PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Escuela de Posgrado

Gestión de riesgos de seguridad de información, bajo el estándar ISO/IEC 27005:2022, aplicando ontologías de dominio

Tesis para obtener el grado académico de Maestro en Informática con mención en Ciencias de la Computación que presenta:

Daniel Elías Santos Llanos

Asesores:

Ian Paul Brossard Núñez
César Armando Beltrán Castañón

Lima, 2024

Informe de Similitud

Yo, ***Ian Paul BROSSARD NUÑEZ***, docente de la Escuela de Posgrado de la Pontificia Universidad Católica del Perú, asesor de la tesis titulada "GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN, BAJO EL ESTÁNDAR ISO/IEC 27005:2022, APLICANDO ONTOLOGÍAS DE DOMINIO" de el autor Daniel Elías Santos Llanos, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 18%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 22/07/2024.
- He revisado con detalle dicho reporte y la tesis, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha:

San Miguel, 22 de Julio de 2024.

Apellidos y nombres del asesor: ***BROSSARD NUÑEZ, Ian Paul***	
DNI: 46134777	Firma 
ORCID: 0000-0003-2073-3829	

Dedicatoria

A papá Rafael, que siempre estuvo presente para compartir su sabiduría, como maestro y protector.

A Zelenia, que construye todos los días el futuro, con amor.

A los Basurto y sus descendientes, cuyas manos cálidas y generosas construyeron el camino que me permitió llegar hasta aquí.

Agradecimientos

A los docentes de la Maestría en Informática, por su guía en la presente investigación.

A los colegas maestros y futuros maestros con los que compartimos camino en estos años de estudios, especialmente a: Carlos Rebaza, John Barrera y Alipio Laboriano.

Finalmente, por su colaboración en la presente investigación, a los colegas especialistas de la comunidad de seguridad de información del Perú e Hispanoamérica.

Resumen

El proceso de gestión de riesgos, en el dominio específico de la seguridad de información, es una labor compleja pero necesaria para prevenir eventos adversos que perjudiquen a las organizaciones. Bien por obligaciones regulatorias o porque se requiere propiciar el logro de los objetivos estratégicos, la gestión de riesgos de seguridad de información (GRSI) se ha convertido en un proceso necesario y recurrente.

El desarrollo de una GRSI se fundamenta en normas locales e internacionales que establecen protocolos, actividades y criterios, que establecen diversos conceptos que guardan relaciones complejas en sus términos y taxonomías. En consecuencia, se requieren especialistas experimentados para ejecutar este proceso de manera competente. Esto, a su vez, ocasiona que los resultados de este proceso estén intrínsecamente expuestos a la subjetividad e influencia de las personas que lo realizan.

En esta tesis se propone e implementa un proceso de gestión de riesgos de seguridad de información, basado en una ontología de dominio, cuyo corpus está basado en los términos establecidos en los estándares ISO de seguridad de información, las normas técnicas peruanas afines y otras regulaciones internacionales relacionadas.

Como resultado de la investigación aplicada se ha comprobado que es posible estructurar los conceptos y taxonomías sobre los dominios de gestión de riesgos y seguridad de la información, en una ontología integrada. Esta ha sido implementada, para guiar y automatizar, mediante una solución informática, la ejecución de una GRSI, de manera que se han mitigado la subjetividad y los errores de consistencia en los resultados de este proceso.

Palabras clave: gestión de riesgos, seguridad de información, ciberseguridad, ontología, ingeniería del conocimiento.

Índice General

Índice de Tablas

Índice de Figuras

Introducción

En la actualidad, el proceso de “Gestión de Riesgos de Seguridad de Información” (GRSI) se realiza utilizando como referentes a estándares que establecen los lineamientos para realizar una adecuada evaluación y tratamiento de riesgos. Se destaca la norma internacional ISO/IEC 27005:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad. Guía sobre la gestión de riesgos de seguridad de la información” [20] y, localmente, su traducción al español en la Norma Técnica Peruana NTP ISO/IEC 27005:2022 [34].

Debido a la complejidad taxonómica de los términos contenidos en las normas de GRSI, estas se sustentan en otros marcos complementarios que contienen glosarios de términos que facilitan su entendimiento. Entre las normas ISO de seguridad de información podemos referir a la ISO/IEC 27000:2018 “Sistemas de gestión de seguridad de la información. Descripción general y vocabulario” [15].

En resumen, se cuenta con metodologías que establecen las etapas y actividades para el proceso de GRSI, pero también con diccionarios que detallan los términos que aquellas utilizan. Sin embargo, la conjunción de ambas fuentes de conocimiento es compleja pues, mientras las primeras establecen algoritmos y protocolos generales sobre la gestión de riesgos, las segundas proponen una descripción específica de los términos empleados y algunas de las relaciones que existen entre estos.

Esta brecha entre los procedimientos y la complejidad de sus conceptos y relaciones es atendida por los especialistas en seguridad de información. En consecuencia, la GRSI se hace dependiente del factor humano, cuya subjetividad inherente podría generar la distorsión de los resultados obtenidos, comprometiendo su calidad y la consecuente efectividad de las decisiones tomadas, producto de la GRSI.

La presente investigación propone una solución que mitiga la distorsión de los resultados de la GRSI, mediante la aplicación de ontologías de dominio sobre este proceso, con una lógica de consistencia permanente. De esta manera, el modelado de los términos usados en la gestión de riesgos, bajo una estructura ontológica de clases, instancias y relaciones, así como su posterior automatización mediante un software de registro y consulta, limitarán la posibilidad de errores incurridos por los gestores de riesgos.

En el capítulo 1 se propone el problema que ha originado la investigación, así como también el marco conceptual necesario para su comprensión. Este marco comprende las definiciones de la gestión de riesgos, gobierno de la seguridad de información y su unión en la gestión de riesgos de la seguridad de información; además, se presentan las normas utilizadas para investigar este tema, así como también las ontologías de dominio y su aplicación a la seguridad de información, expuesta mediante algunos ejemplos.

En el capítulo 2 se desarrollan las generalidades de la investigación, que comprenden: el objetivo general y los objetivos específicos, los resultados esperados de la investigación, los métodos y procedimientos utilizados en para desarrollarla, la justificación del enfoque utilizado para resolver el problema, así como también el alcance de la solución propuesta.

En el capítulo 3 se presenta la ejecución de la revisión sistemática. Inicia con el "planeamiento de la revisión", el diseño del proceso de búsqueda (preguntas de investigación, términos y bases de datos consultadas), el proceso de selección inicial y final (criterios de selección y calidad), así como también el proceso de extracción de datos. Continúa con la etapa de "conducir la revisión", con la ejecución de la búsqueda, el proceso de selección y la extracción. El capítulo finaliza con la etapa de "reportar la revisión", con un resumen de la revisión realizada y la consecuente atención de las preguntas que fueron resueltas.

En el capítulo 4 se presenta el proceso de recolección de datos, mostrando las fuentes de información utilizadas para construir la ontología en cada una de las etapas del proceso de gestión de riesgos, así como también el método bajo el que fue compilada, estructurada y normalizada; complementando su presentación con ejemplos que facilitan el entendimiento de las clases y relaciones identificadas.

En el capítulo 5 se presenta el proceso de construcción de la ontología de gestión de riesgos de seguridad de información, detallando el procedimiento seguido, así como también las estrategias utilizadas para modelar la estructura de datos y su refinamiento, mediante la aplicación del método Delphi.

En el capítulo 6 se presenta el proceso de diseño, implementación y pruebas del Gestor de Riesgos de Seguridad de Información, como una herramienta informática que automatiza y dirige el proceso de gestión de riesgos de seguridad de información. Asimismo, se ha utilizado la opinión de especialistas para verificar que esta solución mitiga de manera efectiva la posibilidad de que se presenten errores en un proceso de gestión de riesgos de seguridad de información.

Finalmente, en el capítulo 7 se presentan las conclusiones obtenidas a partir de la investigación realizada, considerando el cumplimiento de los objetivos y las experiencias derivadas de estos; además, se proponen algunos trabajos futuros que podrían realizarse en temas relacionados o derivados de la presente investigación.

1. Problemática y marco conceptual

Este capítulo presenta el problema que ha originado la presente investigación, respecto al proceso del proceso de Gestión de Riesgos de Seguridad de Información (GRSI). Asimismo, se propone el marco conceptual que sirve de fundamento y sustento para el entendimiento de la tesis expuesta.

1.1. Problema

Relevancia de la seguridad de información y la gestión de riesgos como su herramienta de gobierno. La seguridad de información es un dominio crítico para la supervivencia de las organizaciones, pues, tal como afirmaba el profesor Von Solms [47] *"[…] la seguridad de la información vista como la disciplina para asegurar la confidencialidad, integridad y disponibilidad […] es hoy un aspecto de suma importancia en la gestión estratégica de cualquier compañía"*.

Dada su importancia, las entidades reguladoras han producido estándares para gobernar este ámbito de las organizaciones, tales como la norma americana NIST SP 800-100 [43]; el estándar internacional ISO/IEC 27001:2022 [18] o la norma técnica peruana NTP ISO/IEC 27001:2022 [32], entre otros.

Si bien cada uno de estos marcos cuentan con un enfoque particular, todos coinciden en que, para gobernar la seguridad de información, es necesario aplicar un proceso de gestión de riesgos, tal como se muestra en la siguiente tabla:

Tabla 1. Referencias a GRSI en las normas de gobierno de la seguridad de información

Norma	Referencias a la Gestión de Riesgos
Norma americana NIST SP 800-100 "Information Security Handbook: A guide for Managers".	Capítulo 10 "Gestión de Riesgos"
Estándar internacional ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements".	6.1 Acciones para abordar riesgos y oportunidades 8.2. Evaluación de riesgos de seguridad de información 8.3 Tratamiento de riesgos de seguridad de información
Norma Técnica Peruana ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información". Aplicable a las instituciones del sector público.	6.1 Acciones para abordar riesgos y oportunidades 8.2. Evaluación de riesgos de seguridad de información 8.3 Tratamiento de riesgos de seguridad de información

Fuente: Elaboración propia.

Cabe destacar que, el estándar ISO 27001 [18] precisa la relevancia de la gestión de riesgos en los siguientes términos:
"El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente."
[Subrayado propio]

Complejidad del proceso de gestión de riesgos de seguridad de información. Debido a su relevancia dentro del dominio de la seguridad de información, el proceso de GRSI cuenta a su vez con guías metodológicas. Por ejemplo, si bien en la norma ISO/IEC 27001:2022 [18] se establece la obligación de implementar un proceso de gestión de riesgos, esta labor es especificada en la ISO/IEC 27005:2022 [20], estándar donde se desarrollan detalladamente las etapas y actividades a realizar para lograrlo:

Tabla 2. Proceso de gestión de riesgos según la ISO/IEC 27005

Proceso según la ISO 27005		**Resumen del contenido de la norma**
Cláusula 6. Establecer el Contexto		Se establece el alcance de la gestión de riesgos (organización), realizar un entendimiento de las características de la organización (su información, requisitos, propiedades y activos), así como definir sus criterios y umbrales (apetito de riesgos).
Cláusula 7.1. Evaluación de Riesgos	**Cláusula 7.2** Identificar Riesgos	Se usan los activos de información listados como base para identificar posibles amenazas y vulnerabilidades, constituyendo riesgos, para cada uno de los cuáles se define un propietario del riesgo.
	Cláusula 7.3 Analizar Riesgos	Se cuantifica la probabilidad y consecuencias (impacto) de los riesgos identificados, aplicando los criterios previamente establecidos.
	Cláusula 7.4 Valorar Riesgos	Se determina el valor del riesgo, priorizando aquellos que son más significativos según el apetito de riesgo de la organización.
Cláusula 8. Tratamiento Riesgos		Se toman los riesgos más significativos, resultantes de la evaluación del riesgo y se plantean planes de tratamiento con las consecuentes medidas de remediación (controles), estableciendo responsables, plazos y recursos que permitan mitigarlos.

Fuente: Elaboración propia a partir del estándar ISO/IEC 27005:2022.

En síntesis, el proceso de GRSI comprende la aplicación de conceptos diversos relacionados entre sí, en cada una de sus etapas, constituyendo una ontología compleja de conceptos y relaciones.

En la siguiente tabla se presenta un ejemplo simplificado, basado en el contexto, evaluación y tratamiento de un riesgo, donde se evidencia cómo algunos de los términos referidos se relacionan entre sí para establecer y gestionar los riesgos:

Tabla 3. Ejemplo simplificado de GRSI y algunos conceptos relacionados

Etapa		**Concepto**	**Ejemplo**	**Ejemplo – Resultante**
1. Evaluación	**1.1 Identificación**	**Amenaza**	Fallo de dispositivo [del]	**Riesgo:** Fallo de dispositivo [del] Servidor SRV001 [que contiene la] Cartera de Clientes [debido al] insuficiente mantenimiento [afectando la] Integridad [de la información].
		Activo de información	Servidor SRV001 [que contiene la]	
		Información	Cartera de Clientes [debido al]	
		Vulnerabilidad	insuficiente mantenimiento [afectando la]	
		Propiedad de la Seg. de Inf.	Integridad [de la información]	
		Propietario del Riesgo	Responsable de administrar el activo	Departamento de infraestructura TI
	1.2 Análisis	**Controles [y sus estados]**	7.13 Mantenimiento de Equipos	Plan de mantenimiento periódico de equipos [implementado]
			6.3 Concientización en seguridad de información	Sensibilización a personal de infraestructura TI [implementado mejorable]
		Probabilidad (P)	2. Baja	Ha ocurrido alguna vez en la entidad.
		Impacto (I)	5. Muy Alta	Puede afectar la operatividad de toda la entidad.
	1.3 Valoración	**Valor del riesgo**	Función (P; I) = 3. Alta	Requiere tratamiento
2. Tratamiento		**Opción de tratamiento**	Estrategia 2	Modificar el riesgo [ISO 27005:2022 - numeral 8.2]
		Controles para tratamiento [y acciones]	8.13 Respaldo de información	Plan de respaldos de información en servidores [implementar]
			6.3 Concientización en seguridad de información.	Charla de sensibilización a personal de infraestructura TI [mejorar alcance]

Fuente: Elaboración propia, en base a las definiciones de los estándares ISO 27000 e ISO 27005.

Subjetividad de los especialistas responsables de la gestión de riesgos. Dada la complejidad inherente a la gestión de riesgos de seguridad de información, este proceso suele ser realizado por personal muy especializado. Tal como afirma Haqaf [84], las habilidades de estos expertos comprenden al menos 5 categorías:
"Hay muchas habilidades que pueden derivarse de los estándares, marcos y literatura para los profesionales de seguridad de la información. […] los autores propusieron cinco grupos principales, de la siguiente manera:
-Categoría A: Habilidades técnicas
-Categoría B: Habilidades de gestión de proyectos / procesos
-Categoría C: Habilidades de gestión de riesgos
-Categoría D: Habilidades de negocios
-Categoría E: Habilidades esenciales de seguridad de la información"

Sin embargo, incluso si estos requisitos son alcanzados por un especialista competente, existen investigadores que consideran que este proceso está expuesto de manera intrínseca a un margen de "error humano". Citamos a Slovic [45], quién refiere que las evaluaciones de riesgos son inevitablemente subjetivas:
"[…] La investigación ha comenzado a proporcionar una nueva perspectiva sobre este problema al demostrar la complejidad del concepto de "riesgo" y las insuficiencias de la visión tradicional de la evaluación de riesgos como una empresa puramente científica. […] La evaluación de riesgos es inherentemente subjetiva y representa una combinación de ciencia y juicio con importantes factores psicológicos, sociales, culturales y políticos. […] Quien controla la definición de riesgo controla la solución racional al problema en cuestión. Si el riesgo se define de una manera, entonces una opción ascenderá a la cima como la más rentable o la más segura o la mejor. Si se define de otra manera, tal vez incorporando características cualitativas y otros factores contextuales, es probable que se obtenga un orden diferente de soluciones de acción. Definir el riesgo es, por lo tanto, un ejercicio de poder. […] El público no es irracional. Sus juicios sobre el riesgo están influenciados por la emoción y el afecto de una manera que es a la vez simple y sofisticada. Lo mismo es válido para los científicos."
[Subrayado propio]

Si bien la afirmación de Slovic se refiere a la "gestión de riesgos", como proceso general, se podría extrapolar esta problemática al caso específico de la "gestión de riesgos de seguridad de información".

Para analizar la aplicabilidad de esta afirmación se realizó un cuestionario a especialistas en seguridad de información, poniendo como condición única el haber participado, en los últimos 10 años, en al menos 5 gestiones de riesgos de este dominio con un rol principal, tal como: oficial de seguridad, consultor o gestor responsable de la actividad.

En consecuencia, se han formulado preguntas sobre el conocimiento de estos profesionales respecto a la influencia del gestor responsable en las etapas de evaluación y tratamiento de riesgos, así como también algunas consultas generales respecto del proceso, tal como se muestra:

Tabla 4. Cuestionario y resultados sobre las actividades de GRSI

#	Evaluación del Riesgo	Resultado
1	¿La calidad de la evaluación de riesgos depende principalmente de la experiencia del responsable?	Si: 12; No: 0
2	¿Los procesos de evaluación de riesgos de SI que ha dirigido han sido siempre completamente objetivos?	Si: 5; No: 7
3	En retrospectiva ¿Puede haber cometido un error al evaluar un riesgo de SI (identificar, analizar o valorar)?	Si: 10; No: 2
4	En la etapa de identificación de los riesgos (definir los riesgos) ¿Qué error sería el más común?	Omisión de riesgos: 6 Riesgos mal definidos: 5 Otros: 1 [Influencia negativa de interesados]
5	En la etapa de análisis de los riesgos (definir la probabilidad e impacto) ¿Qué error sería el más común?	Estimación irreal (optimista): 7 Estimación irreal (pesimista): 4 Otros: 1 [Influencia negativa de interesados]
6	En la etapa de valoración de los riesgos (definir los riesgos no aceptables) ¿Qué error sería el más común?	Error de cálculo respecto a los criterios: 12 Otros: 0
#	**Tratamiento del Riesgo**	**Resultado**
7	¿La calidad del tratamiento de riesgo depende de la experiencia del responsable?	Si: 12; No: 0
8	¿Los procesos de tratamiento de riesgos de SI que ha dirigido han sido siempre completamente objetivos?	Si: 2; No:10
9	En retrospectiva ¿Puede haber cometido un error al tratar un riesgo de SI (proponer controles)?	Si: 12; No: 0
10	En la etapa de tratamiento de los riesgos (definir los controles para mitigar riesgos) ¿Qué error sería el más común?	Propuesta de tratamiento inviable: 2 Propuesta de tratamiento incoherente: 10 Otros: 0
#	**Generalidades**	**Resultado**
11	¿Cuál sería el aporte más valioso de una solución informática que automatice la GRSI?	Evitar errores de consistencia: 7 Prevenir omisiones: 2 Agilizar el proceso: 0 Otros: 3 [Orientar al responsable en cada paso]
12	Considerando las alternativas propuestas por la ISO 27005. ¿Cuál es en su opinión el mejor enfoque para evaluar riesgos?	Basado en Activos: 12 Basado en Eventos: 0
13	¿Qué estándar o metodología recomienda como marco referencial para la gestión de riesgos de seguridad de información?	Familia ISO 27000: 11 MAGERIT: 1
14	En una escala del 1 (Muy Bajo) al 5 (Muy Alto) ¿Qué tan confidenciales son para su organización los registros del proceso de GRSI?	Muy Alto: 10; Alto: 2

Fuente: Elaboración propia.

De los resultados obtenidos, se puede concluir que el proceso de gestión de riesgos es complejo y que, en cada una de sus etapas (evaluación, tratamiento), se pueden presentar fallos principalmente relacionados al error humano y la subjetividad de los especialistas que lo realizan. A partir de esta situación expuesta, se plantea el problema.

Planteamiento del Problema. El proceso de gestión de riesgos de seguridad de información es complejo, motivo por el cual debe ser atendido por especialistas en materia de seguridad de información. Sin embargo, esto propicia posibles distorsiones en los resultados de la evaluación y tratamiento de riesgos, ya sea por errores involuntarios o por la subjetividad del responsable.

A partir del problema identificado, la presente tesis propone como solución una ingeniería de ontologías que permita reducir el margen de error de una gestión de riesgos de seguridad de información, con un enfoque basado en activos, mitigando la influencia de la subjetividad y margen de error intrínsecos del personal responsable de realizar este proceso.

1.2. Marco conceptual

Dada la complejidad del proceso de gestión de riesgos de seguridad de información es necesario realizar precisiones respecto a los conceptos que son establecidos en las normas relacionadas a este dominio del conocimiento.

1.2.1. Gestión de riesgos

El estándar ISO 31000 [17] "Gestión del Riesgo. Principios y Directrices" establece un marco general para la gestión de riesgos y presenta las siguientes definiciones:
"3.1 Riesgo. Efecto de la incertidumbre sobre los objetivos […]
3.2 Gestión de riesgos: actividades coordinadas para dirigir y controlar la organización con relación al riesgo".
[Subrayado propio]

Asimismo, propone un modelo para gestionar los riesgos, según se detalla a continuación:

- **Planificar la Gestión de Riesgos.** Consiste en:
  - **Establecer el alcance y contexto de la gestión de riesgos:** Determinar los límites que tendrá la aplicación de la gestión de riesgos, a partir del conocimiento de las características más importantes de la entidad evaluada, así como los aspectos internos y externos que pueden afectarla.
  - **Establecer los criterios para la gestión de riesgos:** Determinar la metodología para valorar a los riesgos y los umbrales para definir si será aceptado o mitigado por la entidad.
- **Evaluar el riesgo.** Consiste en:
  - **Identificar el riesgo:** Determinar los riesgos que son aplicables a la organización y caracterizar los atributos que estos presentan.
  - **Analizar el riesgo:** Establecer la probabilidad e impacto del riesgo en base a la información de los atributos definidos, para determinar el nivel de riesgo.
  - **Valorar el riesgo:** Contrastar los resultados del nivel de riesgo obtenido con los umbrales establecidos en los criterios, para determinar qué riesgos requieren tratamiento y qué riesgos no.
- **Tratar el Riesgo.** Para los riesgos definidos como significativos (no aceptables) se genera un plan de trabajo con estrategias y controles que permitan mitigarlos a un nivel aceptable.

Cabe destacar que este enfoque es referenciado por la ISO/IEC 27001 [18] como fuente para establecer el contexto de la organización, además de identificar, evaluar y tratar los riesgos y oportunidades de seguridad de información.

1.2.2. Gobierno de seguridad de la información

El estándar ISO/IEC 27000 [15] presenta las siguientes definiciones a destacar:

- *"3.28 Seguridad de información. La preservación de la confidencialidad, integridad y disponibilidad de la información".*
- *"3.10 Confidencialidad. propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados".*
- *"3.36 Integridad. propiedad de exactitud y completitud".*
- *"3.7 Disponibilidad. propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada".*
- *"3.23 Gobierno de la seguridad de la información. Sistema mediante el cual se dirigen y controlan las actividades de seguridad de la información de una organización."*

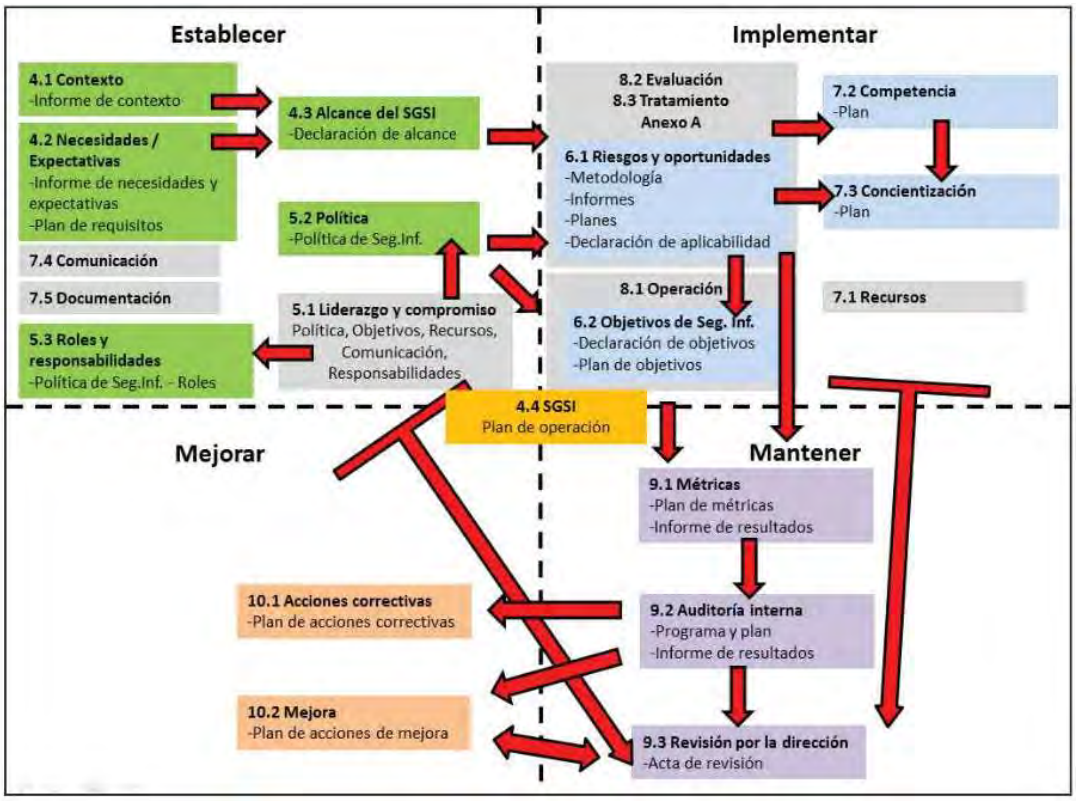
Al integrar las primeras definiciones, puede entenderse que la "seguridad de información" es la salvaguarda de la exposición (confidencialidad), alteración (integridad) o destrucción (disponibilidad) de la información. Sin embargo, esta definición carece de importancia práctica si no se enmarca en el "Gobierno de la Seguridad de Información".

