuario autorizado, obteniendo acceso a sus privilegios y utilizándolos para sus propios fines. Este tipo de amenaza puede ser ejecutada por personal interno, externo a la organización o contratado temporalmente.	Dpto. TI	4	3	3	**36**
RSK-085	Adobe Acrobat Professional	Software	Dpto. TI	[A.6] Abuso de privilegios de acceso (D) (I) (C)	Cuando un usuario utiliza sus privilegios de acceso de manera inadecuada, realizando acciones que están fuera de su ámbito de competencia.	Dpto. TI	4	2	3	**24**
RSK-086	Adobe Acrobat Professional	Software	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	4	3	3	**36**
RSK-087	Microsoft Office 365	Software	Dpto. TI	[E.1] Errores de los usuarios (D) (I) (C)	Desaciertos cometidos por los usuarios al interactuar con los servicios o los datos, lo que puede provocar incidentes de diversa índole.	Dpto. TI	4	2	3	**24**
RSK-088	Microsoft Office 365	Software	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	4	2	3	**24**
RSK-089	Microsoft Office 365	Software	Dpto. TI	[E.4] Errores de configuración (D) (I) (C)	Configuraciones incorrectas o mal gestionadas que causan el deterioro del software, ya sea debido a defectos originales o a problemas surgidos durante la operación del sistema.	Dpto. TI	4	2	3	**24**
RSK-090	Microsoft Office 365	Software	Dpto. TI	[E.20] Vulnerabilidades de los programas (D) (I) (C)	Defectos en el código de los programas que generan un funcionamiento incorrecto sin intervención intencionada por parte del usuario, afectando la integridad de los datos o la capacidad de operación.	Dpto. TI	4	2	3	**24**
RSK-091	Microsoft Office 365	Software	Dpto. TI	[E.21] Errores de mantenimiento /actualización (D) (I) (C)	Defectos en los procesos o controles de actualización del código, lo que permite que se sigan utilizando programas con fallos conocidos y corregidos por el fabricante.	Dpto. TI	4	2	3	**24**

RSK-092	Microsoft Office 365	Software	Dpto. TI	[A.5] Suplantación de la identidad del usuario (I) (C)	Cuando un atacante logra hacerse pasar por un usuario autorizado, obteniendo acceso a sus privilegios y utilizándolos para sus propios fines. Este tipo de amenaza puede ser ejecutada por personal interno, externo a la organización o contratado temporalmente.	Dpto. TI	4	3	3	**36**
RSK-093	Microsoft Office 365	Software	Dpto. TI	[A.6] Abuso de privilegios de acceso (D) (I) (C)	Cuando un usuario utiliza sus privilegios de acceso de manera inadecuada, realizando acciones que están fuera de su ámbito de competencia.	Dpto. TI	4	2	3	**24**
RSK-094	Microsoft Office 365	Software	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	4	3	3	**36**
RSK-095	Aplicaciones internas de administración	Software	Dpto. TI	[E.1] Errores de los usuarios (D) (I) (C)	Desaciertos cometidos por los usuarios al interactuar con los servicios o los datos, lo que puede provocar incidentes de diversa índole.	Dpto. TI	4	2	3	**24**
RSK-096	Aplicaciones internas de administración	Software	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	4	2	3	**24**
RSK-097	Aplicaciones internas de administración	Software	Dpto. TI	[E.4] Errores de configuración (D) (I) (C)	Configuraciones incorrectas o mal gestionadas que causan el deterioro del software, ya sea debido a defectos originales o a problemas surgidos durante la operación del sistema.	Dpto. TI	4	2	3	**24**
RSK-098	Aplicaciones internas de administración	Software	Dpto. TI	[E.20] Vulnerabilidades de los programas (D) (I) (C)	Defectos en el código de los programas que generan un funcionamiento incorrecto sin intervención intencionada por parte del usuario, afectando la integridad de los datos o la capacidad de operación.	Dpto. TI	4	2	3	**24**
RSK-099	Aplicaciones internas de administración	Software	Dpto. TI	[E.21] Errores de mantenimiento /actualización (D) (I) (C)	Defectos en los procesos o controles de actualización del código, lo que permite que se sigan utilizando programas con fallos conocidos y corregidos por el fabricante.	Dpto. TI	4	2	3	**24**