A continuación, se listan algunas regulaciones relevantes respecto a este dominio:

- Estándar NIST (National Institute of Standards and Technology) SP 800-100 "Information Security Handbook: A guide for Managers". [43]
- Estándar ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements". [18]
- Norma Técnica Peruana ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información". Aplicable a las instituciones del sector público. [32]
- "Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad" de la Superintendencia de Banca, Seguros y AFP del Perú (SBS), aplicable a todas las entidades públicas y privadas del sector financiero peruano. [42]

En el caso del estándar ISO/IEC 27001:2022 [18] se establece como mecanismo de gobierno un "Sistema de Gestión de la seguridad de la información" (SGSI) el cual propone diversos artefactos para administrar adecuadamente la salvaguarda de la información, según se muestra en la siguiente figura:

Figura 1. Artefactos y sus precedencias en un SGSI según el estándar ISO 27001



Fuente: Santos [44].

De la revisión a los componentes del SGSI, podemos identificar lo siguiente:

- Las actividades que comprenden la Gestión de Riesgos de Seguridad de Información se encuentran en el cuadrante “Implementar”, y comprenden la implementación de una metodología de GRSI y la consecuente generación de registros (informes y planes) que acrediten su aplicación.
- A diferencia de otras tareas y debido a su complejidad, la gestión de riesgos está normada en diversas secciones de la norma ISO 27001, las cuales, en su versión del 2022 son:
    - 6.1 Acciones para abordar riesgos y oportunidades
    - 8.2 Evaluación de riesgos de seguridad de la información
    - 8.3 Tratamiento de riesgos de seguridad de la información
    - Anexo A. Referencia de controles de seguridad de la información
- En el gráfico, el nodo de gestión de riesgos es fundamental porque recibe los elementos del establecimiento del sistema de gestión y permite generar los resultados para su mantenimiento y mejora.

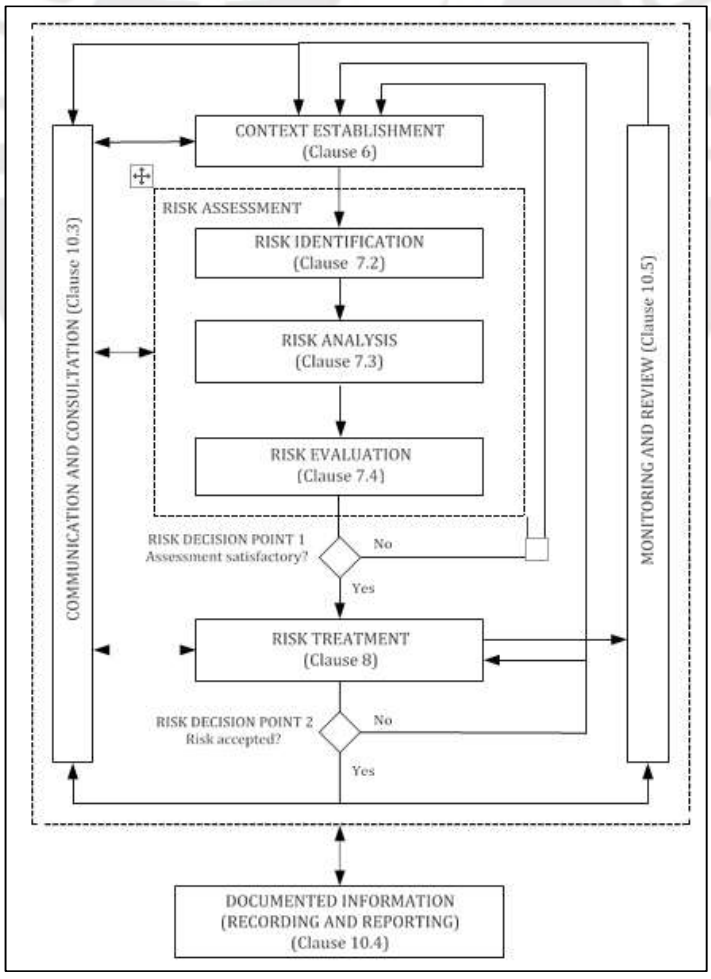
1.2.3. Gestión de riesgos de seguridad de la información

Los marcos normativos en gobierno de la seguridad de la información exigen que las organizaciones implementen y administren controles para prevenir los riesgos de seguridad de información.

Dadas las limitaciones para implementar todos los controles disponibles, las normas referidas establecen que, como parte del gobierno de la seguridad de información, se debe establecer una "gestión de riesgos de seguridad de información". Este proceso permite identificar qué riesgos son los más relevantes y qué medidas o controles exactos deben implementarse para mitigar sus efectos o, si fuera posible, evitarlos.

La norma específica para esta finalidad es la ISO/IEC 27005:2022 "Tecnología de Información. Técnicas de Seguridad. Gestión del Riesgo en Seguridad de Información" [20]. Este estándar propone un marco para la gestión de riesgos de seguridad de la información, bajo un enfoque que comprende las siguientes fases:

Figura 2. Proceso de gestión de riesgos, según la ISO 27005



Fuente: Estándar ISO 27005:2022 [20].

A continuación, se detalla el desarrollo de la actividad de gestión de riesgos de seguridad de la información, según lo establece la norma referida [20]:

- **Establecer el contexto.** Conocer la organización, sus aspectos y requisitos más relevantes; así como también los criterios de selección y aceptación de riesgos.
  Resultado esperado:
  - Alcance de la gestión de riesgos y entendimiento de la organización (inventario de información y sus activos).
  - Criterios metodológicos de medición y aceptación de riesgos.

- **Evaluar el riesgo.** Presenta tres etapas consecutivas, que son:
  - **Identificar el riesgo.**
    Encontrar, reconocer y describir los riesgos que podrían ayudar o impedir que una organización logre sus objetivos.
    Resultado esperado: Matriz de evaluación de riesgos (identificados y caracterizados). Para definir y acotar el riesgo de manera adecuada con los atributos de información, activo de información, amenaza y vulnerabilidad.

  - **Analizar el riesgo.**
    Comprender la naturaleza del riesgo y sus características, incluido, en su caso, el nivel de riesgo.
    Resultado esperado: Matriz de evaluación de riesgos (probabilidad e impacto cuantificados). Para determinar el nivel de riesgo.

  - **Valorar el riesgo.**
    Comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos para determinar si se requiere tomar acción.
    Resultado esperado: Matriz de evaluación de riesgos (priorizada). Divide a los riesgos en aceptables o no aceptables, de acuerdo con el apetito de riesgo de la organización.

- **Tratar los riesgos.** Seleccionar e implementar opciones y controles para abordar el riesgo, ya sea para evitarlo, mitigarlo, transferirlo o aceptarlo.
  Resultado esperado: Plan de tratamiento de riesgos. Establece las estrategias y controles que deben ser mejorados o construidos, así como también los responsables de su implementación.

1.2.4. Estándares sobre la seguridad de información y gestión de riesgos

Susanto [48] afirma que la ISO 27001 es el mayor referente en cuanto a normas para gestionar la seguridad de información: *"es como un lenguaje global en estándares […] en SGSI [Sistemas de Gestión de Seguridad de Información], tal como lo es el inglés como idioma internacional, con un nivel de usabilidad y alcance de confianza de más del 80 % del mundo".* Este estándar es complementado por un conjunto de normas, conocida como la "familia de normas 27000".

En el caso peruano, estas normas ISO cuentan han sido traducidas por el Instituto Nacional de Calidad (INACAL), con la denominación de Normas Técnicas Peruanas (NTP) [1-38] y son usadas en todas las entidades del sector público y en algunas entidades privadas. Se muestra la relación en el tiempo entre ambas fuentes:

Tabla 5. Estándares ISO y NTP referidos a la seguridad de información y gestión de riesgos

#	Estándar ISO	Norma Técnica Peruana	Referencia
1	ISO/IEC 17799:2000 Information technology — Code of practice for information security management. **Edición:** 1 **Publicación:** diciembre de 2000.	NTP-ISO/IEC 17799:2004 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. **Edición:** 1 **Publicación:** Resolución N° 0026-2004/CRT-INDECOPI, del 27 de marzo de 2004. **Uso obligatorio:** Resolución Ministerial N° 224-2004-PCM, del 23 de julio de 2004.	[1] [22] [35]
2	ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice for information security management. **Edición:** 2 **Publicación:** junio de 2005.	NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. **Edición:** 2 **Publicación:** Resolución N° 001-2007/INDECOPI-CRT, del 5 de enero de 2007. **Uso obligatorio:** Resolución Ministerial N° 246-2007-PCM, del 22 de agosto de 2007.	[2] [23] [36]
3	ISO/IEC 27001:2005 Information security management systems. Requirements. **Edición:** 1 **Publicación:** octubre de 2005.	NTP-ISO/IEC 27001:2008 EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. **Edición:** 1 **Publicación:** Resolución N° 42-2008/INDECOPI-CNB, del 11 de enero de 2009. **Uso obligatorio:** Resolución Ministerial N° 129-2012-PCM, del 23 de mayo de 2012.	[3] [24] [37]
4	ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management. **Edición:** 1 **Publicación:** junio de 2005.	Sin traducción.	[4]
5	ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management. **Edición:** 1 **Publicación:** junio de 2008	NTP-ISO/IEC 27005:2009 Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información. **Edición:** 1 **Publicación:** Resolución N° 29-2009/CNB-INDECOPI, del 7 de noviembre de 2009.	[5] [25]

#	Estándar ISO	Norma Técnica Peruana	Referencia
6	ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary. **Edición:** 1 **Publicación:** mayo de 2009	Sin traducción.	[6]
7	ISO 31000:2009 Risk management — Principles and guidelines. **Edición:** 1 **Publicación:** noviembre de 2009.	NTP-ISO 31000:2011 Gestión del riesgo. Principios y directrices. **Edición:** 1 (revisada el 2016) **Publicación:** Resolución Directoral Nº 032-2016-INACAL/DN. 16 de noviembre de 2016.	[7] [26]
8	ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management. **Edición:** 2 **Publicación:** junio de 2011.	Sin traducción.	[8]
9	ISO/IEC 27000:2012 Information technology — Security techniques — Information security management systems — Overview and vocabulary. **Edición:** 2 **Publicación:** diciembre de 2012.	Sin traducción.	[9]
10	ISO/IEC 27001:2013 Information security management systems. Requirements. **Edición:** 2 **Publicación:** octubre de 2013.	NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. **Edición:** 2 **Publicación:** Resolución Nº 129-2014/CNB-INDECOPI, del 20 de noviembre de 2014. **Uso obligatorio:** Resolución Ministerial N° 004-2016-PCM, del 8 de enero de 2016.	[10] [27] [38]
11	ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. **Edición:** 2 **Publicación:** octubre de 2013.	NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. **Edición:** 1 **Publicación:** Resolución Directoral Nº 056-2017-INACAL/DN, del 29 de diciembre de 2017	[11] [28]
12	ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary. **Edición:** 3 **Publicación:** enero de 2014.	Sin traducción.	[12]
13	ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary. **Edición:** 4 **Publicación:** febrero de 2016.	Sin traducción.	[13]
14	ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. **Edición:** 1 **Publicación:** noviembre de 2016.	NTP-ISO/IEC 27035-1:2019 Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1: Principios de la gestión de incidencias. **Edición:** 1 **Publicación:** Resolución Directoral Nº 029-2019-INACAL/DN, del 3 de enero de 2020.	[14] [29]
15	ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. **Edición:** 5 **Publicación:** febrero de 2018.	Sin traducción.	[15]
16	ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. **Edición:** 3 **Publicación:** julio de 2018.	NTP-ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información. **Edición:** 2 **Publicación:** Resolución Directoral Nº 047-2018-INACAL/DN, del 28 de diciembre de 2018. (publicado el 16 de enero de 2019)	[16] [30]

#	Estándar ISO	Norma Técnica Peruana	Referencia
17	ISO 31000:2018 Risk management — Guidelines. **Edición:** 2 **Publicación:** febrero de 2018.	NTP-ISO 31000:2018 Gestión del riesgo. Directrices. **Edición:** 2 **Publicación:** Resolución Directoral Nº 014-2018-INACAL/DN, del 2 de julio de 2018.	[17] [31]
18	ISO/IEC 27001:2022 Information security management systems. Requirements. **Edición:** 3 **Publicación:** octubre de 2022.	NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. **Edición:** 3 **Publicación:** Resolución Directoral N° 022-2022-INACAL/DN, del 29 de diciembre de 2022. **Uso obligatorio:** no establecido a la fecha.	[18] [32]
19	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. **Edición:** 3 **Publicación:** febrero de 2022.	NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. **Edición:** 2 **Publicación:** Resolución Directoral N° 022-2022-INACAL/DN, del 29 de diciembre de 2022.	[19] [33]
20	ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. **Edición:** 4 **Publicación:** octubre de 2022	NTP-ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. **Edición:** 3 **Publicación:** Resolución Directoral N° 022-2022-INACAL/DN, del 29 de diciembre de 2022.	[20] [34]
21	ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process. **Edición:** 2 **Publicación:** febrero de 2023	Sin traducción.	[21]

Fuente: Elaboración propia, en base a las publicaciones de los portales: "iso.org/home.html" y "busquedas.elperuano.pe", entre otras fuentes de diversas entidades del Estado Peruano, realizadas el día: 1 de marzo de 2023.

Para los fines de la presente investigación, se han seleccionado las últimas ediciones de las siguientes normas ISO:

- **ISO 31000:2018** Gestión del riesgo. Directrices. [17]
- **ISO/IEC 27000:2018** Generalidades y vocabulario. [15]
- **ISO/IEC 27001:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. [18]
- **ISO/IEC 27002:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. [19]
- **ISO/IEC 27005:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. [20]
- **ISO/IEC 270035-1:2023** Tecnología de la información - Gestión de incidentes de seguridad de la información Parte 1. Principios y procesos Principios y proceso. [21]

Asimismo, en base a lo referido por especialistas en la tabla 4, pregunta 13, se ha revisado la documentación de la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" (MAGERIT), en su última versión:

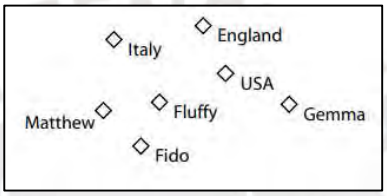
- **MAGERIT – versión 3.0 Libro I** Método. [39]
- **MAGERIT – versión 3.0 Libro II** Catálogo de Elementos. [40]
- **MAGERIT – versión 3.0 Libro III** Guía de Técnicas. [41]

1.2.5. Ontologías de dominio

Etimológicamente, las ontologías surgen como una rama filosófica que estudia las entidades y sus relaciones. Si bien esta puede parecer abstracta, su aplicación en el campo de las ciencias de la computación aporta un enfoque práctico para la resolución de problemas. Para que sean útiles, estas abstracciones son modeladas bajo un esquema organizado. Horridge [46] establece tres componentes básicos que presenta una ontología:

- **Individuos.** También conocidos como instancias, representan objetos en un dominio específico.

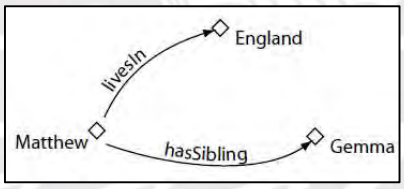
Figura 3. Representación de individuos



Fuente: Horridge [46].

- **Propiedades.** Son relaciones entre individuos, todas son binarias; sin embargo, solo en algunos casos pueden ser inversas, transitivas o simétricas.

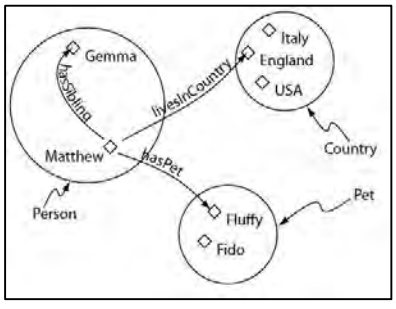
Figura 4. Representación de propiedades



Fuente: Horridge [46].

- **Clases.** También llamadas conceptos, son conjuntos de individuos. Es decir, son una representación concreta de conceptos.

Figura 5. Representación de clases



Fuente: Horridge [46].

1.2.6. Ontologías de dominio aplicadas a la seguridad de información

Respecto a la aplicación de ontologías de dominio al campo de la GRSI, podemos destacar la siguiente terminología definida por el estándar ISO 27000:2018 [15] y cuyas relaciones son estructuradas a partir del estándar ISO 27005:2022 [20].

Etapa: Establecer el Contexto

- Organización (Alcance)
- Información
    - Requisito de Seguridad de Información
        - Propiedad de Seguridad de Información
- Activo de Información
    - Tipo de Activo

Etapa: Evaluación de Riesgos

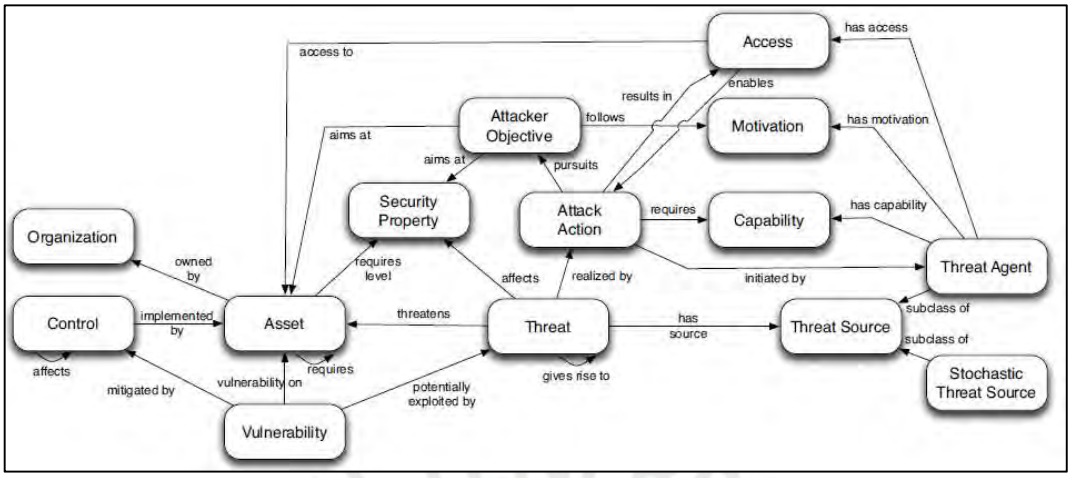
- Activo de Información
- Amenaza
    - Tipo de Amenaza
- Vulnerabilidad
    - Tipo de Vulnerabilidad
- Riesgo
    - Propietario del Riesgo
- Control
    - Tipo de Control
- Valor del riesgo
    - Probabilidad
    - Impacto

Etapa: Tratamiento de Riesgos

- Opción de tratamiento
- Control en tratamiento
- Plan de Tratamiento
    - Acción de tratamiento
    - Responsable
    - Plazos de implementación
    - Recursos

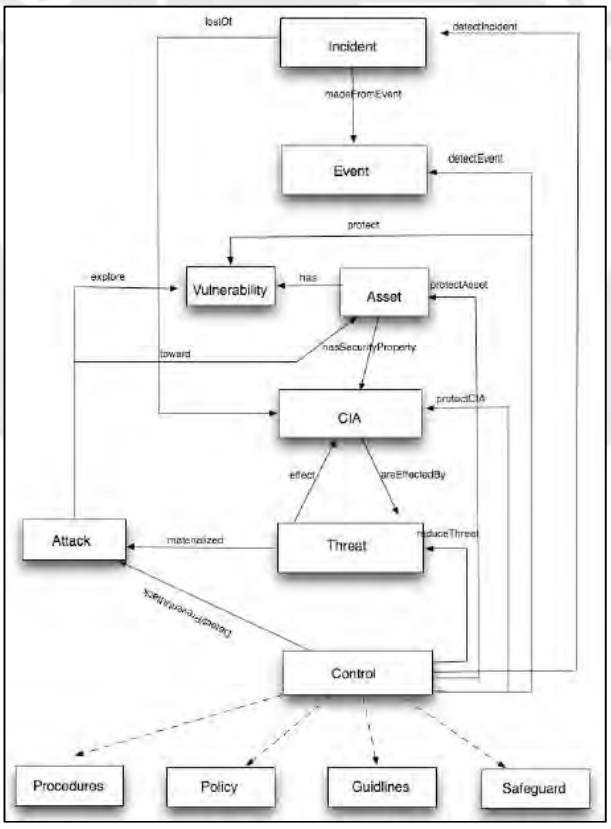
Cabe destacar que, como resultado de la investigación del estado del arte (capítulo 3 de esta investigación), se han identificado distintas propuestas de ontologías de seguridad de información que utilizan algunos de los términos listados. Aquellos que son más significativos son mostrados a continuación:

Figura 6. Ontología de riesgos de seguridad de información propuesta por Kiesling



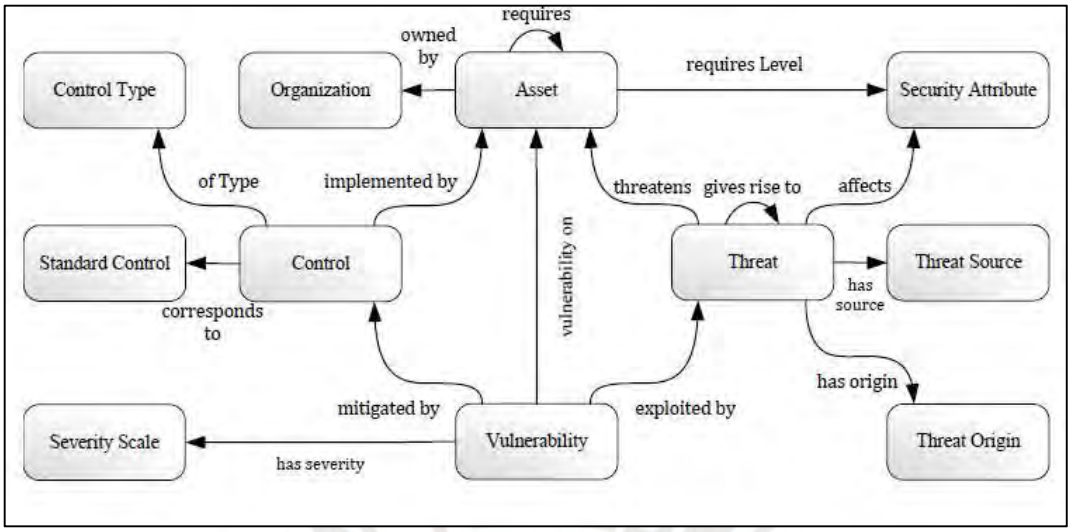
Fuente: Kiesling [54].

Figura 7. Ontología de riesgos de seguridad de información propuesta por Pereira



Fuente: Pereira [57].

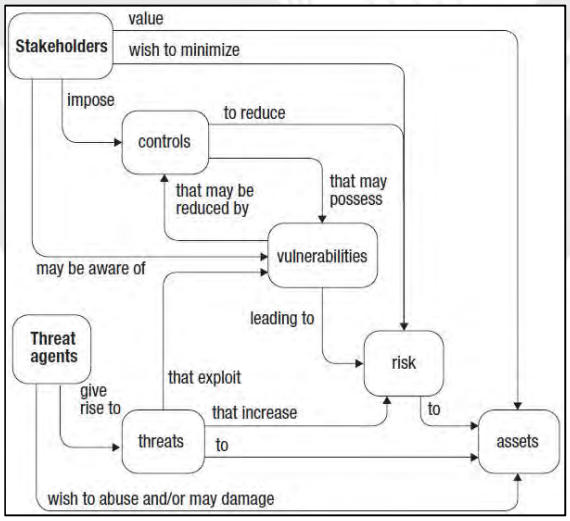
Figura 8. Ontología de riesgos de seguridad de información propuesta por Fenz



Fuente: Fenz [73].

Asimismo, como resultado de la revisión de los estándares de la familia ISO 27000, se ha identificado que en el estándar ISO/IEC 27032:2012 [85] existía un modelo gráfico de las dependencias entre los conceptos ligados a la gestión de riesgos. Cabe precisar que, en la versión más reciente de esta norma [86], este gráfico ha sido retirado:

Figura 9. Ontología propuesta en la ISO 27032:2012



Fuente: ISO 27032:2012 [85].

En los capítulos 4 y 5 de la presente investigación se desarrolla el proceso de diseño y construcción de la ontología propuesta para implementar la solución.

2. Generalidades

Este capítulo presenta el objetivo general de la investigación, así como también los objetivos específicos de cada una de las etapas del proceso de Gestión de Riesgos de Seguridad de Información (GRSI). En base a ello, se proponen los resultados esperados, así como también los métodos, procedimientos y tecnologías a emplear, concluyendo con una breve exposición de los motivos que justifican la presente investigación y sustentan su relevancia.

2.1. Objetivo general

Diseñar e implementar un proceso de gestión de riesgos de seguridad de información, basado en estándares internacionales, aplicando una solución basada en ontologías de dominio del área de ciencias de la computación.

2.2. Objetivos específicos

Dado el objetivo general propuesto, se ha preparado un proyecto para lograrlo, el cual consiste en las siguientes actividades:

- Obtener información para la ontología.
- Construir la ontología en un modelo de datos.
- Construir una aplicación que permita usar el modelo.
- Verificar que los resultados de la solución sean correctos.

En consecuencia, se plantean los siguientes objetivos específicos de la investigación:

Tabla 6. Objetivos específicos de la investigación

#	Objetivo específico
OE1	Recopilar los conceptos y relaciones alrededor del dominio semántico de un proceso de GRSI, para construir su base ontológica.
OE2	Modelar una ontología, utilizando los conceptos y relaciones recopilados, para construir el soporte de datos del proceso de GRSI.
OE3	Implementar una aplicación informática, que permita explotar la ontología modelada, para dar lugar a un proceso de GRSI.
OE4	Validar que la conjunción del modelo y la aplicación informática implementada mitiguen el margen de error humano sobre el proceso de GRSI.

Fuente: Elaboración propia.

Es decir, los objetivos específicos han sido establecidos a partir de la intención de lograr cumplir con el objetivo general.

2.3. Resultados esperados

Para definir los resultados esperados se han tomado los objetivos de la investigación como eje del desarrollo del proyecto. Sin embargo, dado que estos objetivos se desarrollan respecto a la GRSI, se han tomado en cuenta también las etapas de este proceso que, según el estándar ISO 27005:2022 [20] y tal como se expuso en el capítulo anterior, presenta las siguientes etapas:

- Establecer el contexto
- Evaluar el riesgo
- Tratar los riesgos

Es decir, cada resultado esperado se constituye como parte del logro de un objetivo, permitiendo a su vez la implementación del proceso de GRSI, tal como se muestra en la siguiente tabla:

Tabla 7. Resultados esperados del proyecto de investigación

Resultados esperados			
Objetivos de Tesis	**Etapas de la GRSI**		
	Etapa 1: Establecer el Contexto.	**Etapa 2:** Evaluar el Riesgo.	**Etapa 3:** Tratar el Riesgo.
OE1 Recopilar los conceptos y relaciones alrededor del dominio semántico de un proceso de GRSI, para construir su base ontológica.	Información organizada de clases y relaciones sobre "establecer el contexto".	Información organizada de clases y relaciones sobre "evaluar riesgos de seguridad de información".	Información organizada de clases y relaciones sobre "tratar riesgos de seguridad de información".
OE2 Modelar una ontología, utilizando los conceptos y relaciones recopilados, para construir el soporte de datos del proceso de GRSI.	Ontología de dominio que representa los componentes para "establecer el contexto".	Ontología de dominio que representa los componentes para "evaluar riesgos de seguridad de información".	Ontología de dominio que representa los componentes para "tratar riesgos de seguridad de información".
OE3 Implementar una aplicación informática, que permita explotar la ontología modelada, para dar lugar a un proceso de GRSI.	Solución que implementa un módulo de "establecer el contexto".	Solución que implementa un módulo de "evaluar riesgos de seguridad de información".	Solución que implementa un módulo de "tratar riesgos de seguridad de información".
OE4 Validar que la conjunción del modelo y la aplicación informática implementada mitiguen el margen de error humano sobre el proceso de GRSI.	Conformidad sobre los resultados de prueba del módulo de "establecer el contexto".	Conformidad sobre los resultados de prueba del módulo de "evaluar riesgos de seguridad de información".	Conformidad sobre los resultados de prueba del módulo de "tratar riesgos de seguridad de información".

Fuente: Elaboración propia.

2.4. Métodos y procedimientos

Método de investigación. Para iniciar la investigación se ha realizado una revisión del estado del arte, realizada mediante una adaptación del método de Kitchenham establecido en la "Guía para realizar revisiones sistemáticas de la literatura", que contiene los procedimientos de búsqueda y selección de las investigaciones que pueden aportar información a la presente tesis.

Método de gestión de proyectos. Se ha utilizado una adaptación del método Kanban, presentado por Hammarberg [81], donde se ha utilizado principalmente el cronograma del proyecto y el "Tablero Kanban" como artefactos de proyecto, a fin de realizar el seguimiento a las actividades.

Método de diseño e implementación. Para la preparación de la ontología y la implementación de la solución se han establecido etapas del proyecto, relacionadas directamente con los objetivos de la investigación. Además, el trabajo realizado para estas etapas ha sido documentado en capítulos específicos de la presente investigación, según se detalla:

Tabla 8. Etapas del proyecto y capítulos donde son documentadas

Objetivos de Tesis	Etapas del proyecto	Detalle	Capítulos relacionados
OE1 Recopilar los conceptos y relaciones alrededor del dominio semántico de un proceso de GRSI, para construir su base ontológica.	Obtener información para la ontología.	Se indaga sobre trabajos previos y posibles fuentes. Se recopila información de fuentes más relevantes. Se organiza la información de clases y relaciones.	3. Estado del arte 4. Recopilación de componentes para la ontología 7. Conclusiones y trabajos futuros
OE2 Modelar una ontología, utilizando los conceptos y relaciones recopilados, para construir el soporte de datos del proceso de GRSI.	Construir la ontología en un modelo de datos.	Se toman las clases y relaciones identificadas para implementar un modelo ontológico, el cual es validado por un grupo de expertos.	5. Implementación de la ontología de gestión de riesgos de seguridad de información 7. Conclusiones y trabajos futuros
OE3 Implementar una aplicación informática, que permita explotar la ontología modelada, para dar lugar a un proceso de GRSI.	Construir una aplicación que permita usar el modelo.	Se implementa una aplicación que permite consultar el modelo ontológico y complementarlo con información proporcionada por el usuario, para realizar un proceso de GRSI.	6. Gestor de riesgos de seguridad de información 7. Conclusiones y trabajos futuros
OE4 Validar que la conjunción del modelo y la aplicación informática implementada mitiguen el margen de error humano sobre el proceso de GRSI.	Verificar que los resultados de la solución sean correctos.	Se somete al juicio de un grupo de expertos el uso conjugado de la ontología y la aplicación, a fin de validar si los resultados mostrados son correctos.	6. Gestor de riesgos de seguridad de información 7. Conclusiones y trabajos futuros

Fuente: Elaboración propia.

Cabe destacar que, para que el modelado de la ontología tenga un soporte persistente se ha trabajado con los formatos de codificación OWL (basada en RDF). Asimismo, la implementación de la solución que analiza esta información corresponde a la tecnología JAVA (con el entorno de desarrollo Netbeans) y la biblioteca JENA (código abierto).

El detalle de las tecnologías referidas, y otras relacionadas es mostrado a continuación:

Tabla 9. Formatos de codificación de información (ontologías)

Modelos de datos	Descripción	Aplicación en la investigación
RDF	RDF (Resource Description Framework), tal como indica su nombre, es un "Marco de Descripción de Recursos". Es un estándar de modelado de datos para metadatos, creada por la World Wide Web Consortium (W3C). Soporta el modelado de ontologías de dominio.	Codificación de modelado de las tríadas de "sujeto-predicado-objeto" para el modelo sirve como base para la construcción de la ontología.
OWL	OWL (Web Ontology Language) es un lenguaje de marcado para compartir datos en la Web, bajo un modelo de ontologías de dominio. Está construido a partir de RDF y codificado en XML. También ha sido creado por la la World Wide Web Consortium (W3C).	Completar la codificación del modelo base para que se convierta en una ontología.

Fuente: Elaboración propia.

Tabla 10. Lenguajes de programación utilizados

Lenguaje de Programación	Descripción	Aplicación en la investigación
JAVA	Lenguaje de programación usado en el desarrollo de ontologías, presenta bibliotecas y framework tales como: Apache Jena o OWLAPI. Además, permite utilizar lenguajes de consultas ontológicas como SPARQL.	Lenguaje de programación para el modelado parcial en RDF y el posterior análisis de la información de la ontología.

Fuente: Elaboración propia.

Tabla 11. Herramientas de software a utilizar

Aplicativo a utilizar	Descripción	Aplicación en la investigación
PROTÉGÉ	Es un marco y un editor de ontologías gratuito y de código abierto para crear sistemas inteligentes. Permite trabajar con estructuras OWL / RDF.	Modelado de las ontologías de gestión de riesgos de seguridad de información en formato OWL.
JENA (Biblioteca)	Apache Jena es un framework de Java de código abierto, creado por Apache Software Foundation, que presenta un paquete bibliotecas de código para trabajar con tecnologías de web semántica, que puede usarse para la organización de datos en RDF o el modelado y consulta de ontologías de dominio.	Biblioteca de funciones que permiten modelar y aprovechar la información modelada en la ontología.
NETBEANS	Entorno de programación en JAVA que puede ser usado para explotar las librerías del framework JENA.	Entorno para implementar el aplicativo informático que brinde una solución que utilice la ontología.

Fuente: Elaboración propia.

Cabe destacar que los formatos, codificación y demás recursos tecnológicos seleccionados ha sido tomados a partir de los resultados de la revisión sistemática de la presente investigación, la cual es presentada en el capítulo 3.

2.5. Justificación

Como ya se expuso, el problema respecto a la GRSI se refiere a que, para implementar este proceso se usan normas que contienen términos y relaciones complejas, por lo que para su realización se requiere de especialistas y, en consecuencia, se da lugar a errores humanos o sesgos de subjetividad sobre los resultados obtenidos. A continuación, se presentan los motivos que sustentan la importancia que tiene el problema planteado, y que motivaron la presente investigación:

- **Relevancia de la implementación.** De la revisión a los portales de búsqueda de contrataciones del Organismo Supervisor de las Contrataciones del Estado (OSCE)[1] se ha identificado que desde el año 2014 a la fecha, las entidades del gobierno peruano invierten todos los años miles de soles en decenas de proyectos referidos a los Sistemas de Gestión de Seguridad de Información (SGSI), gobernados mediante la NTP ISO/IEC 27001:2022 [32]. Este tipo de proyectos conllevan la realización de procesos de gestión de riesgos en seguridad de información. Es decir, para el gobierno del Perú, el proceso de GRSI es una necesidad recurrente y costosa, atendida mediante consultorías en gestión de riesgos de seguridad de información. La implementación y distribución de la solución propuesta podría reducir los costos operativos de estas actividades.

- **Novedad y vigencia de la investigación.** La presente tesis se realiza tomando como referentes centrales a las normas ISO/IEC 27001:2022 [18], ISO/IEC 27002:2022 [19] e ISO/IEC 27005:2022 [20], las cuales han sido emitidas en el año 2022 y, a la fecha de esta investigación, corresponden a sus últimas ediciones. Mediante una revisión sistemática de la literatura se ha validado que, debido a su reciente emisión, a la fecha no existen investigaciones relacionadas a la aplicación de ontologías que comprendan a estas versiones de las normas referidas.

- **Uso de ontologías como solución.** Si bien existen soluciones informáticas tales como E-GAM, ISOTOOLS, E-PULPO, EAR-PILAR, que permiten registrar las gestiones de riesgos de seguridad de información [44], estas no garantizan la consistencia de sus datos. Para superar esta limitante, se propone que el proceso de gestión de riesgos sea construido a partir de una solución que aplique una ontología. Es decir, que establezca los conceptos (clases), individuos (instancias) y propiedades (relaciones) del proceso de GRSI.

[1] **Fuentes:** https://prodapp2.seace.gob.pe/seacebus-uiwd-pub/buscadorPublico/buscadorPublico.xhtml; https://prod4.seace.gob.pe/contratos/publico/

2.6. Alcance

Este trabajo de investigación corresponde a una aplicación práctica del área de ingeniería ontológica (ciencias de la computación) sobre el dominio de la "seguridad de información" y el subdominio de la "gestión de riesgos de seguridad de información".

En ese sentido, se implementa un proceso de "gestión de riesgos de seguridad de información" mediante un modelo ontológico que contempla las siguientes etapas a cubrir:

- **Etapa 1. Contexto de la Organización:** organización; proceso; información; activo de información; tipo de activo de información; propiedad de seguridad de información (confidencialidad, integridad, disponibilidad).
- **Etapa 2. Evaluación de Riesgos:** activo de información; tipo de activo de información; amenaza; aspecto de seguridad afectado (confidencialidad, integridad, disponibilidad); probabilidad; impacto (consecuencia); control; vulnerabilidad; valor del riesgo; propietario del riesgo.
- **Etapa 3. Tratamiento de Riesgos:** opción de tratamiento, acción de tratamiento, responsable de implementación, plazos de implementación.

La ingeniería de ontologías propuesta permitirá utilizar los modelos construidos para generar nuevo conocimiento y realizar consultas en el marco del desarrollo de las etapas de la gestión de riesgos de seguridad de información.

La base de información utilizada se ha elaborado en base a diversas normas internacionales, según se detalla:

Tabla 12. Normas base de las ontologías

Fase de elaboración de la ontología	Normas utilizadas
Contexto de la gestión de riesgos.	MAGERIT v3 – Libro 1. Método. [39] MAGERIT v3 – Libro 2. Catálogo de Elementos. [40] ISO IEC 27005:2022 Gestión de Riesgos de Seguridad de Información [20]
Identificación de riesgos de seguridad de información:	MAGERIT v3 – Libro 2. Catálogo de Elementos. [40] ISO IEC 27005:2022 Gestión de Riesgos de Seguridad de Información [20] ISO/IEC 27000:2018 Vocabulario. Sistema de Gestión de Seguridad de Información. [15] ISO/IEC 31000:2018. Gestión de Riesgos. [17]
Análisis y valoración de riesgos de seguridad de información:	ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de Información. [18] ISO/IEC 27002:2022 Controles de Seguridad de Información. [19] ISO IEC 27005:2022 Gestión de Riesgos de Seguridad de Información [20]
Tratamiento de riesgos seguridad de información:	ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de Información. [18] ISO/IEC 27002:2022 Controles de Seguridad de Información. [19] ISO IEC 27005:2022 Gestión de Riesgos de Seguridad de Información [20]

Fuente: Elaboración propia.

3. Estado del arte

Este capítulo presenta el estado del arte de la investigación, respecto al proceso de Gestión de Riesgos de Seguridad de Información (GRSI), fundamentada en una metodología de para la identificación, evaluación y selección de la literatura académica relacionada.

Se ha aplicado una adaptación de la "Guía para realizar revisiones sistemáticas de la literatura" de Kitchenham [49]. A continuación, se detallan aquellas fases y etapas que la metodología original establece como obligatorias y que han sido aplicadas:

Tabla 13. Adaptación de la "Revisión Sistemática de Literatura" de Kitchenham

Fase	Actividad	Detalle
1. Planear la revisión	Proceso de búsqueda	Procedimiento de búsqueda
		Preguntas de investigación
		Términos de búsqueda
		Fuentes de investigación
	Proceso de selección inicial y final	Procedimiento de selección inicial
		Criterios de selección de estudios
		Procedimiento de selección final
		Criterios de la calidad de los estudios
	Proceso de extracción de datos	Procedimiento de extracción de datos
		Formulario de extracción
2. Conducir la revisión	Ejecución de la búsqueda	Consultas y descargas realizadas
		Resultados del procedimiento de búsqueda
	Ejecución de la selección inicial y final	Resultados de la selección inicial
		Resultados de la selección final
	Ejecución de la extracción de datos	Síntesis de datos
3. Reportar la revisión	Resumen de revisión	Diagrama de actividades y resultados
	Resultados	Preguntas resueltas

Fuente: Elaboración propia.

3.1. Planear la revisión

Se desarrollan las actividades de la etapa 1 "Planear la revisión", que consisten en diseñar el proceso de búsqueda; el proceso de selección inicial y final; y el proceso de extracción de datos.

3.1.1. Proceso de búsqueda

Procedimiento de búsqueda. Se inicia revisando el objetivo principal la investigación:

Objetivo principal: *"Diseñar e implementar un proceso de gestión de riesgos de seguridad de información, basado en estándares internacionales, aplicando una solución basada en ontologías de dominio del área de ciencias de la computación".*

El objetivo se reestructura para proponer la pregunta principal de investigación:

PPI: *"¿De qué modo se han aplicado las ontologías de dominio (ciencias de la computación) en soluciones del proceso de gestión de riesgos de seguridad de información (basada en estándares)?"*

A partir de este planteamiento, se elaboran los componentes propuestos en la estrategia PICOC, incluida en la guía de Petticrew [51], según se detalla:

Tabla 14. Criterios de análisis PICOC

Criterios	Descripción
Población	Procesos de gestión de riesgos de seguridad de información.
Intervención	Aplicación de ontologías de dominio.
Comparación	No aplica, pues no se está comparando con otra tecnología.
Resultado	Cualquier solución aplicada (estrategia o tecnología).
Contexto	Estudios en el área de las ciencias de la computación para experimentar o automatizar el proceso de gestión de riesgos de seguridad de la información.

Fuente: Elaboración propia.

Preguntas de investigación. A partir del análisis PICOC se plantean las consultas:

Tabla 15. Preguntas específicas de investigación

#	Descripción
1	¿Qué norma se utilizó para la gestión de riesgos de seguridad de la información?
2	¿Qué tecnologías se utilizaron para modelar y utilizar la ontología de dominio?
3	¿Qué componentes principales contienen las ontologías implementadas?

Fuente: Elaboración propia.

Términos de búsqueda. Se ha realizado una búsqueda indagatoria, en la plataforma SCOPUS, para validar los términos de búsqueda base (análisis PICOC). Luego, se han identificado términos alternativos o equivalentes. Finalmente, se ha diseñado una cadena de búsqueda general que los integra, según se muestra:

Tabla 16. Términos de búsqueda del análisis exploratorio

Términos de búsqueda base	Términos de búsqueda alternativos	Cadena de búsqueda (general)
"RISK MANAGEMENT"	"RISK ASSESSMENT" "RISK TREATMENT"	(ONTOLOGY OR ONTOLOGICAL) AND ("INFORMATION SECURITY" OR "COMPUTER SECURITY" OR "CYBER SECURITY" OR CYBERSECURITY) AND ("RISK MANAGEMENT" OR "RISK ASSESSMENT" OR "RISK TREATMENT")
"INFORMATION SECURITY"	"COMPUTER SECURITY" "CYBER SECURITY" CYBERSECURITY	
ONTOLOGY	ONTOLOGICAL	

Fuente: Elaboración propia.

Fuentes de investigación. Se utiliza el "Portal de Recursos en Línea" de la Pontificia Universidad Católica del Perú[2] (contiene 41 bases de datos de publicaciones). Se han seleccionado aquellas 7 fuentes cuyo contenido es más afín al dominio de la ingeniería y las ciencias de la computación:

Tabla 17. Bases de datos consultadas

#	Base de Datos	Enlace
1	ACM DIGITAL LIBRARY	https://dl-acm-org.ezproxybib.pucp.edu.pe/
2	EBSCO RESEARCH DATABASE	https://web-s-ebscohost-com.ezproxybib.pucp.edu.pe/ehost/search/selectdb?vid=0&sid=01162444-bd48-485d-9689-609c12b16c22%40redis
3	IEEE/IET ELECTRONIC LIBRARY	https://ieeexplore-ieee-org.ezproxybib.pucp.edu.pe/Xplore/home.jsp
4	SCIENCEDIRECT - ELSEVIER	https://www-sciencedirect-com.ezproxybib.pucp.edu.pe/
5	SCOPUS	https://www-scopus-com.ezproxybib.pucp.edu.pe/search/form.uri?display=basic
6	SPRINGER LINK	https://link-springer-com.ezproxybib.pucp.edu.pe/
7	WEB OF SCIENCE	http://ezproxybib.pucp.edu.pe:2048/login?url=http://isiknowledge.com

Fuente: Elaboración propia.

[2] https://biblioteca.pucp.edu.pe/recursos-en-linea/bases-de-datos (consultada el 28 de junio de 2023)

3.1.2. Proceso de selección inicial y final

Procedimiento de selección inicial. Se establece el protocolo de búsquedas en las bases de datos, con los siguientes pasos:

- Realizar búsquedas en las bases de datos utilizando adaptaciones de la cadena de búsqueda general.
- Extraer cada consulta con los atributos de su fuente original (formatos: XLSX, CSV y BIB) y convertirla al formato XLSX.
- Para aquellas publicaciones con datos primarios completos (Base de Datos, Título, Autor) integrar y normalizar los registros en un formulario base de extracción de datos (formato XLSX), con los siguientes atributos:

Tabla 18. Atributos del formulario base de extracción de datos

Campo	Descripción	Tipo de dato
N°	Numeral correlativo para identificar cada investigación.	Autogenerado
Base de Datos	Base de datos donde se ha identificado la investigación.	General primario
Título	Título de la publicación.	
Autores	Autores registrados en la investigación.	
Resumen	Reseña que sintetiza el contenido de la investigación.	General secundario
Año	Año de publicación de la investigación.	
Idioma	Lengua original predominante en la investigación.	
Digital Object Identifier (DOI)	Código único para las publicaciones electrónicas.	
Tipo de publicación	Tipo: artículo, documento de conferencia, entre otros.	General terciario
Fuente	Publicación donde se difundió la investigación.	
Enlace	Link de referencia de la publicación.	
Palabras clave	Términos relacionados a la temática de la investigación.	

Fuente: Elaboración propia.

- Depurar la lista, eliminando registros duplicados usando el DOI, Título y Autor (para ediciones distintas se selecciona la más reciente).
- Para los registros con datos secundarios incompletos, indagar en las bases de datos y otras fuentes académicas, para completar esta información manualmente en el formulario.
- Revisar los resúmenes y aplicar los criterios de selección de estudios (inclusión y exclusión) para realizar la selección inicial.

Criterios de selección de estudios. Para realizar la selección de las publicaciones, se han establecido los siguientes criterios:

Tabla 19. Criterios de inclusión y exclusión

Criterios	Sobre la investigación revisada
Inclusión	Trata sobre un proceso de gestión de riesgos de seguridad de información.
	Aplica ontologías de dominio para modelar la información del proceso.
	Propone alguna solución teórica o experimental para el proceso.
	La investigación está escrita en inglés o español.
Exclusión	Es un subconjunto, resumen o versión preliminar de otra obra de alguno de los autores.
	Artículos que han sido registrados como “retractados”.

Fuente: Elaboración propia.

Procedimiento de selección final. Para las investigaciones pre – seleccionadas:

- Obtener los artículos completos, y validar que los criterios de inclusión y exclusión hayan sido correctamente aplicados.
- Calificar los artículos en base a los resultados de los criterios de estimación de

calidad: Evaluar cada artículo con las preguntas del marco de evaluación de calidad: Afirmativo (2 puntos); Parcial (1 punto) y Negativo (0 puntos). Para cada investigación, sumar el puntaje obtenido al responder las 8 preguntas y registrarlo en el formulario.

- Para aquellas que superan el umbral definido (10 puntos), presentar los artículos ordenados según el puntaje obtenido.

Criterios de la calidad de los estudios. Evaluar la calidad de las investigaciones en base a las siguientes preguntas:

Tabla 20. Criterios de evaluación de la calidad

ID	Preguntas Generales (G) y Específicas (E)
G1	¿Se establece un alcance claro del trabajo de investigación?
G2	¿Se establece al menos un objetivo de investigación concreto?
G3	¿Se ha documentado al menos una conclusión?
G4	¿Existe coherencia entre los objetivos y las conclusiones?
E1	¿Se menciona explícitamente a las normas utilizadas para el proceso de GRSI?
E2	¿Se especifica la estrategia para modelar y utilizar la ontología?
E3	¿Se especifica la tecnología para modelar y utilizar la ontología?
E4	¿El documento incluye una propuesta gráfica del modelado de la ontología?

Fuente: Elaboración propia.

3.1.3. Proceso de extracción de datos

Procedimiento de extracción de datos. Para las investigaciones seleccionadas:

- Revisar los artículos seleccionados completos.
- Completar los atributos para responder a las preguntas de investigación.

Formulario de extracción. La versión definitiva del formulario contiene algunos atributos adicionales, que permiten resolver las preguntas planteadas:

Tabla 21. Atributos del formulario base de extracción de datos

Campo	Descripción	Tipo de dato
N°	Numeral correlativo para identificar cada investigación.	Autogenerado
Base de Datos	Base de datos donde se ha identificado la investigación.	General primario
Título	Título de la publicación.	
Autores	Autores registrados en la investigación.	
Resumen	Reseña que sintetiza el contenido de la investigación.	General secundario
Año	Año de publicación de la investigación.	
Idioma	Lengua original predominante en la investigación.	
Digital Object Identifier (DOI)	Código único para las publicaciones electrónicas.	
Tipo de publicación	Tipo: artículo, documento de conferencia, entre otros.	General terciario
Fuente	Publicación donde se difundió la investigación.	
Enlace	Link de referencia de la publicación.	
Palabras clave	Términos relacionados a la temática de la investigación.	
Normas referidas	¿Qué norma se utilizó para la gestión de riesgos de seguridad de la información?	Pregunta 1
Tecnologías	¿Qué tecnologías se utilizaron para modelar y utilizar la ontología de dominio?	Pregunta 2
Componentes ontológicos	¿Qué componentes principales contienen las ontologías implementadas?	Pregunta 3

Fuente: Elaboración propia.

3.2. Conducir la revisión

Se desarrollan las actividades de la etapa 2 “Conducir la revisión”, que consisten en realizar: la ejecución de la búsqueda; la selección inicial y final; y la extracción de datos.