RSK-100	Aplicaciones internas de administración	Software	Dpto. TI	[A.5] Suplantación de la identidad del usuario (I) (C)	Cuando un atacante logra hacerse pasar por un usuario autorizado, obteniendo acceso a sus privilegios y utilizándolos para sus propios fines. Este tipo de amenaza puede ser ejecutada por personal interno, externo a la organización o contratado temporalmente.	Dpto. TI	4	3	3	**36**
RSK-101	Aplicaciones internas de administración	Software	Dpto. TI	[A.6] Abuso de privilegios de acceso (D) (I) (C)	Cuando un usuario utiliza sus privilegios de acceso de manera inadecuada, realizando acciones que están fuera de su ámbito de competencia.	Dpto. TI	4	2	3	**24**
RSK-102	Aplicaciones internas de administración	Software	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	4	3	3	**36**
RSK-103	Herramientas de traducción	Software	Dpto. TI	[E.1] Errores de los usuarios (D) (I) (C)	Desaciertos cometidos por los usuarios al interactuar con los servicios o los datos, lo que puede provocar incidentes de diversa índole.	Dpto. TI	4	2	3	**24**
RSK-104	Herramientas de traducción	Software	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	4	2	3	**24**
RSK-105	Herramientas de traducción	Software	Dpto. TI	[E.4] Errores de configuración (D) (I) (C)	Configuraciones incorrectas o mal gestionadas que causan el deterioro del software, ya sea debido a defectos originales o a problemas surgidos durante la operación del sistema.	Dpto. TI	4	2	3	**24**
RSK-106	Herramientas de traducción	Software	Dpto. TI	[E.20] Vulnerabilidades de los programas (D) (I) (C)	Defectos en el código de los programas que generan un funcionamiento incorrecto sin intervención intencionada por parte del usuario, afectando la integridad de los datos o la capacidad de operación.	Dpto. TI	4	2	3	**24**
RSK-107	Herramientas de traducción	Software	Dpto. TI	[E.21] Errores de mantenimiento /actualización (D) (I) (C)	Defectos en los procesos o controles de actualización del código, lo que permite que se sigan utilizando programas con fallos conocidos y corregidos por el fabricante.	Dpto. TI	4	2	3	**24**

RSK-108	Herramientas de traducción	Software	Dpto. TI	[A.5] Suplantación de la identidad del usuario (I) (C)	Cuando un atacante logra hacerse pasar por un usuario autorizado, obteniendo acceso a sus privilegios y utilizándolos para sus propios fines. Este tipo de amenaza puede ser ejecutada por personal interno, externo a la organización o contratado temporalmente.	Dpto. TI	4	3	3	**36**
RSK-109	Herramientas de traducción	Software	Dpto. TI	[A.6] Abuso de privilegios de acceso (D) (I) (C)	Cuando un usuario utiliza sus privilegios de acceso de manera inadecuada, realizando acciones que están fuera de su ámbito de competencia.	Dpto. TI	4	2	3	**24**
RSK-110	Herramientas de traducción	Software	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	4	3	3	**36**
RSK-111	Licencia del sistema operativo	Licencia de software	Dpto. TI	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Dpto. TI	3	2	3	**18**
RSK-112	Licencia del antivirus	Licencia de software	Dpto. TI	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Dpto. TI	3	2	3	**18**
RSK-113	Licencia del software especializado (traducción)	Licencia de software	Dpto. TI	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Dpto. TI	4	2	3	**24**
RSK-114	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	5	2	3	**30**

RSK-115	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.8] Difusión de software dañino (D) (I) (C)	Un empleado descarga inadvertidamente un archivo infectado con malware en una carpeta compartida, propagando la amenaza a otros usuarios.	Dpto. TI	5	2	3	**30**
RSK-116	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Dpto. TI	5	3	4	**60**
RSK-117	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Dpto. TI	5	2	5	**50**
RSK-118	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Dpto. TI	5	2	5	**50**
RSK-119	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	5	3	3	**45**
RSK-120	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Dpto. TI	5	1	5	**25**
RSK-121	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de esta, ya sea por acciones maliciosas o accidentales.	Dpto. TI	5	2	5	**50**
RSK-122	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Dpto. TI	5	2	3	**30**
RSK-123	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.3] Errores de monitorización (log) (I)	Registro inadecuado de actividades, que puede manifestarse en falta de registros, registros incompletos, registros con fechas incorrectas o atribuciones erróneas.	Dpto. TI	5	2	3	**30**

RSK-124	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.8] Difusión de software dañino (D) (I) (C)	Un empleado descarga inadvertidamente un archivo infectado con malware en una carpeta compartida, propagando la amenaza a otros usuarios.	Dpto. TI	5	2	3	**30**
RSK-125	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Dpto. TI	5	3	4	**60**
RSK-126	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Dpto. TI	5	2	5	**50**
RSK-127	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Dpto. TI	5	2	5	**50**
RSK-128	Archivos de configuración de red	Carpeta de red	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	5	3	3	**45**
RSK-129	Archivos de configuración de red	Carpeta de red	Dpto. TI	[A.15] Modificación deliberada de la información [I]	Modificación accidental o deliberada de los datos e información por parte de usuarios autorizados o atacantes, lo que puede resultar en cambios no deseados en la integridad de la información.	Dpto. TI	5	1	5	**25**
RSK-130	Archivos de configuración de red	Carpeta de red	Dpto. TI	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de la misma, ya sea por acciones maliciosas o accidentales.	Dpto. TI	5	2	5	**50**
RSK-131	Archivos de configuración de red	Carpeta de red	Dpto. TI	[A.19] Divulgación de información (C)	Revelación no autorizada de datos e información confidencial a personas no autorizadas, ya sea de manera intencional o accidental, lo que puede comprometer la seguridad y la privacidad de la información.	Dpto. TI	5	2	3	**30**
RSK-132	VPN	Red	Dpto. TI	[I.8] Fallo de servicios de comunicaciones (D)	Un corte en la infraestructura de red externa deja a la empresa incomunicada con sus clientes y proveedores.	Dpto. TI	3	1	5	**15**

RSK-133	VPN	Red	Dpto. TI	[A.11] Acceso no autorizado (D) (I)	Posibilidad de que individuos no autorizados obtengan acceso a las instalaciones, servicios de comunicaciones contratados a terceros y elementos de infraestructura propia, como LAN, acceso a Internet, red local, DIBA, Wifi, MacroLAN, entre otros.	Dpto. TI	3	2	3	**18**
RSK-134	VPN	Red	Dpto. TI	[A.14] Interceptación de información (escucha) (C)	Riesgo de que terceros intercepten de manera ilícita la información transmitida a través de la red, lo que puede resultar en la exposición de datos confidenciales o sensibles.	Dpto. TI	3	2	3	**18**
RSK-135	Cableado eléctrico	Red	Dpto. TI	[I.8] Fallo de servicios de comunicaciones (D)	Un corte en la infraestructura de red externa deja a la empresa incomunicada con sus clientes y proveedores.	Dpto. TI	3	1	2	**6**
RSK-136	Cableado eléctrico	Red	Dpto. TI	[A.11] Acceso no autorizado (D) (I)	Posibilidad de que individuos no autorizados obtengan acceso a las instalaciones, servicios de comunicaciones contratados a terceros y elementos de infraestructura propia, como LAN, acceso a Internet, red local, DIBA, Wifi, MacroLAN, entre otros.	Dpto. TI	3	2	3	**18**
RSK-137	Cableado eléctrico	Red	Dpto. TI	[A.14] Interceptación de información (escucha) (C)	Riesgo de que terceros intercepten de manera ilícita la información transmitida a través de la red, lo que puede resultar en la exposición de datos confidenciales o sensibles.	Dpto. TI	3	2	3	**18**
RSK-138	Cableado telecomunicaciones	Red	Dpto. TI	[I.8] Fallo de servicios de comunicaciones (D)	Un corte en la infraestructura de red externa deja a la empresa incomunicada con sus clientes y proveedores.	Dpto. TI	3	1	2	**6**
RSK-139	Cableado telecomunicaciones	Red	Dpto. TI	[A.11] Acceso no autorizado (D) (I)	Posibilidad de que individuos no autorizados obtengan acceso a las instalaciones, servicios de comunicaciones contratados a terceros y elementos de infraestructura propia, como LAN, acceso a Internet, red local, DIBA, Wifi, MacroLAN, entre otros.	Dpto. TI	3	2	3	**18**
RSK-140	Cableado telecomunicaciones	Red	Dpto. TI	[A.14] Interceptación de información (escucha) (C)	Riesgo de que terceros intercepten de manera ilícita la información transmitida a través de la red, lo que puede resultar en la exposición de datos confidenciales o sensibles.	Dpto. TI	3	2	3	**18**

RSK-141	Servicio Internet	Red	Dpto. TI	[I.8] Fallo de servicios de comunicaciones (D)	Un corte en la infraestructura de red externa deja a la empresa incomunicada con sus clientes y proveedores.	Dpto. TI	4	1	5	**20**
RSK-142	Servicio Internet	Red	Dpto. TI	[A.11] Acceso no autorizado (D) (I)	Posibilidad de que individuos no autorizados obtengan acceso a las instalaciones, servicios de comunicaciones contratados a terceros y elementos de infraestructura propia, como LAN, acceso a Internet, red local, DIBA, Wifi, MacroLAN, entre otros.	Dpto. TI	4	2	3	**24**
RSK-143	Servicio Internet	Red	Dpto. TI	[A.14] Interceptación de información (escucha) (C)	Riesgo de que terceros intercepten de manera ilícita la información transmitida a través de la red, lo que puede resultar en la exposición de datos confidenciales o sensibles.	Dpto. TI	4	2	3	**24**
RSK-144	Red inalámbrica	Red	Dpto. TI	[I.8] Fallo de servicios de comunicaciones (D)	Un corte en la infraestructura de red externa deja a la empresa incomunicada con sus clientes y proveedores.	Dpto. TI	4	1	2	**8**
RSK-145	Red inalámbrica	Red	Dpto. TI	[A.11] Acceso no autorizado (D) (I)	Posibilidad de que individuos no autorizados obtengan acceso a las instalaciones, servicios de comunicaciones contratados a terceros y elementos de infraestructura propia, como LAN, acceso a Internet, red local, DIBA, Wifi, MacroLAN, entre otros.	Dpto. TI	4	2	3	**24**
RSK-146	Red inalámbrica	Red	Dpto. TI	[A.14] Interceptación de información (escucha) (C)	Riesgo de que terceros intercepten de manera ilícita la información transmitida a través de la red, lo que puede resultar en la exposición de datos confidenciales o sensibles.	Dpto. TI	4	2	3	**24**
RSK-147	Cableado eléctrico	Red	Dpto. TI	[I.8] Fallo de servicios de comunicaciones (D)	Un corte en la infraestructura de red externa deja a la empresa incomunicada con sus clientes y proveedores.	Dpto. TI	3	1	2	**6**
RSK-148	Cableado eléctrico	Red	Dpto. TI	[A.11] Acceso no autorizado (D) (I)	Posibilidad de que individuos no autorizados obtengan acceso a las instalaciones, servicios de comunicaciones contratados a terceros y elementos de infraestructura propia, como LAN, acceso a Internet, red local, DIBA, Wifi, MacroLAN, entre otros.	Dpto. TI	3	2	3	**18**