3.2.1. Ejecución de la búsqueda

Consultas y descargas realizadas. Se han adaptado los términos de búsqueda definidos en la fase anterior, para que puedan utilizarse en cada una de las fuentes seleccionadas:

Tabla 22. Cadenas de búsqueda utilizadas

Base de Datos	Cadena de búsqueda
ACM DIGITAL LIBRARY	[All: ontolog*] AND [[All: "information security"] OR [All: "computer security"] OR [All: "cyber security"] OR [All: cybersecurity]] AND [[All: "risk management"] OR [All: "risk assessment"] OR [All: "risk treatment"]]
EBSCO RESEARCH DATABASE	ontolog* AND (("information security" OR "computer security" OR "cyber security" OR cybersecurity)) AND (("risk management" OR "risk assessment" OR "risk treatment"))
IEEE/IET ELECTRONIC LIBRARY	("All Metadata":ontolog*) AND ("All Metadata":"information security" OR "All Metadata":"computer security" OR "All Metadata":"cyber security" OR "All Metadata":cybersecurity) AND ("All Metadata":"risk management" OR "All Metadata":"risk assessment" OR "All Metadata":"risk treatment")
SCIENCEDIRECT - ELSEVIER	(ontology OR ontological) AND ("information security" OR "computer security" OR "cyber security" OR cybersecurity) AND ("risk management" OR "risk assessment" OR "risk treatment")
SCOPUS	TITLE-ABS-KEY (ontolog* AND ("information security" OR "computer security" OR "cyber security" OR cybersecurity) AND ("risk management" OR "risk assessment" OR "risk treatment"))
SPRINGER LINK	(ontology OR ontological) AND ("information security" OR "computer security" OR "cyber security" OR cybersecurity) AND ("risk management" OR "risk assessment" OR "risk treatment")
WEB OF SCIENCE	ALL=(ontolog* AND ("information security" OR "computer security" OR "cyber security" OR cybersecurity) AND ("risk management" OR "risk assessment" OR "risk treatment"))

Fuente: Elaboración propia.

Resultados del procedimiento de búsqueda. Después de efectuar las descargas, el 28 de junio de 2023, se obtuvieron 1089 investigaciones. Los registros que presentaban atributos secundarios completos (DOI, Idioma, Resumen) se han completado manualmente, utilizando la plataforma LITMAPS[3].

Posteriormente, se han eliminado los registros duplicados, identificados a partir del DOI, Título y Autores. Se muestra un resumen de los resultados:

Tabla 23. Resultados de las descargas y depuración de las investigaciones

Base de Datos	Registros descargados	Total	Registros sin duplicados	Total
ACM DIGITAL LIBRARY	120	1089	116	1025
EBSCO RESEARCH DATABASE	29		20	
IEEE/IET ELECTRONIC LIBRARY	34		31	
SCIENCEDIRECT - ELSEVIER	366		359	
SCOPUS	66		46	
SPRINGER LINK	456		450	
WEB OF SCIENCE	18		3	

Fuente: Elaboración propia.

[3] Literature Maps: https://www.litmaps.com/

3.2.2. Ejecución de la selección inicial y final

Resultados de la selección inicial. Se han aplicado los criterios de inclusión y exclusión definidos en la tabla 15 del presente informe. Obteniéndose como resultado una selección inicial de 28 artículos.

Resultados de la selección final. Luego, se han aplicado los criterios de calidad definidos en la tabla 16 del presente informe. Se han seleccionado aquellas investigaciones que obtuvieron un puntaje superior al umbral establecido (10).

Tabla 24. Selección inicial y final de artículos

Base de Datos	Selección Inicial	Total	Selección Final	Total
ACM DIGITAL LIBRARY	1	28	1	17
EBSCO RESEARCH DATABASE	2		2	
IEEE/IET ELECTRONIC LIBRARY	7		4	
SCIENCEDIRECT - ELSEVIER	0		0	
SCOPUS	18		10	
SPRINGER LINK	0		0	
WEB OF SCIENCE	0		0	

Fuente: Elaboración propia.

El resultado obtenido corresponde a los siguientes artículos:

Tabla 25. Lista final de artículos seleccionados

N°	Título	Autores	Año
1	A Multi-objective Decision Support Framework for Simulation-Based Security Control Selection	E. Kiesling; C. Strausß; C. Stummer	2012
2	An ontological approach to information security management	Pereira T.; Santos H.	2012
3	An ontology- and Bayesian-based approach for determining threat probabilities	Fenz S.	2011
4	An ontology approach in designing security information systems to support organizational security risk knowledge	Pereira T.; Santos H.	2012
5	Automation Possibilities in Information Security Management	R. Montesino; S. Fenz	2011
6	Constructing enterprise information network security risk management mechanism by ontology	Liu F.-H.; Lee W.-T.	2010
7	Corda security ontology: Example of post-trade matching and confirmation	Iqbal M.; Matulevičius R.	2021
8	Formalizing Information Security Knowledge	Fenz S,Ekelhart A	2009
9	Integration of an Ontological Information Security Concept in Risk Aware Business Process Management	G. Goluch; A. Ekelhart; S. Fenz; S. Jakoubi; S. Tjoa; A. T. Muck	2008
10	Knowledge Base for an Intelligent System in order to Identify Security Requirements for Government Agencies Software Projects	Adán B.G.; Cristhian L.C.; Mario C.L.; Sonia O.S.; Yaneth C.C.; Jairo G.	2016
11	Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL).	Riesco, R.; Villagrá, V. A.	2019
12	Ontology and fuzzy measures based system for information security risk assessment	Muratkhan R.; Kabenov D.; Satybaldina D.	2012
13	Ontology-Based Decision Support for Information Security Risk Management	A. Ekelhart; S. Fenz; T. Neubauer	2009
14	Ontology-based information security compliance determination and control selection on the example of ISO 27002	Fenz S.; Neubauer T.	2018
15	Security Ontology OntoSecRPA for Robotic Process Automation Domain	Kurylets A.; Goranin N.	2023
16	Tools and techniques for analysing the impact of information security	Mace, John Charles	2017
17	Towards the Ontology of ISO/IEC 27005:2011 risk management standard	Agrawal V.	2016

Fuente: Elaboración propia.

3.2.3. Ejecución de la extracción de datos

Síntesis de datos. Para el total de 17 investigaciones seleccionadas se revisó el contenido de los artículos, y se procedió a completar los atributos para responder las preguntas de investigación. A manera de ejemplo, se muestra uno de los registros completado:

Tabla 26. Ejemplo de un registro de artículo seleccionado

N°	4
Base de Datos	SCOPUS
Título	An ontology approach in designing security information systems to support organizational security risk knowledge
Autores	Pereira T.; Santos H.
Resumen	Organizations increasingly demand faster and flexible operations promoted by information and communication technologies, particularly on the Internet and the newer technologies, such as the internet enabled services, mobile and wireless devices and networks, with a complete disregard of their security vulnerabilities and underestimating risks that this new technologies impose. A proper information security risk management is difficult and becomes crucial to ensure the daily operational activities of organizations as well as to promote competition and to create new business opportunities. Moreover there is a lack of formal and flexible models to support a proper information security risk management process. This paper presents an ontology developed in the security domain aimed to support organizations to deal with huge security information issues and therefore implement a proper management to facilitate the decision-making regarding their security needs.
Año	2012
Idioma	English
DOI	10.5220/0004180004610466
Tipo de Publicación	Conference paper
Fuente	KEOD 2012 - Proceedings of the International Conference on Knowledge Engineering and Ontology Development
Link	https://www.scopus.com/inward/record.uri?eid=2-s2.0-84881448192&partnerID=40&md5=05375cd1407738e8f16251302f679292
Palabras Clave	Information security; Information security risk management; Information systems security; ISO/IEC 27001; Ontology
Pregunta 1: Normas referidas	ISO/IEC 27001 OCTAVE ISO/IEC_JTC1
Pregunta 2: Estrategias / tecnologías	ontology based on a conceptual model defined according to the ISO/IEC 27001 Web Ontology Language (OWL)
Pregunta 3: Componentes ontológicos	threats attacks vulnerabilities assets countermeasures Incident Event Asset CIA Threat Attack Control Vulnerability

Fuente: Elaboración propia.

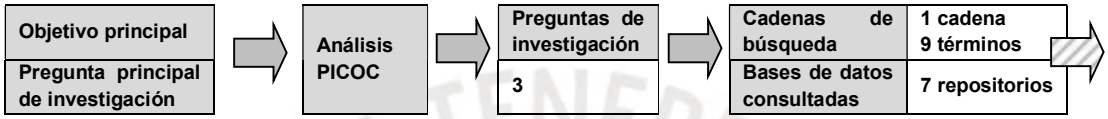
3.3. Reportar la revisión

Se desarrollan las actividades de la etapa 3. “Reportar la revisión”: Realizar el resumen de la revisión y presentar la resolución de las preguntas, con la información recabada.

3.3.1. Resumen de la revisión

Diagrama de actividades y resultados. Se presenta el esquema de las actividades y resultados obtenidos en cada una de las etapas de la revisión sistemática:

Figura 10. Esquema de actividades y resultados de la revisión



Base de Datos	Registros descargados	Registros sin duplicados	Selección Inicial	Selección Final
ACM DIGITAL LIBRARY	120	116	1	1
EBSCO RESEARCH DATABASE	29	20	2	2
IEEE/IET ELECTRONIC LIBRARY	34	31	7	4
SCIENCEDIRECT - ELSEVIER	366	359	0	0
SCOPUS	66	46	18	10
SPRINGER LINK	456	450	0	0
WEB OF SCIENCE	18	3	0	0
TOTAL	**1089**	**1025**	**28**	**17**

Fuente: Elaboración propia.

3.3.2. Resolución de preguntas

Preguntas resueltas. Para las 17 investigaciones seleccionadas, se han tomado los resultados registrados en el Formulario de Extracción de Datos, respecto a las 3 preguntas de investigación, a fin de resolver las preguntas de investigación propuesta, según se detalla a continuación:

Pregunta 1. ¿Qué norma se utilizó para la gestión de riesgos de seguridad de la información? Esta consulta se refiere a la indagación sobre aquellas normas que se usaron como referentes para construir la ontología de dominio, y también aquellas que han sido referenciadas por el artículo por su significancia en este campo.

Tabla 27. Resultados obtenidos en la pregunta #1

Registros más significativos	Discusión de resultados	Registros seleccionados
ISO 27001; ISO 27002; ISO 27005; AURUM; COBIT; CRAMM; French EBIOS standard; German IT Grundschutz Manual; ISO17799; ITIL; NIST SP 800-12; NIST SP 800-30; OCTAVE; ROPE; SCAP; SRM domain model; STRIDE threat model	En términos de la frecuencia de mención, se ha identificado que los estándares de la familia ISO/IEC 27000 son los más referenciados como normas de gestión de riesgos de seguridad de información. Las demás normas suelen ser referidas, pero en entornos de localidades específicas, por ejemplo: el estándar NIST SP 800-12 (Estados Unidos), German IT Grundschutz Manual (Alemania) y French EBIOS standard (Francia).	En consecuencia, se han seleccionado las siguientes normas como referentes: -ISO 27001 -ISO 27002 -ISO 27005

Fuente: Elaboración propia.

Pregunta 2. ¿Qué tecnologías se utilizaron para modelar y utilizar la ontología de dominio? Esta consulta se refiere a la indagación sobre aquellas estrategias de uso de las ontologías de dominio, así como también de las tecnologías que han sido utilizadas con mayor frecuencia.

Tabla 28. Resultados obtenidos en la pregunta #2

Registros más significativos	Discusión de resultados	Registros seleccionados
-Algoritmos de decisión -AURUM TOOL -CARE (Condition, Action, Resource and Environment) -CORDA -Modelos bayesianos -Motor de simulación -Motor de optimización -Protégé -Semantic Web Rule Language (SWRL) -SPARQL -SQWRL -Structured Threat Information Expression (STIX™) -Unified Problem-Solving Method Development Language (UPML) -Web Ontology Language (OWL)	La principal mención en aspectos de arquitectura para el modelado de la información ha sido la referida al lenguaje OWL. Por el lado del software de modelado, se menciona de manera frecuente a la herramienta Protégé: aplicativo que facilita el modelado de la ontología mediante un entorno gráfico. No se realizan mayores precisiones sobre los lenguajes de programación utilizados para implementar soluciones, pero en algunos de los gráficos se pueden identificar soluciones basadas en las plataformas .NET y Java.	-Modelado: Lenguaje de ontología web (OWL) -Software de Modelado: Protégé

Fuente: Elaboración propia.

Pregunta 3. ¿Qué componentes principales contienen las ontologías implementadas? Esta consulta se refiere a la indagación sobre aquellos términos que son más usados en las ontologías de dominio propuestas en los artículos.

Tabla 29. Resultados obtenidos en la pregunta #3

Registros más significativos	Discusión de resultados	Registros seleccionados
-Activo (de información) -Agente/Amenaza -Atributos de Seguridad / Propiedad de Seguridad / CID (confidencialidad, integridad, disponibilidad) -Impacto / Consecuencias -Controles / Contramedidas / Salvaguarda -Eventos -Incidente -Organización -Rol / Propietario -Probabilidad / Posibilidad -Riesgo -Tipos de Controles -Tipos de Amenazas -Tipos de Riesgos -Tratamiento de Riesgo -Vulnerabilidades	En términos de frecuencias de repetición de términos, los principales elementos han sido los: riesgos, activos [de información], amenazas, vulnerabilidades y controles. Se puede inferir que todos ellos son elementos centrales para modelar el riesgo en una ontología de la seguridad de información.	-Riesgo -Activo -Amenaza -Vulnerabilidad -Control -Probabilidad

Fuente: Elaboración propia.

4. Recopilación de componentes para la ontología

Este capítulo presenta el trabajo realizado para identificar las potenciales clases, relaciones e individuos para la ontología del proceso de Gestión de Riesgos de Seguridad de Información (GRSI). Esta compilación se realiza a partir de la revisión de la literatura disponible, siendo la fuente principal el estándar ISO/IEC 27005:2022 [20].

4.1. Fuentes de información

Tal como se ha identificado en la sección de estado del arte (ver Tabla 27), los estándares más consultados para la gestión de riesgos de seguridad de información son los pertenecientes a la familia ISO 27000, destacándose los siguientes:

- **ISO/IEC 27000:2018 Tecnologías de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario**. [15] Presenta un vocabulario general que esclarece los términos utilizados en la familia de normas ISO relacionadas al dominio de seguridad de información, cuya codificación presenta el formato "ISO 27###"; donde el carácter "#" representa un número.
- [18] **ISO/IEC 27001:2022 Sistemas de gestión de seguridad de la información - Requisitos**. En el marco de un Sistema de Gestión de Seguridad de Información (SGSI), establece como obligatorio el requisito de implementar una gestión de riesgos, periódica y bajo un enfoque metodológico.
- [19] **ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información.** Proponer una lista de controles de seguridad de información. Para cada control detalla sus atributos principales, propósito y una guía de tópicos a considerar para su implementación.
- [20] **ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Guía sobre la gestión de riesgos de seguridad de la información.** Establece las etapas de la gestión de riesgos de seguridad de información, detallando en cada caso las actividades que las componen, así como los conceptos a considerar para realizar este análisis.

Se han revisado estos documentos para identificar los elementos ontológicos (clases, individuos, relaciones) y construir con ellos la ontología que soporte al proceso de GRSI. A continuación, se muestran la estructura de presentación de los conceptos y la tabla que muestra el detalle de la documentación revisada:

Tabla 30. Estructura de definición de clases

Concepto	Se nombra la clase y sus "sinónimos" o conceptos equivalentes.
Definición	Contiene una síntesis de las definiciones obtenidas, realizadas a partir de las fuentes disponibles.
Atributos / Subclases	Se listan los atributos asociados a cada clase, según la definición. En los casos de que existan subclases, estas son presentadas con sus atributos.
Tríada	Lista los "conceptos", sus "relaciones directas" y los "conceptos relacionados".
Fuentes	Estándares y normas utilizadas para elaborar esta ficha.

Fuente: Elaboración propia.

Tabla 31. Fuentes revisadas para las identificar elementos de la ontología

Etapas y actividades		Estándares	Referencias (numerales)
1. Establecer el Contexto	1.1 Establecer el contexto de la organización	ISO/IEC 27001:2022	6.1 Acciones para abordar riesgos y oportunidades 6.1.1 Generalidades
		ISO/IEC 27002:2022	5.9 Inventario de información y otros activos asociados
		ISO/IEC 27005:2022	6. Establecimiento del contexto 6.1 Consideraciones organizacionales 6.2 Identificación de requisitos básicos de las partes interesadas 6.3 Aplicación de la evaluación de riesgos 10.1 Contexto de la organización A.2 Técnicas prácticas A.2.1 Componentes del riesgo de seguridad de la información A.2.2 Activos
	1.2 Establecer los criterios de riesgos	ISO/IEC 27001:2022	6.1.2 Evaluación de riesgos de seguridad de la información a) - b)
		ISO/IEC 27005:2022	6.4 Establecer y mantener criterios de riesgo de seguridad de la información 6.4.1 Generalidades 6.4.2 Criterios de aceptación de riesgos 6.4.3 Criterios para realizar evaluaciones de riesgos de seguridad de la información 6.4.3.1 Generalidades 6.4.3.2 Criterios de consecuencias 6.4.3.3 Criterios de probabilidad 6.4.3.4 Criterios para determinar el nivel de riesgo 6.5 Elegir un método apropiado A.1 Criterios de riesgo de seguridad de la información A.1.1 Criterios relacionados con la evaluación de riesgos A.1.1.1 Consideraciones generales sobre la evaluación de riesgos A.1.1.2 Enfoque cualitativo A.1.1.2.1 Escala de consecuencias A.1.1.2.2 Escala de probabilidad A.1.1.2.3 Nivel de riesgo A.1.1.3 Enfoque cuantitativo A.1.1.3.1 Escalas finitas A.1.2 Criterios de aceptación de riesgos
2. Evaluar el riesgo	2.1 Identificar los riesgos	ISO/IEC 27001:2022	6.1.2 Evaluación de riesgos de seguridad de la información c)
		ISO/IEC 27005:2022	7. Proceso de evaluación de riesgos de seguridad de la información 7.1 Generalidades 7.2 Identificación de riesgos de seguridad de la información 7.2.1 Identificación y descripción de riesgos de seguridad de la información 7.2.2 Identificación de los propietarios del riesgo A.2.3 Fuentes de riesgo y estado final deseado A.2.5 Enfoque basado en activos A.2.5.1 Ejemplos de amenazas A.2.5.2 Ejemplos de vulnerabilidades A.2.5.3 Métodos de evaluación de vulnerabilidades técnicas A.2.5.4 Escenarios operacionales A.2.6 Ejemplos de escenarios aplicables en ambos enfoques A.2.7 Monitoreo de eventos relacionados con riesgos
	2.2 Analizar los riesgos	ISO/IEC 27001:2022	6.1.2 Evaluación de riesgos de seguridad de la información d)
		ISO/IEC 27005:2022	7.3 Análisis de riesgos de seguridad de la información 7.3.1 Generalidades 7.3.2 Evaluación de posibles consecuencias 7.3.3 Evaluación de probabilidad 7.3.4 Determinación de los niveles de riesgo
	2.3 Valorar los riesgos	ISO/IEC 27001:2022	6.1.2 Evaluación de riesgos de seguridad de la información e) 8.2 Evaluación de riesgos de seguridad de la información
		ISO/IEC 27005:2022	7.4 Evaluación de los riesgos de seguridad de la información 7.4.1 Comparación de los resultados del análisis de riesgos con los criterios de riesgo 7.4.2 Priorización de los riesgos analizados para el tratamiento de riesgos
3. Tratar el riesgo	3.1 Establecer el plan de tratamiento	ISO/IEC 27001:2022	6.1.3 Tratamiento de riesgos de seguridad de la información a) – c), e) - f) 8.3 Tratamiento de riesgos de seguridad de la información
		ISO/IEC 27002:2022	0.4 Determinación de los controles
		ISO/IEC 27005:2022	8. Proceso de tratamiento de riesgos de seguridad de la información 8.1 Generalidades 8.2 Selección de opciones apropiadas de tratamiento de riesgos de seguridad de la información 8.3 Determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información 8.4 Comparación de los controles determinados con los de ISO/IEC 27001:2022, Anexo A 8.6 Plan de tratamiento de riesgos de seguridad de la información 8.6.1 Formulación del plan de tratamiento de riesgos 8.6.2 Aprobación por parte de los propietarios del riesgo 8.6.3 Aceptación de los riesgos residuales de seguridad de la información

Fuente: Elaboración propia, en base a diversas normas ISO de la familia 27000.

4.2. Etapa 1. Establecer el contexto

Se han revisado los contenidos relacionados con esta etapa, los cuales comprenden dos grupos de tareas:

- **Establecer el contexto de la organización.**
  Según define el estándar ISO/IEC 27005:2022 [20], en su numeral 10.1 "Contexto de la organización", se deben considerar como punto de partida la organización y su información relevante, para establecer los aspectos internos y externos que influyen en la seguridad de información, las partes interesadas en ellas, y sus requisitos de seguridad.

- **Establecer los criterios de riesgos.**
  Según define el estándar ISO/IEC 27005:2022 [20], en su numeral 6.4 "Establecer y mantener los riesgos de riesgos de seguridad de información", se deben establecer las reglas o parámetros metodológicos para realizar la gestión de riesgos. Es decir: los posibles niveles de probabilidad, los posibles niveles de impacto, la forma en que se calculará el nivel de riesgo y los criterios de aceptación de riesgos.

Estas actividades y los componentes ontológicos relacionados a ellas son mostrados a continuación:

4.2.1. Establecer el contexto de la organización

Se han identificado aquellos conceptos de las normas relacionados a la actividad de "establecer contexto de la organización sobre la que se aplica la gestión de riesgos". Son los siguientes:

- Organización
- Información
- Activo [de Información]
- Interesado (Parte interesada)
- Requisito [de seguridad de información]

Organización. También entendida como "Alcance".

- **Definición:** En el contexto de la GRSI el término difiere de su uso coloquial, pues puede corresponder a una unidad más pequeña dentro de una compañía y no necesariamente a la totalidad de esta. En ese sentido, puede entenderse como el alcance que tendrá la gestión de riesgos en la compañía. Es uno de los elementos iniciales que requieren ser establecidos al realizar una gestión de riesgos.
- **Atributos:** "Nombre de la Organización".
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Organizacion / tieneInteresados / Interesado
  - Organizacion / tieneInformacion / Informacion
- **Fuentes:**

- ISO/IEC 27000:2018 [15], 3.50. Organización.
- ISO/IEC 27005:2022 [20], 6.1. Consideraciones Organizacionales.

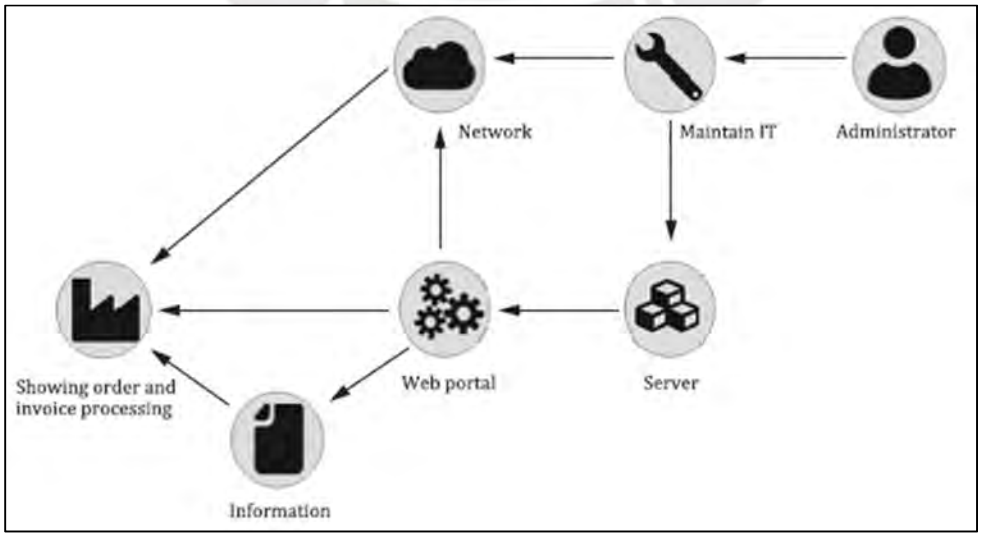
Información. También referido en las normas ISO como “Data”.

- **Definición:** Es un activo importante y esencial para la organización, por lo que requiere ser protegido, puede ser almacenado de manera digital o material. En el contexto del proceso de GRSI es considerada un activo primario.
- **Atributos:** “Nombre de Información”.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Informacion / esDeLaOrganizacion / Organizacion
  - Informacion / estaEnActivo / Activo
  - Informacion / generaRequisito / Requisito
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 4.2.2. Información.
  - ISO/IEC 27002:2022 [19], 3.1.2. Activo.

Activo. También denominado como “Activo de información”.

- **Definición:** La penúltima edición del estándar ISO 27032 (2012) define a los activos de manera general, como aquello que tiene valor para una persona u organización; en el contexto de la seguridad de información podemos entenderlos como todos aquellos activos que contienen o son utilizados en el ciclo de vida de la información. Cabe precisar que, en la ISO 27002, se detalla que las organizaciones deben identificar su información y los activos asociados para determinar su importancia respecto a la seguridad de información. El estándar 27005 presenta un ejemplo donde los activos son mostrados como elementos que soportan al procesamiento de la información de una actividad de la organización:

Figura 11. Ejemplo de la información, sus activos de información y sus interdependencias



Fuente: Estándar ISO 27005:2022. Figura A.2. “Ejemplo de un gráfico de dependencia de activos” [20]

- **Atributos:** “Nombre de Activo”, “Tipo de Activo”.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Activo / contieneInformacion / Informacion
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 4.2.1 Vista general y principios, 4.2.2 Información.
  - ISO/IEC 27002:2022 [19], 3.1.2 Activo, 5.9 Inventario de información y otros activos asociados.
  - ISO/IEC 27005:2022 [20], A.2.2. Activos.
  - ISO/IEC 27032:2012 [85], 4.6. Activo.