RSK-149	Cableado eléctrico	Red	Dpto. TI	[A.14] Interceptación de información (escucha) (C)	Riesgo de que terceros intercepten de manera ilícita la información transmitida a través de la red, lo que puede resultar en la exposición de datos confidenciales o sensibles.	Dpto. TI	3	2	3	**18**
RSK-150	Sistema climatización	Elemento auxiliar	Instalaciones	[I.9] Interrupción de otros suministros y servicios esenciales (D)	Posibilidad de interrupción en el suministro o funcionamiento de equipos auxiliares críticos para el soporte de los sistemas de información, como sistemas de alimentación ininterrumpida (SAI), grupos electrógenos, equipos de climatización, sistemas de extinción de incendios, centralitas, entre otros. Esta interrupción puede causar la incapacidad de mantener la operatividad de los sistemas de información ante situaciones de emergencia o Fallos en la infraestructura auxiliar.	Instalaciones	2	1	2	**4**
RSK-151	Sistema detección incendios	Elemento auxiliar	Instalaciones	[I.9] Interrupción de otros suministros y servicios esenciales (D)	Posibilidad de interrupción en el suministro o funcionamiento de equipos auxiliares críticos para el soporte de los sistemas de información, como sistemas de alimentación ininterrumpida (SAI), grupos electrógenos, equipos de climatización, sistemas de extinción de incendios, centralitas, entre otros. Esta interrupción puede causar la incapacidad de mantener la operatividad de los sistemas de información ante situaciones de emergencia o Fallos en la infraestructura auxiliar.	Instalaciones	2	1	2	**4**
RSK-152	Caja fuerte	Elemento auxiliar	Jefe Administrativo y Financiero	[I.9] Interrupción de otros suministros y servicios esenciales (D)	Posibilidad de interrupción en el suministro o funcionamiento de equipos auxiliares críticos para el soporte de los sistemas de información, como sistemas de alimentación ininterrumpida (SAI), grupos electrógenos, equipos de climatización, sistemas de extinción de incendios, centralitas, entre otros. Esta interrupción puede causar la incapacidad de mantener la operatividad de los sistemas de información ante situaciones de emergencia o Fallos en la infraestructura auxiliar.	Jefe Administrativo y Financiero	4	1	2	**8**

RSK-153	Destructor de papeles	Elemento auxiliar	Dpto. TI	[I.9] Interrupción de otros suministros y servicios esenciales (D)	Posibilidad de interrupción en el suministro o funcionamiento de equipos auxiliares críticos para el soporte de los sistemas de información, como sistemas de alimentación ininterrumpida (SAI), grupos electrógenos, equipos de climatización, sistemas de extinción de incendios, centralitas, entre otros. Esta interrupción puede causar la incapacidad de mantener la operatividad de los sistemas de información ante situaciones de emergencia o Fallos en la infraestructura auxiliar.	Dpto. TI	1	1	2	**2**
RSK-154	Director Ejecutivo	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-155	Director Ejecutivo	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-156	Director Ejecutivo	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-157	Director Ejecutivo	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-158	Director Ejecutivo	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-159	Director Ejecutivo	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-160	Director Ejecutivo	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-161	Jefe de TI	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-162	Jefe de TI	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-163	Jefe de TI	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-164	Jefe de TI	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-165	Jefe de TI	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-166	Jefe de TI	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-167	Jefe de TI	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-168	Empleado interno de TI	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-169	Empleado interno de TI	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-170	Empleado interno de TI	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-171	Empleado interno de TI	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-172	Empleado interno de TI	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-173	Empleado interno de TI	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-174	Empleado interno de TI	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-175	Jefe Administrativo y Financiero	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-176	Jefe Administrativo y Financiero	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-177	Jefe Administrativo y Financiero	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-178	Jefe Administrativo y Financiero	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-179	Jefe Administrativo y Financiero	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-180	Jefe Administrativo y Financiero	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-181	Jefe Administrativo y Financiero	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-182	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-183	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-184	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-185	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-186	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-187	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-188	Responsable de Administración/RRHH/Contabilidad/Comercial	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-189	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-190	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-191	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-192	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-193	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-194	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-195	Jefes de Proyectos de Traducción e Interpretación	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-196	Traductores e Intérpretes	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-197	Traductores e Intérpretes	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-198	Traductores e Intérpretes	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-199	Traductores e Intérpretes	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-200	Traductores e Intérpretes	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-201	Traductores e Intérpretes	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-202	Traductores e Intérpretes	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-203	Estudiantes en prácticas	Personal	Él mismo	[E.7] Deficiencias en la organización (D)	Riesgo de que la organización no tenga un proceso adecuado para gestionar y mantener actualizadas las licencias de software comerciales. Esto puede llevar a un uso no autorizado del software, violaciones de los términos de licencia y posibles sanciones legales por parte de los proveedores de software.	Él mismo	2	2	3	**12**
RSK-204	Estudiantes en prácticas	Personal	Él mismo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Él mismo	2	3	4	**24**
RSK-205	Estudiantes en prácticas	Personal	Él mismo	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Él mismo	2	2	5	**20**
RSK-206	Estudiantes en prácticas	Personal	Él mismo	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Él mismo	2	2	3	**12**
RSK-207	Estudiantes en prácticas	Personal	Él mismo	[E.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**
RSK-208	Estudiantes en prácticas	Personal	Él mismo	[A.28] Indisponibilidad del personal (D)	Ausencia prolongada del personal crítico para el funcionamiento de los procesos de negocio, ya sea por motivos de salud, conflictos laborales u otras razones, lo que puede afectar la continuidad operativa y la respuesta ante incidentes.	Él mismo	2	2	2	**8**