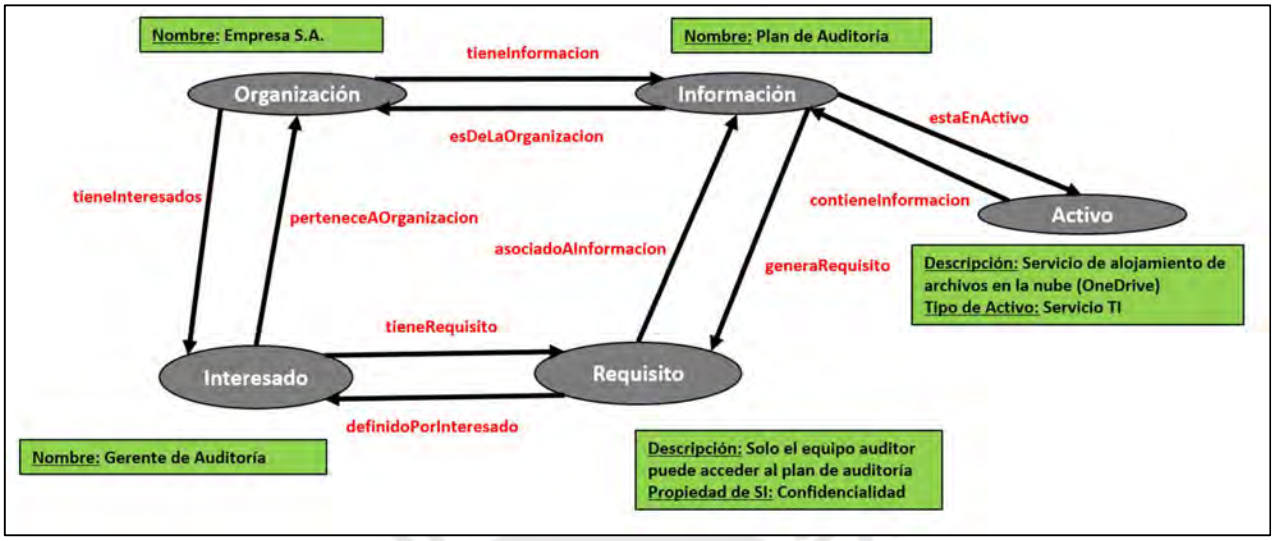
Interesado. También denominado como “Parte Interesada” o “Stakeholder”.

- **Definición:** Este término se refiere a la persona u organización que puede ser afectada por una decisión o actividad relacionada a la información. Además, tienen responsabilidades e intereses respecto a la seguridad de su información.
- **Atributos:** “Nombre de Parte Interesada”.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Interesado / perteneceAOrganizacion / Organizacion
  - Interesado / tieneRequisito / Requisito
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.37. Parte Interesada / Stakeholder.
  - ISO/IEC 27005:2022 [20], 6.2. Identificar requisitos básicos de partes interesadas.

Requisito. También referidas como “requisito de partes interesadas”, “necesidad”, “expectativa”, “requisito de seguridad de información”.

- **Definición:** Son las necesidades y expectativas que las partes interesadas de la organización presentan respecto a la seguridad de su información. Su identificación se realiza a partir de los activos de información de la organización, para establecer si para cada uno de ellos existen normas, contratos o, simplemente, necesidades del negocio respecto a la seguridad de la información. En ese sentido, un requisito siempre está vinculado a la confidencialidad, integridad o disponibilidad de la información.
- **Atributos:** “Descripción del Requisito”, “Propiedad de SI”
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Requisito / definidoPorInteresado / Interesado
  - Requisito / asociadoAInformacion / Informacion
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 4.5.2. Identificar requisitos de seguridad de información.
  - ISO/IEC 27001:2022 [18], 4.2 Entender las necesidades y expectativas de partes interesadas.
  - ISO/IEC 27005:2022 [20], 6.2. Identificar requisitos básicos de partes interesadas.

Figura 12. Modelo y ejemplo para la etapa "Establecer el contexto de la organización"



Fuente: Elaboración propia. A partir de la revisión realizada.

4.2.2. Establecer los criterios de riesgos

Se han identificado aquellos conceptos de las normas relacionados a la actividad de "establecer los criterios para la gestión de riesgos". Son los siguientes:

- Organización
- Criterio [de Gestión de Riesgos]

Organización. Ver 4.2.1.

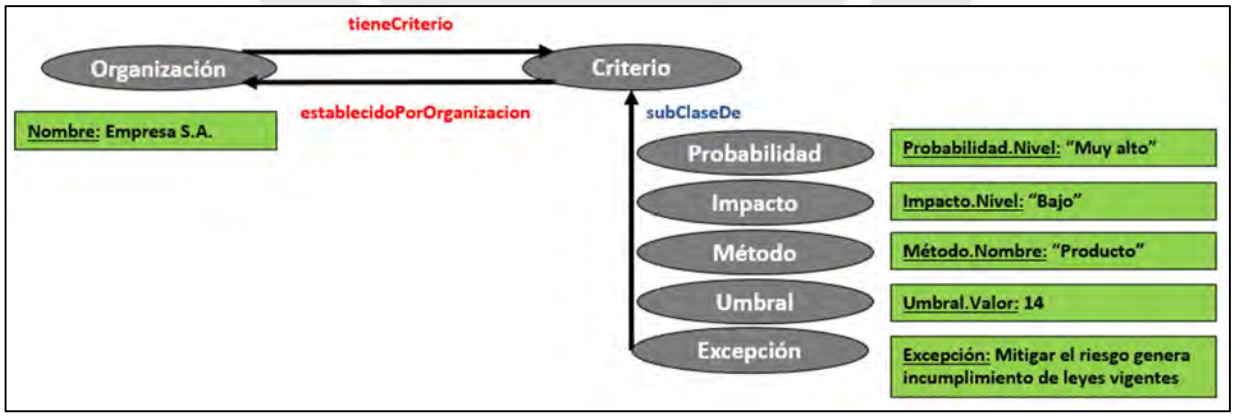
- **Definición:** Ver 4.2.1. Según el estándar 27005 [20], los criterios se revisan y pueden cambiar cada periodo o ciclo de ejecución de la GRSI.
- **Atributos:** "Periodo".
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Organización / tieneCriterio / Criterio
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.50. Organización.
  - ISO/IEC 27001:2022 [18], 4.1 Entender la organización y su contexto.
  - ISO/IEC 27005:2022 [20], 6.1. Consideraciones Organizacionales.

Criterio. También referidas como "criterio de gestión de riesgos".

- **Definición:** Son aquellos términos de referencia que sirven para establecer en una organización específica la importancia de los riesgos para su selección y posterior tratamiento, y están basados en los objetivos de la organización, así como también en los factores presentes en su contexto interno y externo. Según las normas ISO estos comprenden:
  - Criterios de aceptación de riesgos: umbral de aceptación de riesgos, excepciones para aceptar riesgos.
  - Criterios para evaluar riesgos: niveles de probabilidad, niveles de impacto, metodología para determinar el nivel de riesgo.

- **Subclases / Atributos:** Dada la complejidad de los distintos criterios se han estructurado en subclases, que son detalladas a continuación:
    - Criterio.
        - Probabilidad: “Nivel de Probabilidad”, “Descripción”.
        - Impacto: “Nivel de Impacto”, “Descripción”.
        - Método [de cálculo del nivel de riesgos]: “Nombre”, “Descripción”.
        - Umbral [de aceptación de riesgos]: “Valor”
        - Excepción [para la aceptación de riesgos]: “Descripción”.
- **Tríada: Concepto / Relación / Concepto relacionado**
    - Criterio / establecidoPorOrganización / Organizacion
- **Fuentes:**
    - ISO/IEC 27000:2018 [15], 3.66 Criterios de riesgos.
    - ISO/IEC 27001:2022 [18], 6.1.2. a) Evaluación de riesgos de seguridad de información.
    - ISO/IEC 27005:2022 [20]
        - 6.4. Establecer y mantener los criterios de riesgos de seguridad de información.
        - 6.4.1 General.
        - 6.4.2 Criterios de aceptación de riesgos.
        - 6.4.3 Criterios para realiza evaluaciones de riesgos de seguridad de información.
            - 6.4.3.1 General.
            - 6.4.3.2 Criterios de consecuencias.
            - 6.4.3.3 Criterios de probabilidad.
            - 6.4.3.4 Criterios para determinar el nivel de riesgo.
        - 6.5 Escoger un método apropiado.

Figura 13. Modelo y ejemplo para la etapa “Establecer los criterios de riesgos”



Fuente: Elaboración propia. A partir de la revisión realizada.

4.3. Etapa 2. Evaluar el riesgo

Se han revisado los contenidos relacionados con esta etapa, los cuales comprenden tres grupos de tareas:

- **Identificar riesgos.**
  Según define el estándar ISO/IEC 27005:2022 [20], en su numeral 7.2 "Identificar riesgos de seguridad de información", se deben identificar potenciales eventos que puedan comprometer los objetivos de seguridad de información de la organización. Para ello, existen dos enfoques: el basado en eventos y el basado en activos. La presente investigación usa el enfoque basado en activos, que implica el uso de: activos, amenazas y vulnerabilidades, y la consecuente identificación de los propietarios de los riesgos.

- **Analizar riesgos.**
  Según define el estándar ISO/IEC 27005:2022 [20], en su numeral 7.3 "Analizar riesgos de seguridad de información", se debe estimar la probabilidad, el impacto y el consecuente nivel de riesgos. Para ello, frente a los riesgos identificados, se evalúan los controles existentes y su efectividad para mitigar los riesgos.

- **Valorar riesgos.**
  Según define el estándar ISO/IEC 27005:2022 [20], en su numeral 7.4 "Valorar riesgos de riesgos de seguridad de información", se utilizan los resultados obtenidos del análisis de riesgos para establecer qué riesgos son aceptables o inaceptables, al compararlos contra los criterios de aceptación de riesgos. De esta forma, se obtiene una lista de riesgos seleccionados para su tratamiento.

Estas actividades y los componentes ontológicos relacionados a ellas son mostrados a continuación:

4.3.1. Identificar los riesgos

Se han identificado aquellos conceptos de las normas relacionados a la actividad de "identificar los riesgos". Son los siguientes:

- Riesgo
- Activo
- Amenaza
- Vulnerabilidad

Riesgo. También denominado como "Oportunidad" (en un escenario positivo).

- **Definición:** Su definición establece que es el efecto de la incertidumbre respecto al logro de los objetivos. Sin embargo, en el ámbito de la seguridad de información se precisa que está asociado con el potencial de que las amenazas exploten las vulnerabilidades de uno o varios activos de información causando daño a la organización (nota 6 del numeral 3.61 de la ISO 27000:2018 [15]). También se establece que cada riesgo tenga un propietario.

- **Atributos:** “Propietario del Riesgo”.
- **Tríada: Concepto / Relación / Concepto relacionado**
    - Riesgo / afectaActivo / Activo
    - Riesgo / producidoPorAmenaza / Amenaza
    - Riesgo / propiciadoPorVulnerabilidad / Vulnerabilidad
- **Fuentes:**
    - ISO/IEC 27000:2018 [15], 3.61 Riesgo
    - ISO/IEC 27001:2022 [18], 6.1.2 Evaluación de Riesgos de Seguridad de Información, literal c.
    - ISO/IEC 27005:2022 [20], 7.2 Identificar riesgos de seguridad de información.

Activo. Ver 4.2.1. Al identificar riesgos, se consideran los activos que podrían ser afectados por estos.

- **Definición:** Ver 4.2.1.
- **Atributos:** “Tipo de Activo”.
- **Tríada: Concepto / Relación / Concepto relacionado**
    - Activo / afectadoPorRiesgo / Riesgo
- **Fuentes:**
    - ISO/IEC 27000:2018 [15], 4.2.1 Vista general y principios, 4.2.2 Información.
    - ISO/IEC 27002:2022 [19], 3.1.2 Activo, 5.9 Inventario de información y otros activos asociados.
    - ISO/IEC 27005:2022 [20], A.2.2. Activos.
    - ISO/IEC 27032:2012 [85], 4.6. Activo.

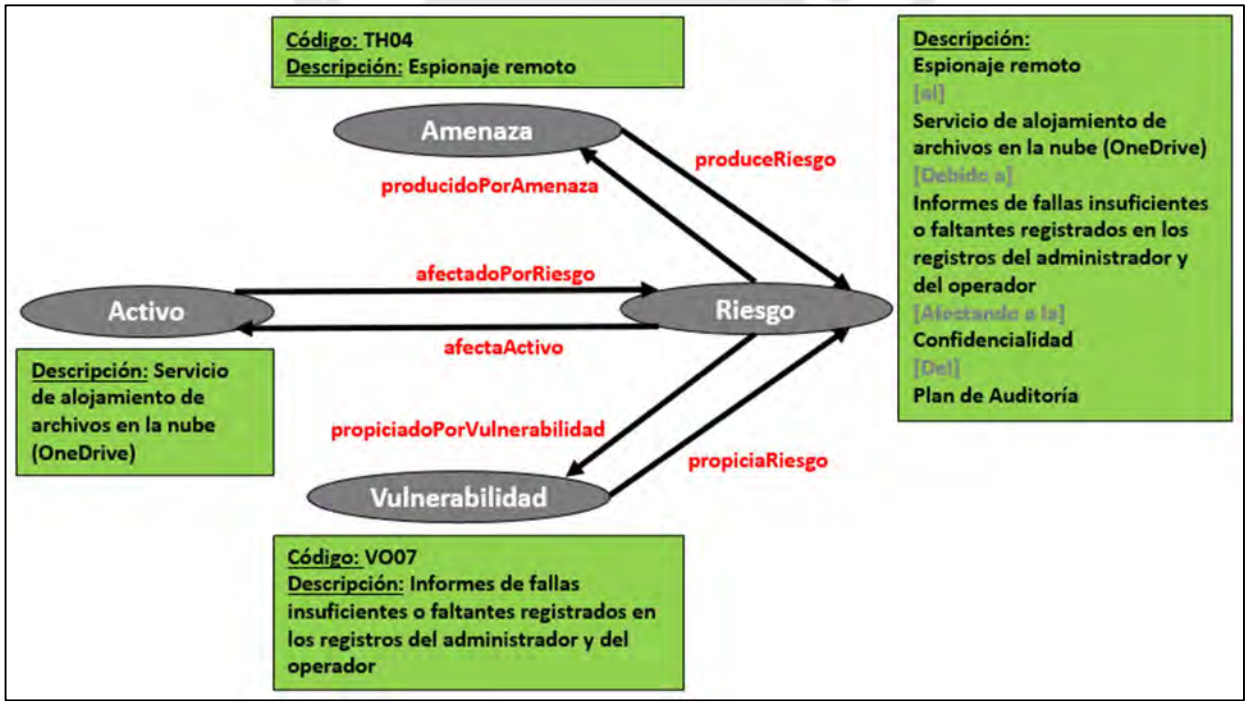
Amenaza. También existe el concepto “fuente de riesgo”, que para efectos prácticos del GRSI es equivalente.

- **Definición:** Se define como la causa potencial de un incidente no deseado, que podría resultar en daño a la organización. Además, la ISO 27005 precisa en su numeral A.2.5.1 que “las amenazas son consideradas como fuentes de riesgos”. Análogamente, el concepto “fuente de riesgo” es definido como un “elemento que solo o en combinación tiene el potencial de dar lugar a un riesgo”. Finalmente, cabe precisar que en el estándar ISO 27005 se proponen, a manera de ejemplos, algunos tipos de amenaza los cuales son los siguientes: física, natural, infraestructural, técnica, humana, que compromete funciones o servicios y organizacional.
- **Atributos:** “Tipo de Amenaza”.
- **Tríada: Concepto / Relación / Concepto relacionado**
    - Amenaza / produceRiesgo / Riesgo
- **Fuentes:**
    - ISO/IEC 27000:2018 [15], 3.74 Amenaza.
    - ISO/IEC 27002:2022 [19], 3.1.34 Amenaza.
    - ISO/IEC 27005:2022 [20], 3.1.6 Fuente de riesgo, 3.1.9 Amenaza, A.2.5.1 Ejemplos de amenazas.

Vulnerabilidad. También existen menciones al concepto de "debilidad", como equivalencia.

- **Definición:** Se define como la debilidad de un control respecto a un activo; haciendo énfasis en que puede ser explotado por una amenaza. Finalmente, cabe precisar que la ISO 27005 contiene algunas categorías de vulnerabilidad propuestas como ejemplos: hardware, software, red, personal, locación, organización.
- **Atributos:** "Tipo de Vulnerabilidad".
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Vulnerabilidad / propiciaRiesgo / Riesgo
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.77 Vulnerabilidad.
  - ISO/IEC 27002:2022 [19], 3.1.38 Vulnerabilidad.
  - ISO/IEC 27005:2022 [20], 3.1.10 Vulnerabilidad, A.2.5.2 Ejemplos de vulnerabilidades.

Figura 14. Modelo y ejemplo para la etapa "Identificar riesgos"



Fuente: Elaboración propia. A partir de la revisión realizada.

4.3.2. Analizar los riesgos

Se han identificado aquellos conceptos de las normas relacionados a la actividad de "analizar los riesgos". Son los siguientes:

- Riesgo
- Control
- Criterio

Riesgo. Ver 4.3.1. Al analizar los riesgos, se consideran los controles que tiene asociados, para determinar su probabilidad, impacto y nivel de riesgo.

- **Definición:** Ver 4.3.1.
- **Atributos:** "Nivel de Probabilidad", "Nivel de Impacto", "Nivel del Riesgo", "Descripción".
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Riesgo / mitigadoPorControl / Control
  - Riesgo / evaluadoConCriterio / Criterio
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.61 Riesgo.
  - ISO/IEC 27001:2022 [18], 6.1.2 Evaluación de Riesgos de Seguridad de Información, literal d.
  - ISO/IEC 27005:2022 [20], 7.3 Analizar riesgos de seguridad de información.

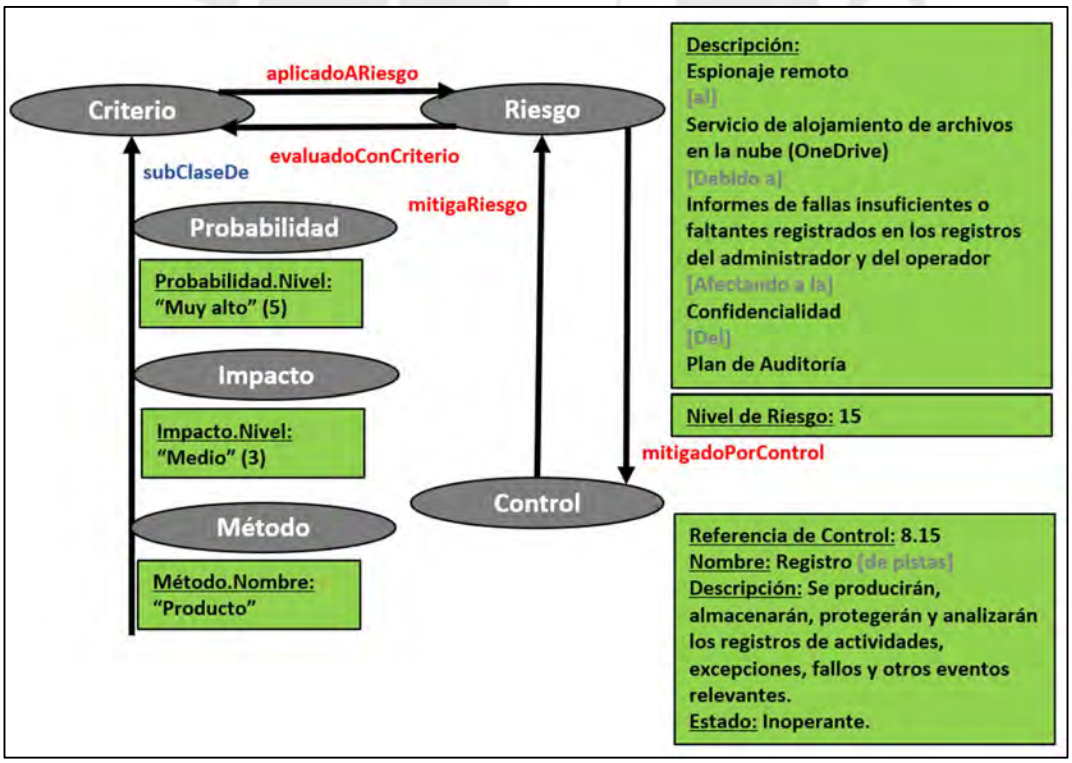
Control. También referido en las normas como "salvaguarda".

- **Definición:** Corresponde a una medida que modifica el riesgo. También se precisa que los controles pueden comprender procesos, políticas, dispositivos, prácticas u otras acciones que modifican el riesgo. El estándar ISO 27005 [20], precisa en su numeral 7.3.2 que los controles deben evaluarse considerando su efectividad, implementación y uso; es decir, el estado real en el que se encuentran operando en la organización. Cabe destacar que los estándares ISO 27001 e ISO 27002 proponen una clasificación de los controles con los siguientes tipos: organizacional, personal, físico, tecnológico y, a su vez, proponen una lista de controles. El atributo de "referencia de control" corresponde a uno de los identificadores de los 93 controles presentados en el Anexo A del estándar ISO 27001 [18] y desarrollados en los numerales 5 al 8 del estándar ISO 27002 [20].
- **Atributos:** "Referencia de Control", "Nombre", "Descripción", "Estado", "Tipo de Control".
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Control / mitigaRiesgo / Riesgo
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.14 Control.
  - ISO/IEC 27001:2022 [18], Anexo A.
  - ISO/IEC 27002:2022 [19], 0.3 Controles, 0.4 Determinar controles.
  - ISO/IEC 27005:2022 [20], 7.3 Analizar riesgos de seguridad de información.

Criterio. Ver 4.2.2. Los criterios nivel de probabilidad y nivel de impacto permiten calcular el nivel de riesgo, aplicando el método de cálculo de nivel de riesgos, como parte del análisis de riesgo.

- **Definición:** Ver 4.2.2.
- **Subclases / Atributos:** Ver 4.2.2:
  - Criterio.
    - Probabilidad: “Nivel de Probabilidad”, “Descripción”.
    - Impacto: “Nivel de Impacto”, “Descripción”.
    - Método [de cálculo del nivel de riesgos]: “Nombre”, “Descripción”.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Criterio / aplicadoARiesgo / Riesgo
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.66 Criterios de riesgos.
  - ISO/IEC 27001:2022 [18], 6.1.2. a) Evaluación de riesgos de seguridad de información.
  - ISO/IEC 27005:2022 [20], 6.4. Establecer y mantener los criterios de riesgos de seguridad de información.

Figura 15. Modelo y ejemplo para la etapa “Analizar riesgos”



Fuente: Elaboración propia. A partir de la revisión realizada.

4.3.3. Valorar los riesgos

Se han identificado aquellos conceptos de las normas relacionados a la actividad de "valorar los riesgos". Son los siguientes:

- Riesgo
- Criterio

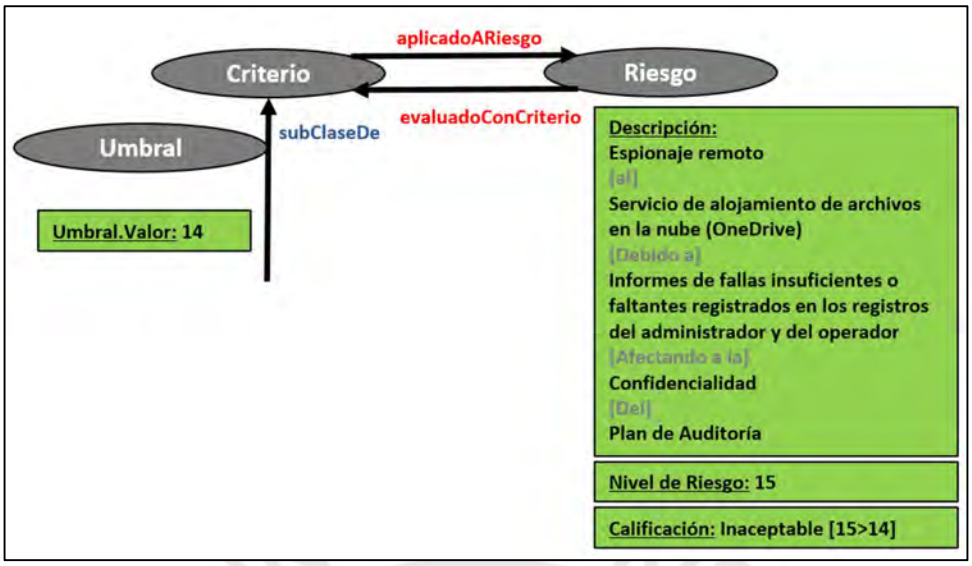
Riesgo. Ver 4.3.1. Los riesgos definidos son evaluados y, considerando su nivel de riesgo son calificados como "aceptables" o "inaceptables". En este último caso, requerirán de tratamiento.

- **Definición:** Ver 4.3.1.
- **Atributos:** "Calificación" (Definido, Aceptable, Inaceptable)
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Riesgo / evaluadoConCriterio / Criterio
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.61 Riesgo.
  - ISO/IEC 27001:2022 [18], 6.1.2 Evaluación de Riesgos de Seguridad de Información, literal e.
  - ISO/IEC 27005:2022 [20], 7.4 Evaluar riesgos de seguridad de información.

Criterio. Ver 4.2.2. Se utiliza el umbral de valor de riesgos para determinar la calificación de un riesgo como "aceptable" si es menor o igual al umbral o "inaceptable", si es mayor.

- **Definición:** Ver 4.2.2.
- **Subclases / Atributos:** Ver 4.2.2:
  - Criterio.
    - Umbral [de aceptación de riesgos]: "Valor"
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Criterio / aplicadoARiesgo / Riesgo
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.66 Criterios de riesgos.
  - ISO/IEC 27001:2022 [18], 6.1.2. a) Evaluación de riesgos de seguridad de información.
  - ISO/IEC 27005:2022 [20], 6.4. Establecer y mantener los criterios de riesgos de seguridad de información.

Figura 16. Modelo y ejemplo para la etapa "Valorar los riesgos"



Fuente: Elaboración propia. A partir de la revisión realizada.

Nota: Esta etapa de la GRSI permite determinar los riesgos, sus probabilidades e impactos para determinar el nivel de riesgo y, utilizando el criterio de "umbral de aceptación de riesgos", determinar cuáles de ellos son aceptables o inaceptables (requieren de tratamiento). Para el caso expuesto como ejemplo, la probabilidad (5), el impacto (3) y el método de cálculo (producto) generan un nivel de riesgo (15) que es superior al umbral definido para los riesgos "aceptables" (14).

Tabla 32. Ejemplo de riesgo en mapa de aceptación de riesgos según el umbral

Nivel de Riesgo aceptable P x I > 14		Impacto (Consecuencias)				
		1	2	3	4	5
Probabilidad (Antecedentes)	1	A	A	A	A	A
	2	A	A	A	A	A
	3	A	A	A	A	I
	4	A	A	A	I	I
	5	A	A	(15)	I	I

Fuente: Elaboración propia.

El resultado final de esta etapa produce una Matriz de Evaluación de Riesgos que muestra los riesgos aceptados y no aceptados; estos últimos pasan a la etapa de tratamiento:

Tabla 33. Ejemplo de matriz de evaluación de riesgos

ID	Riesgo					Probabilidad	Impacto	Nivel de riesgo	Calificación
	Amenaza	Activo	Vulnerabilidad	Propiedad	Información				
1	Espionaje remoto	Servicio de alojamiento de archivos en la nube (OneDrive)	Informes de fallas insuficientes o faltantes registrados en los registros del administrador y del operador	Confidencialidad	Plan de Auditoría	Muy Alto (5)	Medio (3)	15	Inaceptable
	Espionaje remoto [al] Servicio de alojamiento de archivos en la nube (OneDrive) [Debido a] Informes de fallas insuficientes o faltantes registrados en los registros del administrador y del operador [Afectando a la] Confidencialidad [Del] Plan de Auditoría								

Fuente: Elaboración propia.

4.4. Etapa 3. Tratar el riesgo

Se han revisado los contenidos relacionados con esta etapa, los cuales comprenden la siguiente tarea:

- **Establecer el plan de tratamiento.**
  Según define el estándar ISO/IEC 27005:2022 [20], en su numeral 8.2 "Seleccionar apropiadas opciones de tratamiento de riesgos de seguridad de información" se debe tomar la lista de riesgos priorizados (calificados como inaceptables), para que el propietario del riesgo opte por alguna opción de tratamiento (evitar, modificar, retener o compartir). Luego, en el numeral 8.3 "Determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgos de seguridad de información" se precisa que, para cada riesgo priorizado, se defina qué controles serían necesarios para implementar la opción de tratamiento seleccionada. Finalmente, en el numeral 8.6 "Plan de tratamiento de riesgos de seguridad de información", se debe planificar la implementación de los controles en un "Plan de Tratamiento de Riesgos".

Estas actividades y los componentes ontológicos relacionados a ellas son mostrados a continuación:

4.4.1. Establecer el plan de tratamiento

Se han identificado aquellos conceptos de las normas relacionados a la actividad de "seleccionar opciones de tratamiento y controles". Son los siguientes:

- Riesgo
- Tratamiento
- Opción
- Control
- Acción

Riesgo. Ver 4.3.1. En la etapa de tratamiento solo se consideran aquellos riesgos priorizados para ser tratados, con un nivel "inaceptable". Para lo cual es sometido a un tratamiento.

- **Definición:** Ver 4.3.1.
- **Atributos:** Descripción.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Riesgo / mitigadoPorTratamiento / Tratamiento
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.61 Riesgo.
  - ISO/IEC 27001:2022 [18], 6.1.3 Tratamiento de Riesgos de Seguridad de Información, literales a, b.
  - ISO/IEC 27005:2022 [20], 8.2 Seleccionar apropiadas opciones de tratamiento de riesgos de seguridad de información, 8.3 Determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgos de seguridad de información.

Tratamiento. También referido como “Tratamiento del Riesgo” o “Plan de Tratamiento”.

- **Definición:** Para los riesgos priorizados, se debe aplicar un tratamiento, seleccionando alguna de sus opciones y, en consecuencia, seleccionando los controles que deberán implementarse o mejorarse para poder realizar la implementación. Este tratamiento está compuesto de acciones.
- **Atributos:** Opción, Control, Acción, Justificación [de la opción], Aprobador, Fecha Base, Fecha Límite, Estado.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Tratamiento / mitigaRiesgo / Riesgo
  - Tratamiento / usaControl / Control
  - Tratamiento / aplicaOpcion / Opción
  - Tratamiento / compuestoDeAcciones / Acción
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.72 Tratamiento de Riesgo.
  - ISO/IEC 27001:2022 [18], 6.1.3 Tratamiento de Riesgos de Seguridad de Información, literales a, b.
  - ISO/IEC 27005:2022 [20], 8.2 Seleccionar apropiadas opciones de tratamiento de riesgos de seguridad de información, 8.3 Determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgos de seguridad de información.

Opción. También referidas como “opciones de tratamiento”.

- **Definición:** Las opciones son las alternativas de estrategias que se deben seguir cuando se ha identificado que hay un riesgo de valor alto priorizado para su tratamiento. Los estándares ISO establecen 4 opciones para el tratamiento de riesgos: Evitar, se aplica cuando se opta por eliminar la actividad de negocio que produce el riesgo. Modificar, se realiza mitigando mediante controles el nivel de riesgo. Retener, o aceptar el riesgo, aplicando algunos criterios de excepción. Compartir, dividiendo las responsabilidades con otras partes interesadas externas o internas.
- **Atributos:** Nombre (evitar, modificar, retener o compartir)
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Opción / aplicadoEnTratamiento / Tratamiento
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.72 Tratamiento de Riesgo.
  - ISO/IEC 27001:2022 [18], 6.1.3 Tratamiento de Riesgos de Seguridad de Información, literales a, b.
  - ISO/IEC 27005:2022 [20], 8.2 Seleccionar apropiadas opciones de tratamiento de riesgos de seguridad de información.

Control. Ver 4.3.2. En la etapa de tratamiento se le suele referir como “control proyectado”.

- **Definición:** Ver 4.3.2. Mientras que en la etapa de evaluación los controles son entendidos como salvaguardas existentes en los activos de información, en la etapa de tratamiento, los controles son reconocidos como elementos

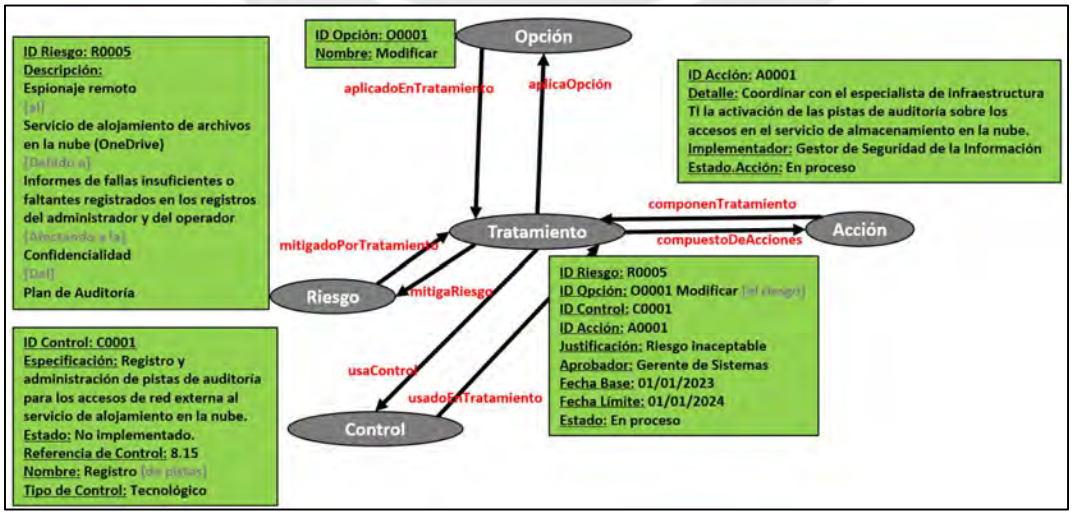
proyectados a ser implementados o mejorados.

- **Atributos:** “Especificación”, “Estado”, “Referencia de Control”, “Nombre”, “Descripción”, “Estado”, “Tipo de Control”.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Control / usadoEnTratamiento / Tratamiento
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.14 Control.
  - ISO/IEC 27001:2022 [18], Anexo A.
  - ISO/IEC 27002:2022 [19], 0.3 Controles, 0.4 Determinar controles.
  - ISO/IEC 27005:2022 [20], 8.3 Determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgos de seguridad de información.

Acción. Eventualmente referidas como “actividad” o “acción de tratamiento”.

- **Definición:** Si bien los estándares no lo definen como un concepto específico, si son referidos en los cuerpos de las normas como un subconjunto o componente de los tratamientos, es decir, los tratamientos son comprendidos como un conjunto de acciones.
- **Atributos:** Detalle, Recursos, Estado, Restricciones, Responsable, Fecha Inicio, Fecha Fin.
- **Tríada: Concepto / Relación / Concepto relacionado**
  - Acción / componenTratamiento / Tratamiento
- **Fuentes:**
  - ISO/IEC 27000:2018 [15], 3.14 Control.
  - ISO/IEC 27001:2022 [18], Anexo A.
  - ISO/IEC 27002:2022 [19], 0.3 Controles, 0.4 Determinar controles.
  - ISO/IEC 27005:2022 [20], 7.3 Analizar riesgos de seguridad de información.

Figura 17. Modelo y ejemplo para la etapa “Establecer el plan de tratamiento”



Fuente: Elaboración propia.

4.5. Discusión de resultados

Se han utilizado las fuentes identificadas en el capítulo 3, para recopilar la información e identificar los componentes de una ontología de GRSI. A partir de la experiencia realizada, se destacan los siguientes hechos:

- Los conceptos utilizados han sido tomados, principalmente, de la familia de estándares 27000, la cual fue la principal fuente de información identificada mediante la revisión sistemática, en el capítulo anterior.
- Si bien el capítulo se ha estructurado en las etapas del proceso de GRSI (contexto, evaluación y tratamiento de riesgos), se destaca que existen conceptos que pertenecen a más de una etapa y que, más bien, se enriquecen de nuevos atributos o relaciones, conforme se les va a analizando en el flujo del proceso.
- Para facilitar al lector el entendimiento de los conceptos expuestos y sus relaciones en el marco del proceso de GRSI, se ha optado por complementarlos con prototipos de los diagramas ontológicos, así como también con ejemplos.

5. Implementación de la ontología de gestión de riesgos de seguridad de información

En base a la información recopilada en el capítulo 4 y considerando algunas propuestas de investigaciones afines del capítulo 3, se han elaborado los componentes de una ontología que soporte al proceso de Gestión de Riesgos de Seguridad de Información (GRSI), la cual ha sido refinada a partir de la aplicación del método Delphi y las opiniones de expertos.

5.1. Diseño de la ontología base

Se ha modelado una estructura de datos ontológica basada en los Conceptos (clases) y Propiedades (relaciones). A continuación, se muestran los componentes recopilados en el capítulo anterior, a partir de la familia de normas de los estándares ISO 27000 [15] [18] [19] [20], que han sido usados como base de la ontología:

Tabla 34. Componentes base de la ontología de GRSI

Etapa	Clases	Propiedades
Establecer el contexto de la organización (1.1)	Organización	Organizacion / tieneInteresados / Interesado Organizacion / tieneInformacion / Informacion
	Información	Informacion / esDeLaOrganizacion / Organizacion Informacion / estaEnActivo / Activo Informacion / generaRequisito / Requisito
	Activo [de Información]	Activo / contieneInformacion / Informacion
	Interesado (Parte interesada)	Interesado / perteneceAOrganizacion / Organizacion Interesado / tieneRequisito / Requisito
	Requisito [de seguridad de información]	Requisito / definidoPorInteresado / Interesado Requisito / asociadoAInformacion / Informacion
Establecer los criterios de riesgos (1.2)	Organización	Organizacion / tieneCriterio / Criterio
	Criterio [de Gestión de Riesgos]	Criterio / establecidoPorOrganizacion / Organizacion
Identificar los riesgos (2.1)	Riesgo	Riesgo / afectaActivo / Activo Riesgo / producidoPorAmenaza / Amenaza Riesgo / propiciadoPorVulnerabilidad / Vulnerabilidad
	Activo	Activo / afectadoPorRiesgo / Riesgo
	Amenaza	Amenaza / produceRiesgo / Riesgo
	Vulnerabilidad	Vulnerabilidad / propiciaRiesgo / Riesgo
Analizar los riesgos (2.2)	Riesgo	Riesgo / mitigadoPorControl / Control Riesgo / evaluadoConCriterio / Criterio
	Control	Control / mitigaRiesgo / Riesgo
	Criterio	Criterio / aplicadoARiesgo / Riesgo
Valorar los riesgos (2.3)	Riesgo	Riesgo / evaluadoConCriterio / Criterio
	Criterio	Criterio / aplicadoARiesgo / Riesgo
Establecer el plan de tratamiento (3.1)	Riesgo	Riesgo / mitigadoPorTratamiento / Tratamiento
	Tratamiento	Tratamiento / mitigaRiesgo / Riesgo Tratamiento / usaControl / Control Tratamiento / aplicaOpcion / Opcion Tratamiento / compuestoDeAcciones / Accion
	Opción	Opcion / aplicadoEnTratamiento / Tratamiento
	Control	Control / usadoEnTratamiento / Tratamiento
	Acción	Accion / componenTratamiento / Tratamiento

Fuente: Elaboración propia.

Cabe destacar que, como producto de la revisión al estándar 27005:2022 [20] y otras normas de esa familia [18] [19], se ha identificado que algunas de las clases listadas presentan subclases o subtipos, tal como se muestra en la siguiente tabla, con las respectivas referencias desde las que fueron extraídas:

Tabla 35. Clases que presentan subclases

Clase	Subclases	Referencia
Activo [de Información]	Recurso humano	ISO/IEC 27005:2022 [20] A.2.2 Activos
	Servicio	
	Hardware	
	Conectividad de Red	
	Aplicación	
	De Negocio	
Criterio [de Gestión de Riesgos]	Probabilidad	ISO/IEC 27005:2022 [20] 6.4 Establecer y mantener criterios de riesgos de seguridad de información
	Impacto	
	Método [de cálculo del nivel de riesgos]	
	Umbral [de aceptación de riesgos]	
	Excepción [para la aceptación de riesgos]	
Amenaza	Física	ISO/IEC 27005:2022 [20] A.2.5.1 Ejemplos de amenazas
	Natural	
	Infraestructural	
	Técnica	
	Humana	
	Funcional	
	Organizacional	
Vulnerabilidad	Hardware	ISO/IEC 27005:2022 [20] A.2.5.2 Ejemplos de vulnerabilidades ISO/IEC 27002:2022
	Software	
	Red	
	Personal	
	Ubicación	
	Organización	
Control	Organizacional	ISO/IEC 27001:2022 [18] Anexo A Referencia de controles de seguridad de información ISO/IEC 27002:2022 [19]
	Personal	
	Físico	
	Tecnológico	
Opción	Evitar	ISO/IEC 27005:2022 [20], 8.2 Seleccionar apropiadas opciones de tratamiento de riesgos de seguridad de información
	Modificar	
	Retener	
	Compartir	

Fuente: Elaboración propia. En base a los estándares ISO 27001, ISO 27002 e ISO 27005.

En consecuencia, la estructura de clases y subclases que compondrían la ontología sería la mostrada a continuación:

Tabla 36. Jerarquía de clases y subclases de la ontología

Clase	Subclase
Organizacion	-
Informacion	-
Activo	ActivoRecursoHumano
	ActivoServicio
	ActivoHardware
	ActivoConectividadDeRed
	ActivoAplicacion
	ActivoDeNegocio
Control	ControlOrganizacional
	ControlPersonal
	ControlFisico
	ControlTecnológico
Interesado	-

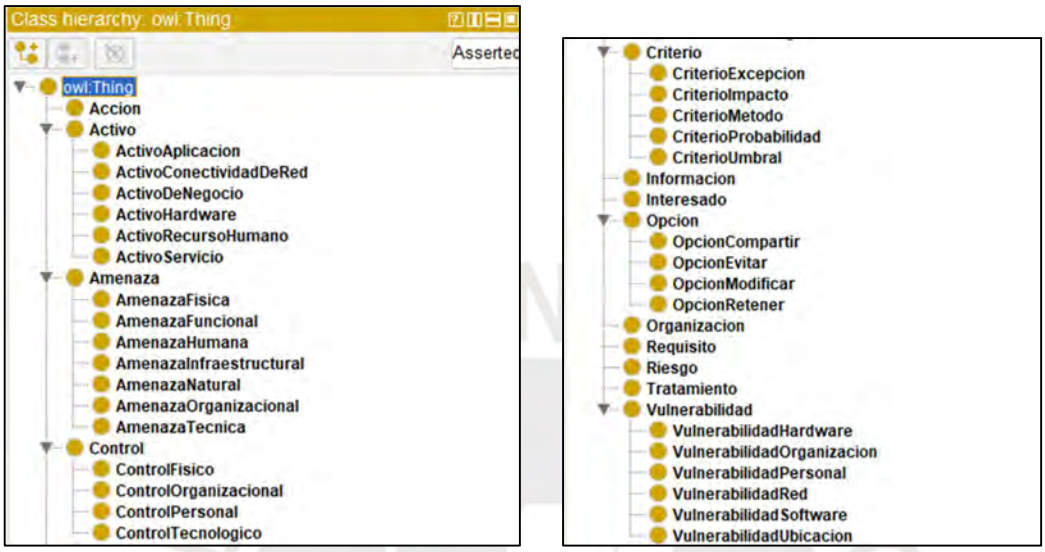
Clase	Subclase
Criterio	CriterioProbabilidad
	CriterioImpacto
	CriterioMetodo
	CriterioUmbral
	CriterioExcepcion
Amenaza	AmenazaFisica
	AmenazaNatural
	AmenazaInfraestructural
	AmenazaTecnica
	AmenazaHumana
	AmenazaFuncional
	AmenazaOrganizacional
Requisito	-

Clase	Subclase
Vulnerabilidad	VulnerabilidadHardware
	VulnerabilidadSoftware
	VulnerabilidadRed
	VulnerabilidadPersonal
	VulnerabilidadUbicacion
	VulnerabilidadOrganizacion
Opcion	OpcionEvitar
	OpcionModificar
	OpcionRetener
	OpcionCompartir
Riesgo	-
Tratamiento	-
Accion	-

Fuente: Elaboración propia.

Se ha elaborado un prototipo utilizando las clases y propiedades definidas en las tablas anteriores, utilizando la herramienta Protégé. Cabe destacar que esta herramienta fue identificada a partir de la segunda pregunta de la revisión sistemática presentada en el capítulo 3 de la presente investigación:

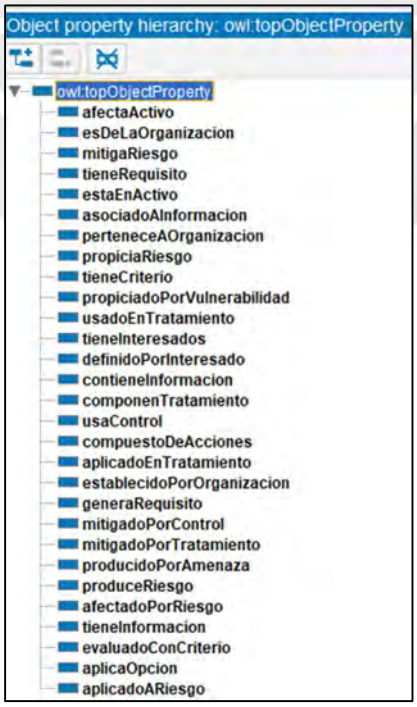
Figura 18. Prototipo base de clases de la GRSI (Protégé).



Fuente: Elaboración propia.

Posteriormente, se han creado y relacionado las propiedades para relacionar a las clases involucradas en el modelo.

Figura 19. Prototipo base de propiedades de la GRSI (Protégé).



Fuente: Elaboración propia.

5.2. Refinamiento de la ontología

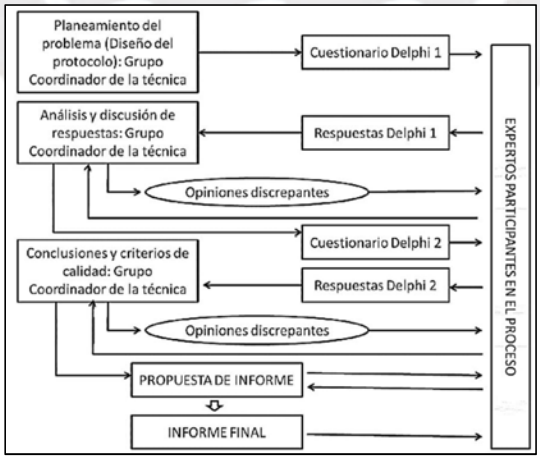
Los registros producidos a partir de las gestiones de riesgos en las organizaciones (evaluaciones y tratamiento) presentan información confidencial y, según establece el estándar ISO 27001 [18] en su numeral 7.5.3 debe estar adecuadamente protegida. Debido a esto, si bien es posible encontrar algunos datos dispersos sobre parte de los términos relacionados a la ontología, es muy difícil obtener de manera convencional acceso a la información de las matrices de evaluación de riesgos o los consecuentes planes de tratamiento de riesgos.

Para resolver esta limitación, se ha optado por aplicar el método Delphi; pues, Landeta [87], refiere sobre este método: *"Se ha utilizado desde los años sesenta en ámbitos académicos y empresariales, y se ha empleado principalmente como técnica para la planificación y el consenso en situaciones de incertidumbre en las que no es posible utilizar otras técnicas basadas en información objetiva"*
[Subrayado propio]

A continuación, se muestra una adaptación del método Delphi, considerando los lineamientos de la metodología la propuesta por Reguant [82], con las siguientes etapas y dinámica de trabajo:

- **Definición.** Formular un objetivo, alcance e identificar la información a utilizar en el análisis.
- **Conformación del grupo.** Elegir especialistas competentes y experimentados en el problema a analizar.
- **Ejecución de rondas.** Iterar a partir de la aplicación de cuestionarios y el análisis posterior, tomando los puntos discrepantes o de mayor complejidad para consultarse en una iteración posterior.

Figura 20. Ciclo de iteraciones Delphi.



Fuente: Reguant [82].

- **Resultados.** Se documentan las conclusiones de la última iteración como solución final.

Definición. Se han establecido las siguientes condiciones para el análisis Delphi del

modelo ontológico:

Tabla 37. Definiciones para la aplicación del método Delphi

Objetivo	Identificar debilidades y errores del modelo ontológico de GRSI
Alcance	Etapas que componen el proceso de GRSI
Fuentes de información	Diagramas de la ontología de las etapas del proceso Ejemplo usado en las etapas del proceso Estándar ISO IEC 27005:2022

Fuente: Elaboración propia.

Conformación del grupo. La selección de los perfiles de expertos se ha realizado en base a los requisitos de conocimiento y experiencia en con el proceso de GRSI, como también la cantidad de estos procesos en los que han participad. Además, para evitar ambigüedades ontológicas, se ha requerido el dominio del idioma español. En consecuencia, se ha obtenido la participación de 15 especialistas, según detalle:

Tabla 38. Resumen del perfil de expertos seleccionados

Perfil	Requisitos	Resultado (15 especialistas)
Experiencia	Haber participado en al menos 5 gestiones de riesgos de seguridad de información, con un rol activo como gestor de riesgos y no uno pasivo como oyente.	Los diversos especialistas han participado con un rol activo entre 8 hasta 50 gestiones de riesgos, según su experiencia.
Conocimiento	Conocer un estándar o norma de gestión de riesgos de seguridad de información.	Todos conocen el estándar ISO 27001 e ISO 27005; 2 refieren aplicar el estándar MAGERIT.
Profesión	Profesión afín a las tecnologías de información	Ingenieros Informáticos o de Sistemas (9); Ingenieros Industriales (4), Licenciada en Ciencias de la Información (1), Licenciado en Matemática (1).
Idioma	Dominio del idioma español	Han participado peruanos (12), hondureños (1) y mexicanas (2).

Fuente: Elaboración propia.