RSK-209	Estudiantes en prácticas	Personal	Él mismo	[A.30] Ingeniería social (picaresca) (D) (I) (C)	Manipulación de la buena fe o confianza de los empleados para obtener información confidencial o realizar acciones perjudiciales para la organización, mediante técnicas como el engaño, la persuasión o el aprovechamiento de situaciones sociales.	Él mismo	2	2	3	**12**
RSK-210	Oficinas	Instalación	Dpto. TI	[I.*] Desastres industriales (D)	Posibilidad de eventos no controlados dentro de instalaciones industriales que podrían resultar en daños significativos a los recursos del sistema, como fugas químicas, explosiones, o Fallos en procesos industriales.	Dpto. TI	1	1	2	**2**
RSK-211	Oficinas	Instalación	Dpto. TI	[I.1] Fuego (D)	Deficiencia en la detección temprana y extinción de incendios, lo que aumenta el riesgo de que un incendio destruya los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-212	Oficinas	Instalación	Dpto. TI	[I.2] Daños por agua (D)	Posibilidad de daños causados por escapes, fugas o inundaciones, especialmente en áreas cercanas a los recursos del sistema, debido a sistemas de fontanería defectuosos o inadecuados.	Dpto. TI	1	1	2	**2**
RSK-213	Oficinas	Instalación	Dpto. TI	[I.3] Contaminación mecánica (D)	Exposición a vibraciones, polvo, suciedad, interferencias de radio, campos magnéticos, luz ultravioleta, y otros factores que pueden deteriorar o interferir con los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-214	Oficinas	Instalación	Dpto. TI	[I.4] Contaminación electromagnética (D)	Exposición a interferencias de radio, campos magnéticos, luz ultravioleta y otros fenómenos electromagnéticos que pueden provocar perturbaciones en los sistemas electrónicos y afectar su funcionamiento normal.	Dpto. TI	1	1	2	**2**
RSK-215	Oficinas	Instalación	Dpto. TI	[I.6] Corte del suministro eléctrico (D)	Interrupción en el suministro de energía eléctrica, lo que resulta en la falta de alimentación de potencia y la incapacidad de operar los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-216	Oficinas	Instalación	Dpto. TI	[I.7] Condiciones inadecuadas de temperatura o humedad (D)	Falta de control adecuado sobre las condiciones ambientales, como temperatura y humedad, lo que puede afectar negativamente la funcionalidad y la integridad de los recursos del sistema.	Dpto. TI	1	1	2	**2**

RSK-217	Oficinas	Instalación	Dpto. TI	[A.11] Acceso no autorizado (D)	Deficiencias en los controles físicos de acceso y en las políticas y procedimientos de seguridad, que podrían permitir el acceso no autorizado a las instalaciones y la realización de actos destructivos por parte de personal interno o externo.	Dpto. TI	1	1	5	**5**
RSK-218	Oficinas	Instalación	Dpto. TI	[A.26] Ataque destructivo (D)	Riesgo de actos de vandalismo, terrorismo, o acción militar que podrían resultar en la destrucción deliberada de los recursos del sistema, llevados a cabo por individuos internos o externos a la organización.	Dpto. TI	1	1	5	**5**
RSK-219	Despacho del director	Instalación	Dpto. TI	[I.*] Desastres industriales (D)	Posibilidad de eventos no controlados dentro de instalaciones industriales que podrían resultar en daños significativos a los recursos del sistema, como fugas químicas, explosiones, o Fallos en procesos industriales.	Dpto. TI	1	1	2	**2**
RSK-220	Despacho del director	Instalación	Dpto. TI	[I.1] Fuego (D)	Deficiencia en la detección temprana y extinción de incendios, lo que aumenta el riesgo de que un incendio destruya los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-221	Despacho del director	Instalación	Dpto. TI	[I.2] Daños por agua (D)	Posibilidad de daños causados por escapes, fugas o inundaciones, especialmente en áreas cercanas a los recursos del sistema, debido a sistemas de fontanería defectuosos o inadecuados.	Dpto. TI	1	1	2	**2**
RSK-222	Despacho del director	Instalación	Dpto. TI	[I.3] Contaminación mecánica (D)	Exposición a vibraciones, polvo, suciedad, interferencias de radio, campos magnéticos, luz ultravioleta, y otros factores que pueden deteriorar o interferir con los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-223	Despacho del director	Instalación	Dpto. TI	[I.4] Contaminación electromagnética (D)	Exposición a interferencias de radio, campos magnéticos, luz ultravioleta y otros fenómenos electromagnéticos que pueden provocar perturbaciones en los sistemas electrónicos y afectar su funcionamiento normal.	Dpto. TI	1	1	2	**2**
RSK-224	Despacho del director	Instalación	Dpto. TI	[I.6] Corte del suministro eléctrico (D)	Interrupción en el suministro de energía eléctrica, lo que resulta en la falta de alimentación de potencia y la incapacidad de operar los recursos del sistema.	Dpto. TI	1	1	5	**5**

RSK-225	Despacho del director	Instalación	Dpto. TI	[I.7] Condiciones inadecuadas de temperatura o humedad (D)	Falta de control adecuado sobre las condiciones ambientales, como temperatura y humedad, lo que puede afectar negativamente la funcionalidad y la integridad de los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-226	Despacho del director	Instalación	Dpto. TI	[A.11] Acceso no autorizado (D)	Deficiencias en los controles físicos de acceso y en las políticas y procedimientos de seguridad, que podrían permitir el acceso no autorizado a las instalaciones y la realización de actos destructivos por parte de personal interno o externo.	Dpto. TI	1	1	5	**5**
RSK-227	Despacho del director	Instalación	Dpto. TI	[A.26] Ataque destructivo (D)	Riesgo de actos de vandalismo, terrorismo, o acción militar que podrían resultar en la destrucción deliberada de los recursos del sistema, llevados a cabo por individuos internos o externos a la organización.	Dpto. TI	1	1	5	**5**
RSK-228	Despacho de cada empleado	Instalación	Dpto. TI	[I.*] Desastres industriales (D)	Posibilidad de eventos no controlados dentro de instalaciones industriales que podrían resultar en daños significativos a los recursos del sistema, como fugas químicas, explosiones, o Fallos en procesos industriales.	Dpto. TI	1	1	2	**2**
RSK-229	Despacho de cada empleado	Instalación	Dpto. TI	[I.1] Fuego (D)	Deficiencia en la detección temprana y extinción de incendios, lo que aumenta el riesgo de que un incendio destruya los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-230	Despacho de cada empleado	Instalación	Dpto. TI	[I.2] Daños por agua (D)	Posibilidad de daños causados por escapes, fugas o inundaciones, especialmente en áreas cercanas a los recursos del sistema, debido a sistemas de fontanería defectuosos o inadecuados.	Dpto. TI	1	1	2	**2**
RSK-231	Despacho de cada empleado	Instalación	Dpto. TI	[I.3] Contaminación mecánica (D)	Exposición a vibraciones, polvo, suciedad, interferencias de radio, campos magnéticos, luz ultravioleta, y otros factores que pueden deteriorar o interferir con los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-232	Despacho de cada empleado	Instalación	Dpto. TI	[I.4] Contaminación electromagnética (D)	Exposición a interferencias de radio, campos magnéticos, luz ultravioleta y otros fenómenos electromagnéticos que pueden provocar perturbaciones en los sistemas electrónicos y afectar su funcionamiento normal.	Dpto. TI	1	1	2	**2**

RSK-233	Despacho de cada empleado	Instalación	Dpto. TI	[I.6] Corte del suministro eléctrico (D)	Interrupción en el suministro de energía eléctrica, lo que resulta en la falta de alimentación de potencia y la incapacidad de operar los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-234	Despacho de cada empleado	Instalación	Dpto. TI	[I.7] Condiciones inadecuadas de temperatura o humedad (D)	Falta de control adecuado sobre las condiciones ambientales, como temperatura y humedad, lo que puede afectar negativamente la funcionalidad y la integridad de los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-235	Despacho de cada empleado	Instalación	Dpto. TI	[A.11] Acceso no autorizado (D)	Deficiencias en los controles físicos de acceso y en las políticas y procedimientos de seguridad, que podrían permitir el acceso no autorizado a las instalaciones y la realización de actos destructivos por parte de personal interno o externo.	Dpto. TI	1	1	5	**5**
RSK-236	Despacho de cada empleado	Instalación	Dpto. TI	[A.26] Ataque destructivo (D)	Riesgo de actos de vandalismo, terrorismo, o acción militar que podrían resultar en la destrucción deliberada de los recursos del sistema, llevados a cabo por individuos internos o externos a la organización.	Dpto. TI	1	1	5	**5**
RSK-237	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[I.*] Desastres industriales (D)	Posibilidad de eventos no controlados dentro de instalaciones industriales que podrían resultar en daños significativos a los recursos del sistema, como fugas químicas, explosiones, o Fallos en procesos industriales.	Dpto. TI	1	1	2	**2**
RSK-238	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[I.1] Fuego (D)	Deficiencia en la detección temprana y extinción de incendios, lo que aumenta el riesgo de que un incendio destruya los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-239	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[I.2] Daños por agua (D)	Posibilidad de daños causados por escapes, fugas o inundaciones, especialmente en áreas cercanas a los recursos del sistema, debido a sistemas de fontanería defectuosos o inadecuados.	Dpto. TI	1	1	2	**2**
RSK-240	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[I.3] Contaminación mecánica (D)	Exposición a vibraciones, polvo, suciedad, interferencias de radio, campos magnéticos, luz ultravioleta, y otros factores que pueden deteriorar o interferir con los recursos del sistema.	Dpto. TI	1	1	2	**2**