Ejecución de rondas. A continuación, se presentan un resumen del cuestionario y los resultados obtenidos para la primera y segunda iteración:

Primera Iteración:

Se facilita a los especialistas los diagramas y ejemplos presentados en el capítulo 4, así como una copia del estándar ISO 27005 [20], y se formula un total de 28 consultas a cada uno de ellos:

Tabla 39. Resumen de preguntas y resultados de la iteración 1

#	Grupo de consultas	Resultados obtenidos
1	Deficiencias en el diagrama de "Establecer el contexto" (4 consultas)	a) La "Organización" no debería tener un atributo periodo. Se debería agregar una clase o concepto "Gestión" o "Gestión de riesgos" que registre un periodo o ciclo de GRSI, para la "Organización". Los criterios pueden cambiar de un ciclo a otro y estos deberían estar asociados a la "Gestión". b) Los "Requisitos" son más relevantes que las "Partes Interesadas". Podría evaluarse la posibilidad de que estas sean solo un atributo de los primeros. c) La "Propiedad" de la seguridad de información de cada "Requisito" es un atributo importante.
2	Deficiencias en el diagrama de "Establecer los criterios" (3 consultas)	d) Los "Criterios" deberían estar asociados a una "Gestión" y no a una "Organización". e) Evaluar la posibilidad de individualizar los "Criterios", para un modelo menos complejo.
3	Deficiencias en el diagrama de "Identificar riesgos" (4 consultas)	f) El riesgo debería estar relacionado a una "Gestión" (asociada a un periodo), ya que sus valores evolucionan en el tiempo. g) El riesgo debe tener un "propietario de riesgo".
4	Deficiencias en el diagrama de "Analizar riesgos" (4 consultas)	h) El principal atributo del "Control" no debería ser la referencia del control, ni la descripción genérica del control que aparece en la norma, sino una descripción específica de los controles.

#	Grupo de consultas	Resultados obtenidos
5	Deficiencias en el diagrama de "Valorar riesgos" (4 consultas)	i) En el caso del "Riesgo" su calificación debe tener un atributo "valor" cuantitativo, para contrastarlo con el umbral de nivel de riesgo. El atributo cualitativo "calificación" es menos relevante.
6	Deficiencias en el diagrama de "Tratar riesgos" (4 consultas)	j) Las "opciones" podrían ser solo un atributo del tratamiento de riesgos.
7	Deficiencias en el diagrama del modelo en Protégé - propiedades (2 consultas)	k) La cantidad de propiedades registradas en el modelo son innecesarias, dado que solo algunas de ellas son necesarias para implementar la GRSI.
8	Deficiencias en el diagrama del modelo en Protégé - clases (3 consultas)	l) Los tipos de "activos" están incompletos, existen otros tipos de activos como documentos físicos, que no estarían contemplados. Pueden usarse marcos como MAGERIT para buscar alternativas de tipos de activos. m) No se ha modelado la restricción que limita que una "amenaza" es aplicable a determinado "tipo de activo". n) No se ha modelado la restricción que limita que una "amenaza" es aplicable a determinada "propiedad" de la seguridad de información. o) No se ha modelado la restricción que limita que una "vulnerabilidad" es aplicable a determinada "amenaza". p) No se ha modelado la restricción que limita que un "control" es aplicable a determinada "vulnerabilidad".

Fuente: Elaboración propia.

Como resultado de la primera iteración, se han aplicado las correcciones sobre el modelo, referidas a los grupos de preguntas 1 al 6. Además, para la pregunta 7 se han reevaluado las propiedades para aplicar una depuración que aligere el modelo. Finalmente, para el numeral 8 se han replanteado los tipos de activos y se han diseñado las relaciones entre clases. Los resultados finales son mostrados en el numeral 5.3 de este informe, donde se presenta la implementación de la ontología.

Segunda Iteración:

Se facilita a los especialistas para cada pregunta la siguiente información, derivada de las respuestas a la primera ronda de preguntas, para luego formular las nuevas:

- Pregunta 1: Los diagramas actualizados e integrados del modelo de GRSI.
- Pregunta 2: Matriz de relaciones entre tipos de activos versus amenazas.
- Pregunta 3: Matriz de relaciones entre propiedades [de seguridad de información] versus amenazas.
- Pregunta 4: Matriz de relaciones entre vulnerabilidades versus controles.

Tabla 40. Resumen de preguntas y resultados de la iteración 2

#	Grupo de consultas	Referencia Iteración 1	Resultados obtenidos
1	Deficiencias en el diagrama de GRSI integrado (4 consultas)	a) – j)	Sin correcciones
2	Propuesta de propiedades simplificadas (2 consultas)	k)	Sin correcciones
3	Propuesta de tipos de activos (2 consultas)	l)	Sin correcciones
4	Propuesta de matriz de relación entre tipo de activo y amenaza (1 consulta)	m)	Correcciones a registros de la matriz
5	Propuesta de matriz de relación entre propiedad y amenaza (1 consulta)	n)	Correcciones a registros de la matriz
6	Propuesta de matriz de relación entre amenaza y vulnerabilidad (1 consulta)	o)	Correcciones a registros de la matriz
7	Propuesta de matriz de relación entre vulnerabilidad y control (1 consulta)	p)	Correcciones a registros de la matriz

Fuente: Elaboración propia.

Resultados. Como resultado de las dos iteraciones realizadas se han obtenidos los siguientes resultados:

- Modelo refinado de la ontología.
- Matrices de restricciones entre clases.

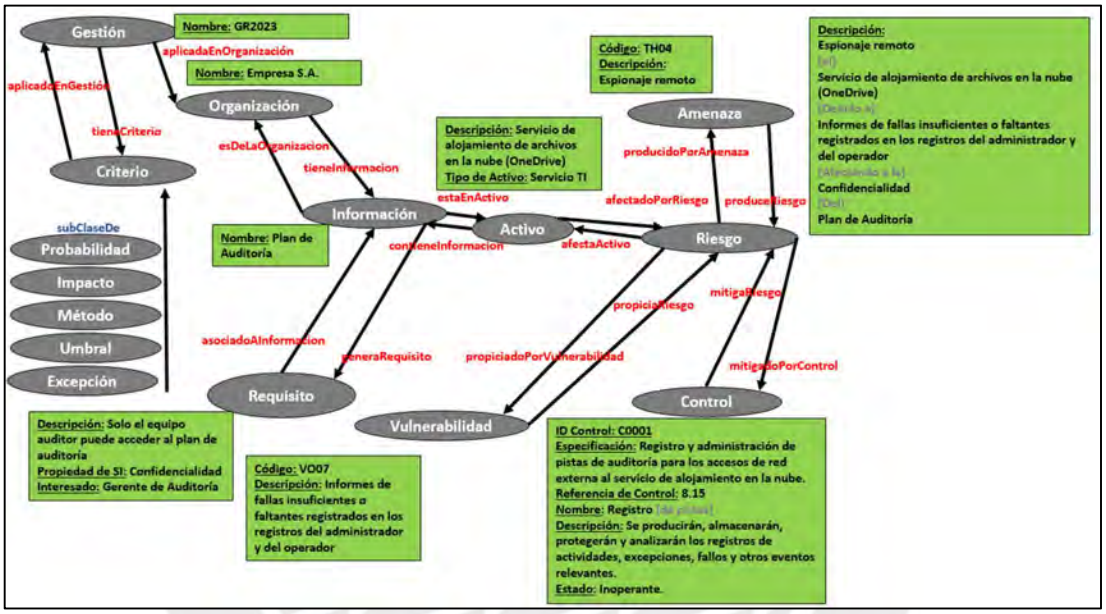
5.3. Implementación de la ontología

Como resultado de la aplicación del método Delphi, se ha modificado la ontología base, aplicando las correcciones propuestas por el grupo de expertos involucrado. En consecuencia, la estructura de la ontología se ha refinado.

5.3.1. Actualización de la arquitectura

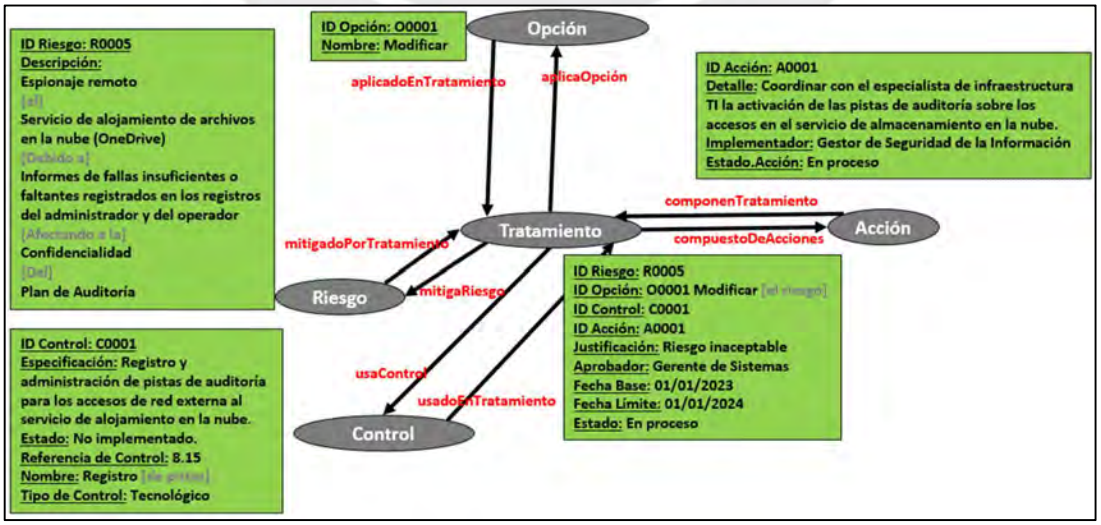
A continuación, se muestra una vista simplificada del modelo actualizado, para las etapas de evaluación y tratamiento de riesgo:

Figura 21. Ontología simplificada de la evaluación de riesgos



Fuente: Elaboración propia.

Figura 22. Ontología simplificada del tratamiento de riesgos



Fuente: Elaboración propia.

5.3.2. Clases y subclases iniciales

Existen relaciones complejas que se desarrollan durante el proceso de GRSI entre algunas clases y subclases del modelo, bajo la forma de restricciones. Estas clases, subclases y relaciones particulares son explicadas a continuación:

La Clase Activo y las Subclases Tipo de Activo

Los estándares ISO 27000 no proponen formalmente tipos de activos de información. Por ello, durante la primera iteración del análisis Delphi se refirió el catálogo de elementos de MAGERIT [39] para elaborar uno propio. A continuación, se muestra la propuesta de "tipos de activos de información" que fue validada durante la segunda iteración con los expertos del análisis Delphi.

Tabla 41. Tipos de activos de la ontología, basados en MAGERIT

Tipos de Activos según MAGERIT		Tipos de Activos (propios)
Grupo	**Definición**	
Datos / Información	La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.	Digital
Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.	Físicos
Servicios	Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.	Servicio
Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.	
Software (Aplicaciones informáticas)	Con múltiples denominaciones (programas, aplicativos, etc.) se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático.	Aplicación
Hardware (Equipamiento informático)	Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, responsables del procesado o la transmisión de datos.	Hardware
Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.	Locación
Personal	Personas relacionadas con los sistemas de información.	Personal

Fuente: Elaboración propia. Utilizando fuentes de MAGERIT Libro II - Catálogo de elementos [39].

La Clase Amenaza y las Subclases Tipo de Amenaza

El estándar ISO 27001:2022 [18] propone los siguientes tipos de amenazas en su numeral A.2.5.1, según se detalla a continuación, con algunos ejemplos:

Tabla 42. Tipos de amenazas de la ontología

Tipos de Amenazas	No.	Descripción
Físicas	TP01	Fuego
	TP06	Polvo, corrosión, congelación
Naturales	TN01	Fenómeno climático
	TN06	Pandemia/fenómeno epidémico
Fallos de Infraestructura	TI01	Fallo de un sistema de suministro
	TI08	Pulsos electromagnéticos
Fallos Técnicos	TT01	Fallo del dispositivo o sistema.
	TT03	Violación de la mantenibilidad del sistema de información.
Humanas	TH01	Terrorismo, ataque, sabotaje
	TH26	Detección de posición
Compromiso de Funciones y Servicios	TC01	Error de uso
	TC02	Abuso de derechos o permisos
	TC03	Falsificación de derechos o permisos
	TC04	Negación de acciones
Organizacionales	TO01	Falta de personal
	TO02	Falta de recursos
	TO03	Fallo de los proveedores de servicios.
	TO04	Violación de leyes o reglamentos.

Fuente: ISO/IEC 27005:2022 [20]

La Clase Vulnerabilidad y las Subclases Tipo de Vulnerabilidad

El estándar ISO 27001:2022 [18] propone los siguientes tipos de vulnerabilidades en su numeral A.2.5.2, según se detalla a continuación, con algunos ejemplos:

Tabla 43. Tipos de vulnerabilidades de la ontología

Tipos de Vulnerabilidades	No.	Descripción
Hardware	VH01	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento
	VH10	Copia incontrolada
Software	VS01	Pruebas de software nulas o insuficientes
	VS22	No producir informes de gestión.
Servicio de Red	VN01	Mecanismos insuficientes para la prueba del envío o recepción de un mensaje
	VN10	Conexiones de red pública no protegidas
Personal	VP01	Ausencia de personal
	VP08	Ineficaces o falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Ubicación	VS01	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones.
	VS04	Protección física insuficiente del edificio, puertas y ventanas.
Organización	VO01	No se ha desarrollado un procedimiento formal para el registro y baja de usuarios, o su implementación es ineficaz.
	VO28	Procedimientos de cumplimiento de disposiciones sobre derechos intelectuales no desarrollados, o su implementación es ineficaz

Fuente: ISO/IEC 27005:2022 [20]

La Clase Control y las Subclases Tipo de Control

El estándar ISO 27001:2022 [18] propone tipos de controles en su Anexo A, y los desarrolla en el cuerpo del estándar ISO 27002:2022 [19], según se detalla a continuación, con algunos ejemplos:

Tabla 44. Extracto de controles según la ISO/IEC 27002:2022

Tipos de Controles	Número	Control
Controles organizacionales	**5.1**	Políticas para la seguridad de la información
	5.37	Procedimientos operativos documentados
Controles de personas	**6.1**	Filtración de personal
	6.8	Reportar eventos de seguridad de la información
Controles físicos	**7.1**	Perímetros de seguridad física
	7.14	Eliminación segura o reutilización de equipos
Controles tecnológicos	**8.1**	Dispositivos terminales de usuario
	8.34	Protección de los sistemas de información durante las pruebas de auditoría

Fuente: ISO/IEC 27001:2022 [18] e ISO/IEC 27002:2022 [19]

En todos los casos expuestos se han mostrado solo algunos ejemplos de las clases y subclases propuestas, debido a su extensión. En particular, en los casos de las amenazas, vulnerabilidades y controles las normas ISO presentan las siguientes cantidades de registros:

- Amenazas: 57 registros, agrupados en 7 tipos.
- Vulnerabilidades: 82 registros, agrupados en 6 tipos.
- Controles: 93 registros, agrupados en 4 tipos.

Estos conjuntos de datos presentan relaciones complejas entre sí, que son desarrolladas en la siguiente sección.

5.3.3. Relaciones semánticas

A partir de las clases y subclases se mencionan algunas de las relaciones construidas con el apoyo de los especialistas mediante la segunda iteración del ejercicio Delphi:

La relación entre los tipos de activos de información versus las amenazas.
Si bien el estándar ISO 27005:2022 [20] propone hasta 57 amenazas, no todas ellas son aplicables a todo tipo de activo de información. Según se ver en el ejemplo:

Tabla 45. Ejemplos de relación activos - amenazas

Activo	Tipo de Activo	Aplica	Categoría	No.	Descripción
Auditor	Personal	SI	Amenazas Físicas	TP01	Fuego
		SI		TP02	Agua
		SI		TP03	Contaminación, radiación nociva.
		SI		TP04	Grave accidente
		SI		TP05	Explosión
		NO		TP06	Polvo, corrosión, congelación.
		NO	Amenazas Naturales	TN01	Fenómeno climático
		NO		TN02	Fenómeno sísmico
		NO		TN03	Fenómeno volcánico
		NO		TN04	Fenómeno meteorológico
		NO		TN05	Inundación
		SI		TN06	Pandemia/fenómeno epidémico
		NO	Fallos de Infraestructura	TI01	Fallo de un sistema de suministro
		NO		TI02	Fallo del sistema de refrigeración o ventilación.
		NO		TI03	Pérdida de suministro de energía
		NO		TI04	Fallo de una red de telecomunicaciones
		NO		TI05	Fallo de los equipos de telecomunicaciones.
		NO		TI06	Radiación electromagnética
		SI		TI07	Radiación termal
		NO		TI08	Pulsos electromagnéticos

Fuente: Elaboración propia. Utilizando fuentes de la ISO/IEC 27005:2022 [20].

No existe correlación entre los tipos de activo y amenaza. Es decir, no existe una relación semántica que implique que un activo de tipo “Personal” sea afectado todas las amenazas “Físicas”. Por esto, se ha rediseñado esta clasificación, para que cuente con categorías afines a las de los activos de información. Se han integrado amenazas similares o redundantes, para evitar ambigüedades y, en los casos en que una amenaza aplica a distintos tipos de activos, se han duplicado para establecer las relaciones.

Tabla 46. Extracto de la matriz de amenazas (mejorada) versus activos

Activos	Amenazas		
Tipos de Activos	Tipos de Amenazas	ID	Descripción
Digital	Digital	AD1	Corrupción de datos
		AD2	Envío o distribución de malware.
Físico	Físico	AF1	Fuego
		AF2	Robo de soportes o documentos.
Servicio	Servicio	AS1	Fallo del dispositivo o sistema.
		AS2	Espionaje remoto
Aplicación	Aplicación	AA1	Error de uso
		AA2	Abuso de derechos o permisos
Hardware	Hardware	AH1	Fuego
		AH2	Fallo de un sistema de suministro
Locación	Locación	AL1	Fenómeno sísmico
		AL2	Fuego
Personal	Personal	AP1	Fenómeno sísmico
		AP2	Pandemia/fenómeno epidémico

Fuente: Elaboración propia. Utilizando fuentes de la ISO/IEC 27005:2022 [20]

La relación entre las propiedades de seguridad de información de los requisitos de la información versus las amenazas.

De manera similar al caso anterior, existe una relación entre las amenazas aplicables y las propiedades de la seguridad de información (Confidencialidad, Integridad y Disponibilidad) que son relevantes para la información que procesa o aloja el activo. En este aspecto el estándar ISO 27005:2022 [20] tampoco establece esta relación.

Según se puede ver en el siguiente ejemplo, para un activo de información que tiene requisitos asociados con la "Confidencialidad", no todas las amenazas serían aplicables:

Tabla 47. Ejemplos de relación propiedad de seguridad – amenazas

Activos				¿Aplica a la propiedad?	Amenazas	
Información	**Requisito**	**Propiedad**	**Activo**		**ID**	**Descripción**
Plan de Auditoría	Solo el equipo auditor puede acceder al plan de auditoría	Confidencialidad	Servicio de alojamiento de archivos en la nube (OneDrive)	NO	AD1	Corrupción de datos
				SI	AD2	Envío o distribución de malware.
				SI	AD3	Espionaje remoto
				SI	AD4	Abuso de derechos o permisos

Fuente: Elaboración propia. Utilizando fuentes de la ISO/IEC 27005:2022 [20]

Es decir, si mi análisis se enfoca en identificar riesgos relacionados a la pérdida de confidencialidad, no debería distorsionar mis resultados permitiendo una amenaza que afecta a la integridad (En el ejemplo: AD1 – Corrupción de datos).

Del ejemplo mostrado, se evidencia que hace falta complementar el modelo con un atributo que permita a las amenazas establecer si tienen relación con una o muchas de las propiedades de seguridad de información.

Las propiedades que pueden presentar los requisitos de seguridad de información corresponden a la: confidencialidad, integridad y disponibilidad. La implementación de esta mejora se muestra en la siguiente tabla:

Tabla 48. Extracto de la matriz de amenazas (mejorada)

Amenazas			Propiedades de Seguridad de Información		
Tipos de Amenazas	**ID**	**Descripción**	**Confidencialidad**	**Integridad**	**Disponibilidad**
Digital	AD1	Corrupción de datos	NO	SI	SI
	AD2	Envío o distribución de malware.	SI	SI	SI
Físico	AF1	Fuego	NO	SI	SI
	AF2	Robo de soportes o documentos.	SI	NO	SI
Servicio	AS1	Fallo del dispositivo o sistema.	NO	SI	SI
	AS2	Espionaje remoto	SI	NO	NO
Aplicación	AA1	Error de uso	NO	SI	SI
	AA2	Abuso de derechos o permisos	SI	NO	NO
Hardware	AH1	Fuego	NO	SI	SI
	AH2	Fallo de un sistema de suministro	NO	NO	SI
Locación	AL1	Fenómeno sísmico	NO	NO	SI
	AL2	Fuego	NO	SI	SI
Personal	AP1	Fenómeno sísmico	NO	NO	SI
	AP2	Pandemia/fenómeno epidémico	NO	NO	SI

Fuente: Elaboración propia. Utilizando fuentes de la ISO/IEC 27005:2022 [20]

La relación entre las amenazas y activos versus las vulnerabilidades.
Si bien el estándar ISO 27005:2022 [20] propone hasta 82 amenazas, como en los casos anteriores, no existe una forma de correlacionarla directamente con las amenazas y los activos que influyen en su aplicabilidad.

Por este motivo, se ha aplicado una normalización similar a la aplicada a las amenazas, bajo el siguiente esquema:

Tabla 49. Extracto de la matriz de vulnerabilidades (adaptada)

Tipos de Vulnerabilidades	ID	Descripción
Digital	VD1	Auditorías (supervisión) no realizadas de forma regular
	VD2	Insuficiente o inexistente política de escritorio limpio
Físico	VF1	Control insuficiente de los activos fuera de las instalaciones
	VF2	Procedimientos para el manejo de información clasificada no desarrollados o su implementación es ineficaz
Servicio	VS1	Líneas de comunicación desprotegidas
	VS2	Arquitectura de red insegura
Aplicación	VA1	Pruebas de software nulas o insuficientes
	VA2	Configuración de parámetros incorrecta
Hardware	VH1	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento
	VH2	Susceptibilidad a la humedad, al polvo y a la suciedad.
Locación	VL1	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones.
	VL2	Red eléctrica inestable
Personal	VP1	Procedimientos de contratación inadecuados
	VP2	Formación insuficiente en seguridad.

Fuente: Elaboración propia. Utilizando fuentes de la ISO/IEC 27005:2022 [20]

La relación entre los controles versus las vulnerabilidades.
Como parte del proceso de normalización, se han tomado los 93 controles propuestos en el Anexo A del estándar ISO 27001:2022 [18] y desarrollados en el estándar ISO/IEC 27002:2022 [19]. Estas clases se han reclasificado como en los casos anteriores:

Tabla 50. Extracto de la matriz de controles (adaptada)

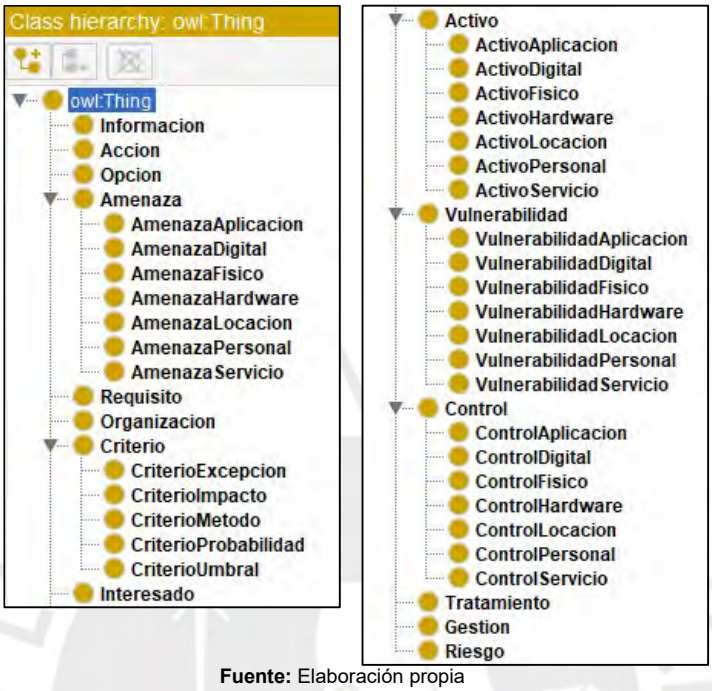
Tipos de Controles	ID	Descripción	Ref. 27002
Digital	CD1	Políticas para la seguridad de la información	**5.1**
	CD2	Control de acceso	**5.15**
Físico	CF1	Clasificación de la información	**5.12**
	CF2	Etiquetado de la información	**5.13**
Servicio	CS1	Gestión del cambio	**8.32**
	CS2	Gestión de vulnerabilidades técnicas	**8.8**
Aplicación	CA1	Protección contra malware	**8.7**
	CA2	Requisitos de seguridad de la aplicación	**8.26**
Hardware	CH1	Gestión del cambio	**8.32**
	CH2	Emplazamiento y protección de equipos	**7.8**
Locación	CL1	Perímetros físicos de seguridad	**7.1**
	CL2	Monitoreo de seguridad física	**7.4**
Personal	CP1	Términos y condiciones de empleo	**6.2**
	CP2	Proceso Disciplinario	**6.4**

Fuente: Elaboración propia. Utilizando fuentes de la ISO/IEC 27002:2022 [19]

Cabe destacar que, debido a la importancia que tiene el identificador de cada control en la gestión de riesgos, se ha mantenido el código identificador de control, establecido en el estándar ISO/IEC 27002:2022 [19].