RSK-241	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[I.4] Contaminación electromagnética (D)	Exposición a interferencias de radio, campos magnéticos, luz ultravioleta y otros fenómenos electromagnéticos que pueden provocar perturbaciones en los sistemas electrónicos y afectar su funcionamiento normal.	Dpto. TI	1	1	2	**2**
RSK-242	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[I.6] Corte del suministro eléctrico (D)	Interrupción en el suministro de energía eléctrica, lo que resulta en la falta de alimentación de potencia y la incapacidad de operar los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-243	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[I.7] Condiciones inadecuadas de temperatura o humedad (D)	Falta de control adecuado sobre las condiciones ambientales, como temperatura y humedad, lo que puede afectar negativamente la funcionalidad y la integridad de los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-244	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[A.11] Acceso no autorizado (D)	Deficiencias en los controles físicos de acceso y en las políticas y procedimientos de seguridad, que podrían permitir el acceso no autorizado a las instalaciones y la realización de actos destructivos por parte de personal interno o externo.	Dpto. TI	1	1	5	**5**
RSK-245	Laboratorios de traducción e interpretación	Instalación	Dpto. TI	[A.26] Ataque destructivo (D)	Riesgo de actos de vandalismo, terrorismo, o acción militar que podrían resultar en la destrucción deliberada de los recursos del sistema, llevados a cabo por individuos internos o externos a la organización.	Dpto. TI	1	1	5	**5**
RSK-246	Salas	Instalación	Dpto. TI	[I.*] Desastres industriales (D)	Posibilidad de eventos no controlados dentro de instalaciones industriales que podrían resultar en daños significativos a los recursos del sistema, como fugas químicas, explosiones, o Fallos en procesos industriales.	Dpto. TI	1	1	2	**2**
RSK-247	Salas	Instalación	Dpto. TI	[I.1] Fuego (D)	Deficiencia en la detección temprana y extinción de incendios, lo que aumenta el riesgo de que un incendio destruya los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-248	Salas	Instalación	Dpto. TI	[I.2] Daños por agua (D)	Posibilidad de daños causados por escapes, fugas o inundaciones, especialmente en áreas cercanas a los recursos del sistema, debido a sistemas de fontanería defectuosos o inadecuados.	Dpto. TI	1	1	2	**2**

RSK-249	Salas	Instalación	Dpto. TI	[I.3] Contaminación mecánica (D)	Exposición a vibraciones, polvo, suciedad, interferencias de radio, campos magnéticos, luz ultravioleta, y otros factores que pueden deteriorar o interferir con los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-250	Salas	Instalación	Dpto. TI	[I.4] Contaminación electromagnética (D)	Exposición a interferencias de radio, campos magnéticos, luz ultravioleta y otros fenómenos electromagnéticos que pueden provocar perturbaciones en los sistemas electrónicos y afectar su funcionamiento normal.	Dpto. TI	1	1	2	**2**
RSK-251	Salas	Instalación	Dpto. TI	[I.6] Corte del suministro eléctrico (D)	Interrupción en el suministro de energía eléctrica, lo que resulta en la falta de alimentación de potencia y la incapacidad de operar los recursos del sistema.	Dpto. TI	1	1	5	**5**
RSK-252	Salas	Instalación	Dpto. TI	[I.7] Condiciones inadecuadas de temperatura o humedad (D)	Falta de control adecuado sobre las condiciones ambientales, como temperatura y humedad, lo que puede afectar negativamente la funcionalidad y la integridad de los recursos del sistema.	Dpto. TI	1	1	2	**2**
RSK-253	Salas	Instalación	Dpto. TI	[A.11] Acceso no autorizado (D)	Deficiencias en los controles físicos de acceso y en las políticas y procedimientos de seguridad, que podrían permitir el acceso no autorizado a las instalaciones y la realización de actos destructivos por parte de personal interno o externo.	Dpto. TI	1	1	5	**5**
RSK-254	Salas	Instalación	Dpto. TI	[A.26] Ataque destructivo (D)	Riesgo de actos de vandalismo, terrorismo, o acción militar que podrían resultar en la destrucción deliberada de los recursos del sistema, llevados a cabo por individuos internos o externos a la organización.	Dpto. TI	1	1	5	**5**

Tabla 0-15. Riesgo actual.
Fuente: Elaboración propia.

Anexo XIV. Riesgo no aceptable

IDENTIFICADOR	NOMBRE DEL ACTIVO	CATEGORÍA DEL ACTIVO	PROPIETARIO DEL ACTIVO	AMENAZA	VULNERABILIDAD	PROPIETARIO DEL RIESGO	VALOR ACTIVO	FRECUENCIA DE LA AMENAZA ACTUAL	IMPACTO DE LA AMENAZA ACTUAL	NIVEL RIESGO ACTUAL
RSK-001	Información financiera	Datos	Jefe Administrativo y Financiero	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Jefe Administrativo y Financiero	5	3	4	**60**
RSK-002	Información financiera	Datos	Jefe Administrativo y Financiero	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Jefe Administrativo y Financiero	5	2	5	**50**
RSK-003	Información financiera	Datos	Jefe Administrativo y Financiero	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Jefe Administrativo y Financiero	5	2	5	**50**
RSK-005	Información financiera	Datos	Jefe Administrativo y Financiero	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de esta, ya sea por acciones maliciosas o accidentales.	Jefe Administrativo y Financiero	5	2	5	**50**
RSK-007	Propiedad intelectual	Datos	Director Ejecutivo	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Director Ejecutivo	4	3	4	**48**
RSK-013	Datos de los empleados	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Responsable de Administración (RRHH) / Contabilidad / Comercial	4	3	4	**48**
RSK-019	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	3	4	**60**

RSK-020	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	5	**50**
RSK-021	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	5	**50**
RSK-023	Datos de los clientes	Datos	Responsable de Administración (RRHH) / Contabilidad / Comercial	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de esta, ya sea por acciones maliciosas o accidentales.	Responsable de Administración (RRHH) / Contabilidad / Comercial	5	2	5	**50**
RSK-025	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Jefes de Proyectos de Traducción e Interpretación	5	3	4	**60**
RSK-026	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Jefes de Proyectos de Traducción e Interpretación	5	2	5	**50**
RSK-027	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Jefes de Proyectos de Traducción e Interpretación	5	2	5	**50**
RSK-029	Proyectos de traducción e interpretación	Datos	Jefes de Proyectos de Traducción e Interpretación	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de esta, ya sea por acciones maliciosas o accidentales.	Jefes de Proyectos de Traducción e Interpretación	5	2	5	**50**

RSK-068	Sistema operativo	Software	Dpto. TI	[A.5] Suplantación de la identidad del usuario (I) (C)	Cuando un atacante logra hacerse pasar por un usuario autorizado, obteniendo acceso a sus privilegios y utilizándolos para sus propios fines. Este tipo de amenaza puede ser ejecutada por personal interno, externo a la organización o contratado temporalmente.	Dpto. TI	5	3	3	**45**
RSK-070	Sistema operativo	Software	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	5	3	3	**45**
RSK-116	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Dpto. TI	5	3	4	**60**
RSK-117	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Dpto. TI	5	2	5	**50**
RSK-118	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Dpto. TI	5	2	5	**50**
RSK-119	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	5	3	3	**45**

RSK-121	Almacenamiento de archivos compartidos	Carpeta de red	Dpto. TI	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de esta, ya sea por acciones maliciosas o accidentales.	Dpto. TI	5	2	5	**50**
RSK-125	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.15] Alteración accidental de la información [I]	Accidentalmente, un empleado modifica datos críticos en una base de datos mientras realiza tareas de mantenimiento.	Dpto. TI	5	3	4	**60**
RSK-126	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.18] Destrucción de la información (D)	Un fallo técnico no detectado borra por completo los archivos de una carpeta compartida, resultando en la pérdida de información valiosa.	Dpto. TI	5	2	5	**50**
RSK-127	Archivos de configuración de red	Carpeta de red	Dpto. TI	[E.19] Fugas de información (C)	Un empleado envía por error un correo electrónico a destinatarios incorrectos, revelando información confidencial.	Dpto. TI	5	2	5	**50**
RSK-128	Archivos de configuración de red	Carpeta de red	Dpto. TI	[A.11] Acceso no autorizado (D) (I) (C)	Cuando un atacante logra acceder a los recursos del sistema sin tener la autorización correspondiente, generalmente aprovechando fallos en los sistemas de identificación y autorización.	Dpto. TI	5	3	3	**45**
RSK-130	Archivos de configuración de red	Carpeta de red	Dpto. TI	[A.18] Destrucción de la información (D)	Eliminación intencionada de datos e información almacenados, con el fin de causar daño o pérdida de esta, ya sea por acciones maliciosas o accidentales.	Dpto. TI	5	2	5	**50**

Tabla 0-16. Riesgo no aceptable.
Fuente: Elaboración propia