Como resultado de los cambios realizados, tras aplicar los cambios obtenidos a partir del análisis Delphi, el modelo presenta la siguiente estructura:

Figura 23. Modelo clases de la GRSI (Protégé)



Fuente: Elaboración propia

5.4. Discusión de resultados

Se ha utilizado la información recopilada en el capítulo 4, para elaborar y refinar una ontología de GRSI a lo largo del presente capítulo. En base a los resultados obtenidos se puede precisar lo siguiente:

- Los conceptos utilizados han sido tomados, principalmente, de los términos recopilados desde el estándar ISO/IEC 27005 [20]. Sin embargo, para la sección de la ontología relativa a los activos y tipos de activos se ha utilizado la norma española MAGERIT [40].
- Si bien es cierto que las normas referidas presentan categorías y relaciones válidas, estas no permiten dar semántica a las relaciones entre los activos, amenazas, vulnerabilidades y controles. Por ello, ha sido necesario realizar una categorización propia para estas clases, a fin de poder explotar el significado de las relaciones que existen entre ellas.
- Se destaca el uso del método Delphi como una herramienta para refinar y validar el modelo, con el apoyo especialistas del dominio. Solución que se aplica, según Reguant [82], en “situaciones de incertidumbre o cuando se carece de información objetiva”, que es el caso del problema investigado.

6. Gestor de riesgos de seguridad de información

A continuación, se presenta el diseño, implementación y pruebas de la solución que permite automatizar el proceso de Gestión de Riesgos de Seguridad de Información (GRSI). Para el diseño se han elaborado diagramas de flujo que representan el comportamiento funcional de la aplicación, para el diseño se muestran los módulos creados para el procesamiento de la información y, para las pruebas se ha aplicado un análisis Delphi, a fin de verificar que los resultados son los adecuados.

6.1. Diseño de la solución

Se ha estructurado una solución organizada en módulos, que de manera similar al proceso de GRSI, se organiza según la siguiente arquitectura:

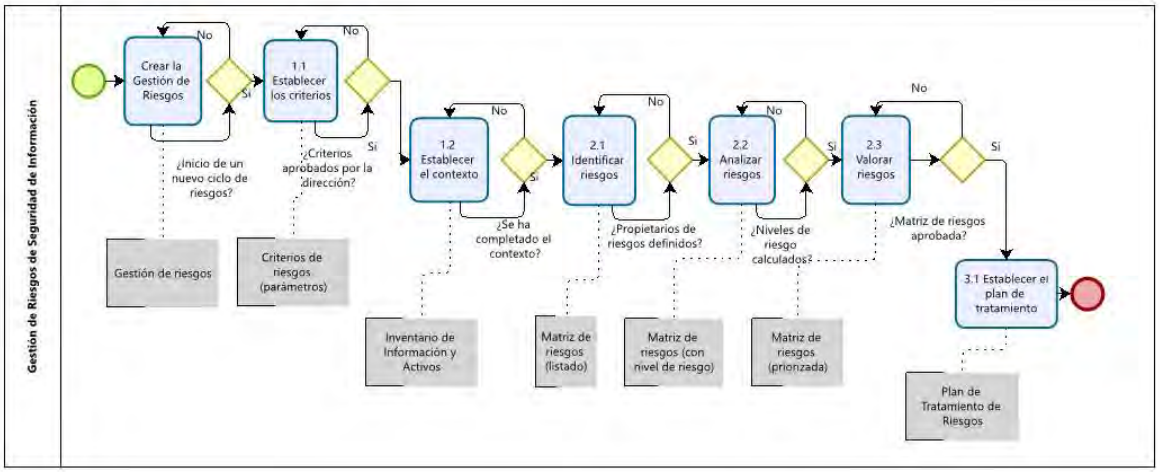
Tabla 51. Arquitectura de la aplicación

Módulo	Componente
1. Establecer el Contexto	1.1 Establecer los criterios de riesgos
	1.2 Establecer el contexto de la organización
2. Evaluar el riesgo	2.1 Identificar los riesgos
	2.2 Analizar los riesgos
	2.3 Valorar los riesgos
3. Tratar el riesgo	3.1 Establecer el plan de tratamiento

Fuente: Elaboración propia.

A partir de esta distribución, se han diagramado los flujos de información de cada uno de los componentes. Cabe destacar que, si bien no es mostrado como un componente, la creación de una “gestión de riesgos” es el paso inicial de crear una instancia del proceso, para un periodo en específico:

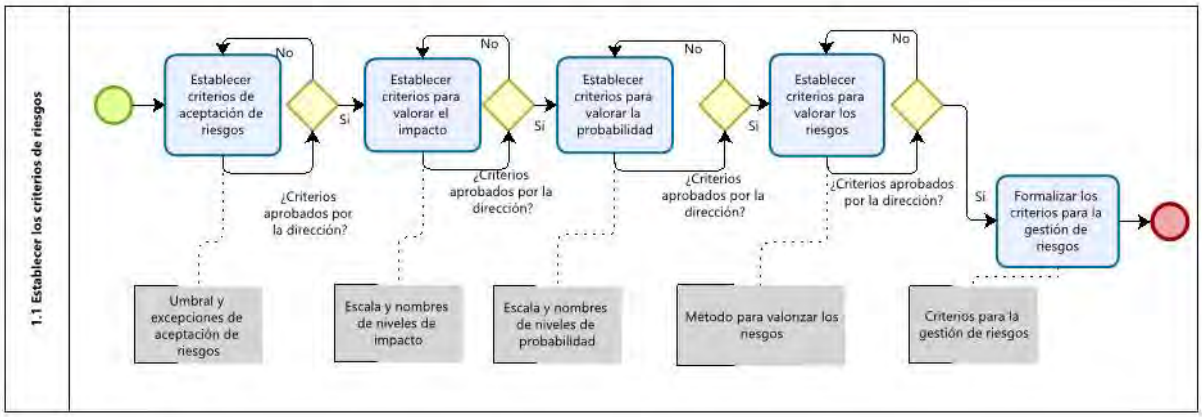
Figura 24. Diagrama general del proceso



Fuente: Elaboración propia.

- **Establecer los criterios de riesgos.** Se parametrizan los atributos que permitirán establecer la forma de calcular el valor del riesgo (probabilidad, impacto), el umbral de aceptación del riesgo, así como también establecer las excepciones en las que el riesgo podría ser aceptado.

Figura 25. Diagrama del sub - proceso: Establecer los criterios de riesgos

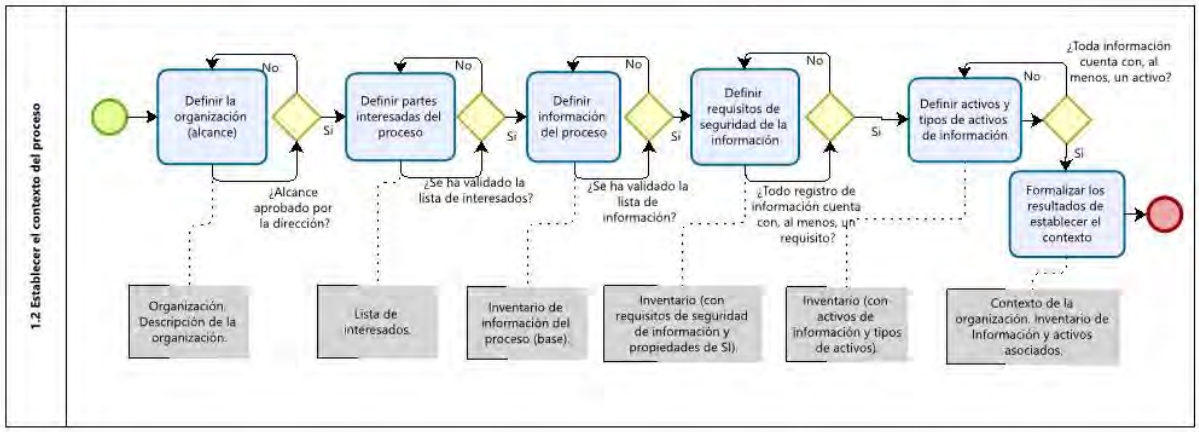


Fuente: Elaboración propia.

Establecer el contexto. Para la fase inicial "Establecer el contexto de la organización", se han aplicado dos subprocesos:

- **Establecer el contexto del alcance.** Se define la forma de establecer el alcance de la gestión de riesgos a nivel de la organización, su información, sus requisitos, y aquellos activos de información involucrados.

Figura 26. Diagrama del sub - proceso: Establecer el contexto del proceso



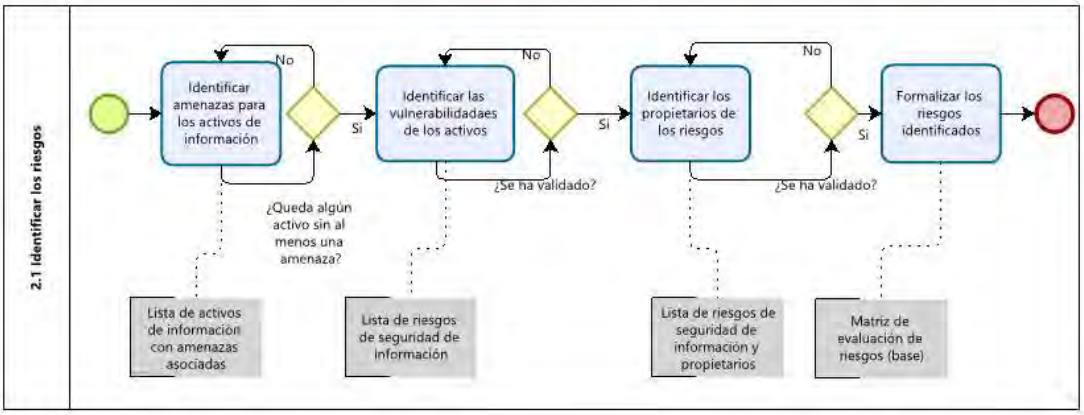
Fuente: Elaboración propia.

Evaluar el riesgo

Para la fase de “Evaluar el riesgo”, se han aplicado tres subprocesos:

- **Identificar el riesgo.** Se identifican para cada activo las posibles amenazas y vulnerabilidades que existen y que podrían dar lugar a un riesgo identificado, que también tiene un propietario asignado.

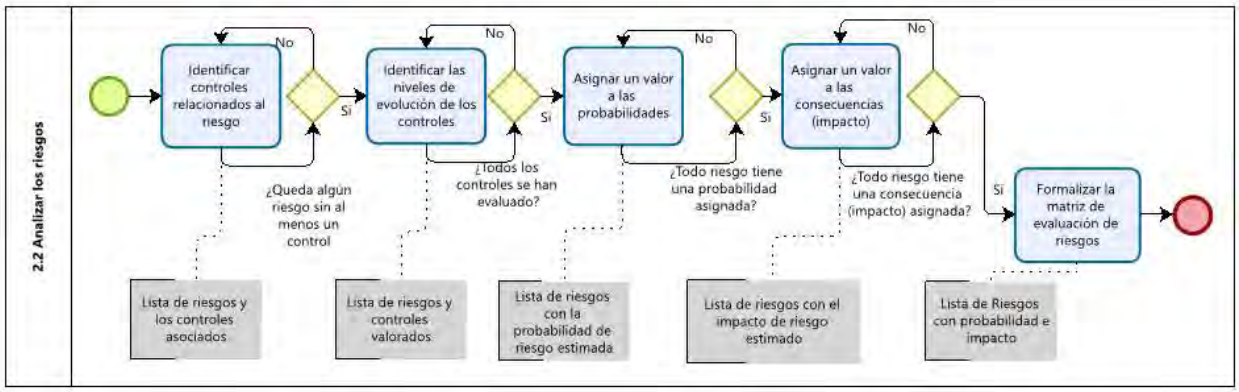
Figura 27. Diagrama del sub - proceso: Identificar los riesgos



Fuente: Elaboración propia.

- **Analizar el riesgo.** Se revisa el riesgo identificado respecto a los controles vigentes en la organización ya su nivel de efectividad; para determinar la probabilidad, impacto y el respectivo nivel de riesgo resultante.

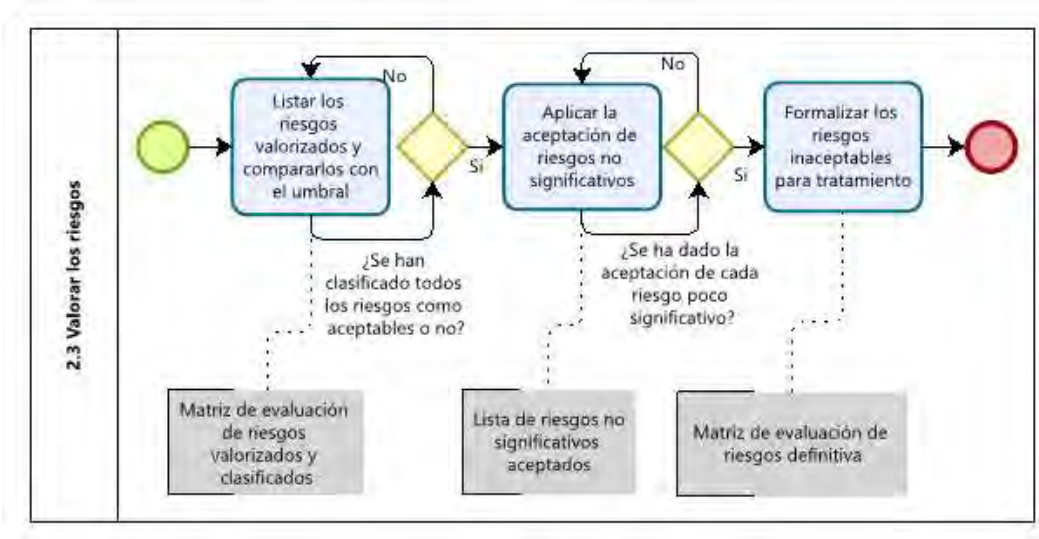
Figura 28. Diagrama del sub - proceso: Analizar los riesgos



Fuente: Elaboración propia.

- **Valorar el riesgo.** Se compara, para cada riesgo, los niveles obtenidos contra el umbral de aceptación de riesgos, establecido para la organización en el periodo de gestión de riesgos. Se definen así los riesgos de valor aceptable e inaceptable.

Figura 29. Diagrama del sub - proceso: Valorar los riesgos

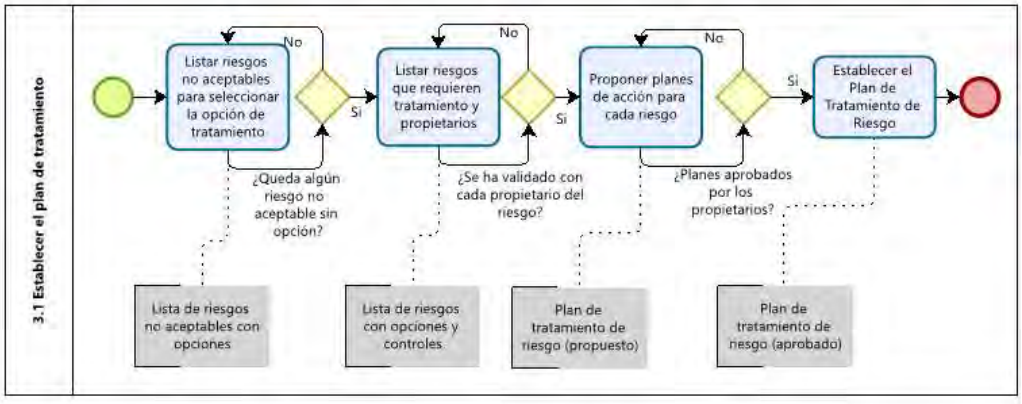


Fuente: Elaboración propia.

Tratar el riesgo. Para la fase de "Tratar el riesgo", se ha un subproceso:

- **Establecer el plan de tratamiento.** Donde se define la forma de establecer el alcance de la gestión de riesgos a nivel de organización, procesos, información y activos involucrados. Donde se define la forma de establecer el alcance de la gestión de riesgos a nivel de organización, procesos, información y activos involucrados.

Figura 30. Diagrama del sub - proceso: Establecer el plan de tratamiento



Fuente: Elaboración propia.

6.2. Implementación de la solución

Como base para la implementación se generó un prototipo básico utilizando el lenguaje de programación JAVA, tal como se especificó en el capítulo 2. Mediante este código se creó un modelo con las clases principales alrededor del riesgo (activo, vulnerabilidad y amenaza), según se muestra a continuación:

Figura 31. Código fuente del prototipo inicial

```
import org.apache.jena.ontology.*;
import org.apache.jena.rdf.model.*;

public class Gestor {
    public static void main(String[] args) {
        // Modelo base
        OntModel m = ModelFactory.createOntologyModel(OntModelSpec.OWL_MEM);

        // Namespace: Gestión de Riesgos de Seguridad de Información (GRSI)
        String NS = "http://grsi.org/grsi#";
        m.setNsPrefix("grsi", NS);

        // Classes: riesgo, amenaza, vulnerabilidad, y activo
        OntClass riesgo = m.createClass(NS + "riesgo");
        OntClass amenaza = m.createClass(NS + "amenaza");
        OntClass vulnerabilidad = m.createClass(NS + "vulnerabilidad");
        OntClass activo = m.createClass(NS + "activo");

        // Propiedades para tieneAmenaza, tieneVulnerabilidad, y afectaActivo
        DatatypeProperty tieneAmenaza = m.createDatatypeProperty(NS + "tieneAmenaza");
        tieneAmenaza.addDomain(riesgo);
        tieneAmenaza.addRange(amenaza);

        DatatypeProperty tieneVulnerabilidad = m.createDatatypeProperty(NS + "tieneVulnerabilidad");
        tieneVulnerabilidad.addDomain(riesgo);
        tieneVulnerabilidad.addRange(vulnerabilidad);

        ObjectProperty afectaActivo = m.createObjectProperty(NS + "afectaActivo");
        afectaActivo.addDomain(riesgo);
        afectaActivo.addRange(activo);

        // Crear el riesgo
        Individual instanciaRiesgo = m.createIndividual(NS + "instanciaRiesgo", riesgo);
        instanciaRiesgo.addProperty(tieneAmenaza, "Espionaje Remoto");
        instanciaRiesgo.addProperty(tieneVulnerabilidad, "Registros insuficientes de incidencias");
        instanciaRiesgo.addProperty(afectaActivo, m.createIndividual(NS + "Servicio de alojamiento en la nube"));

        // Imprimir
        m.write(System.out, "RDF/XML-ABBREV");
    }
}
```

Fuente: Elaboración propia.

Sin embargo, versiones posteriores incorporaron la lectura del modelo OWL, como base de información, así como también las interfases de usuario, como medio para la interacción, según se detalla a continuación:

Figura 32. Interfaz principal de la solución

Fuente: Elaboración propia.

Para organizar las funcionalidades de la solución se ha organizado la siguiente estructura de módulos y componentes, acorde a las etapas de la gestión de riesgos:

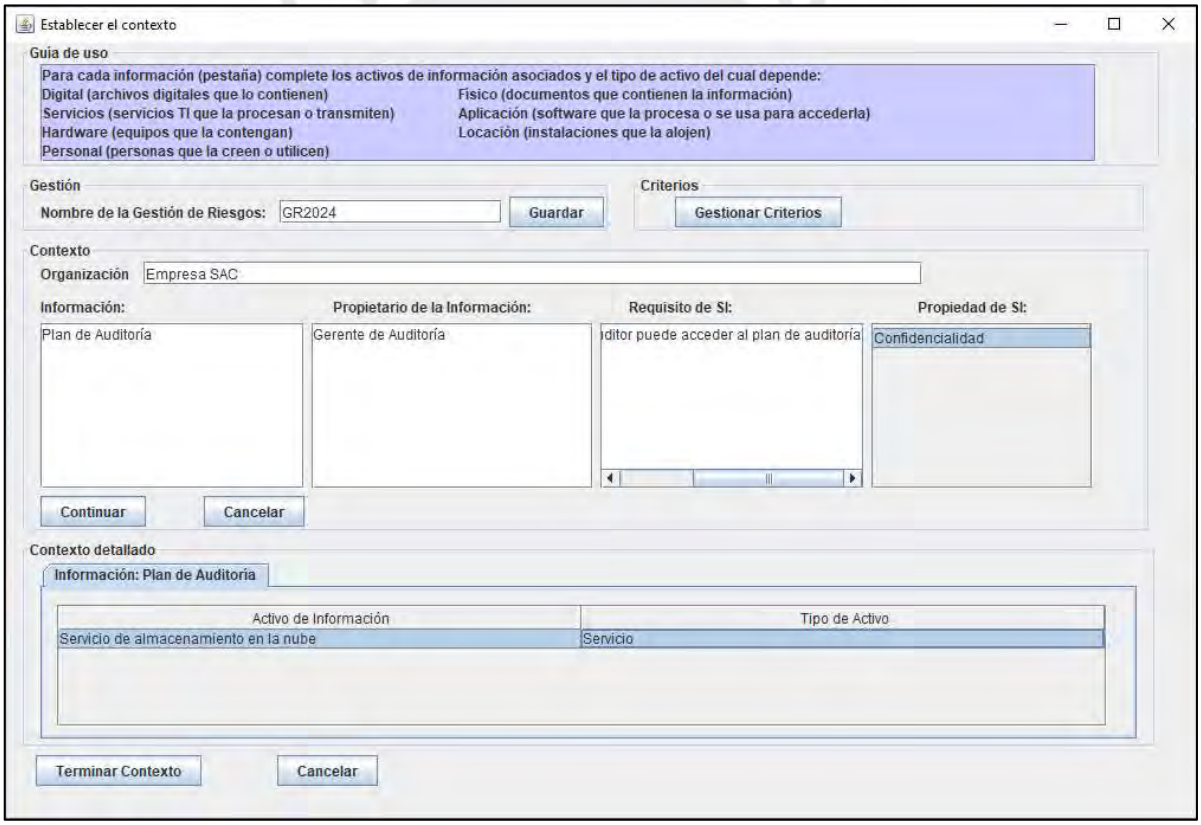
Tabla 52. Arquitectura de módulos y componentes

Módulo	Componentes
1. Contexto	1.0 Crear la gestión de riesgos
	1.1 Establecer el contexto del proceso
	1.2 Establecer los criterios de riesgos
2. Evaluar el riesgo	2.1 Identificar los riesgos
	2.2 Analizar los riesgos
	2.3 Valorar los riesgos
3. Tratar el riesgo	3.1 Establecer el plan de tratamiento

Fuente: Elaboración propia.

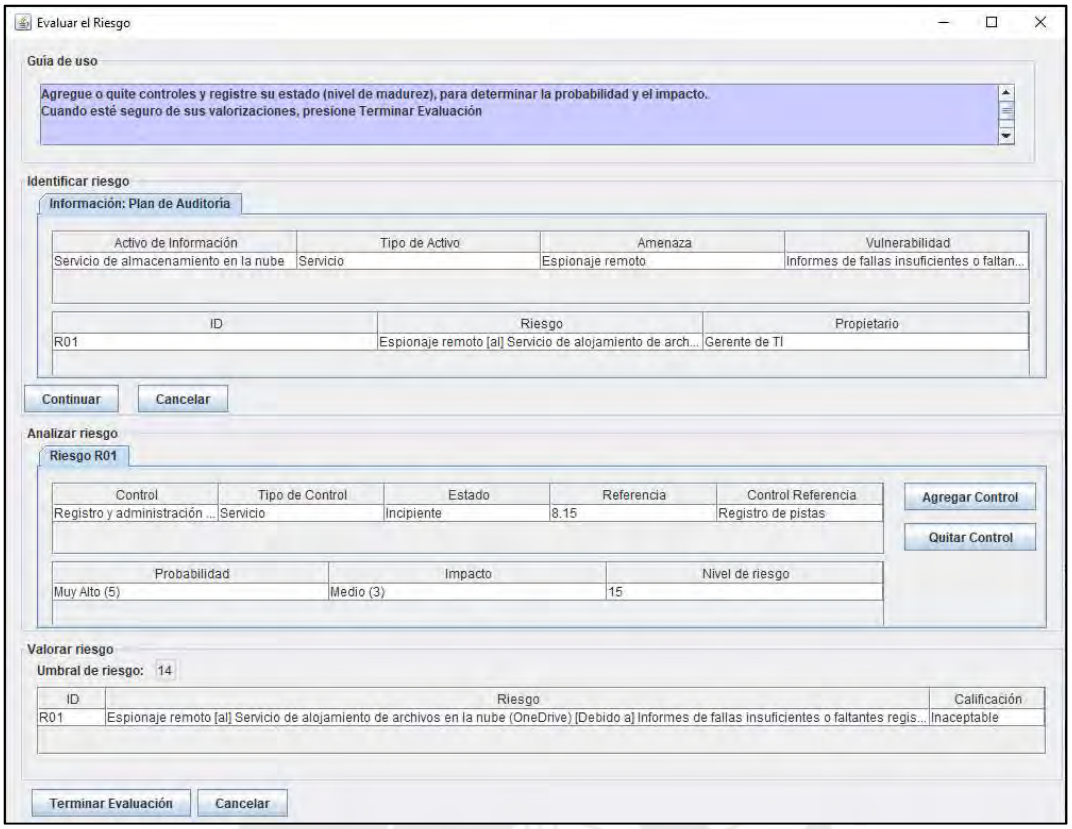
Si bien los componentes se implementaron originalmente bajo una distribución diferente, las pruebas posteriores (expuestas en el numeral 6.3 de esta investigación) conllevaron a que estas se integren en una ventana por módulo, diseño que se muestra a continuación:

Figura 33. Interfaz del módulo "Establecer el Contexto"



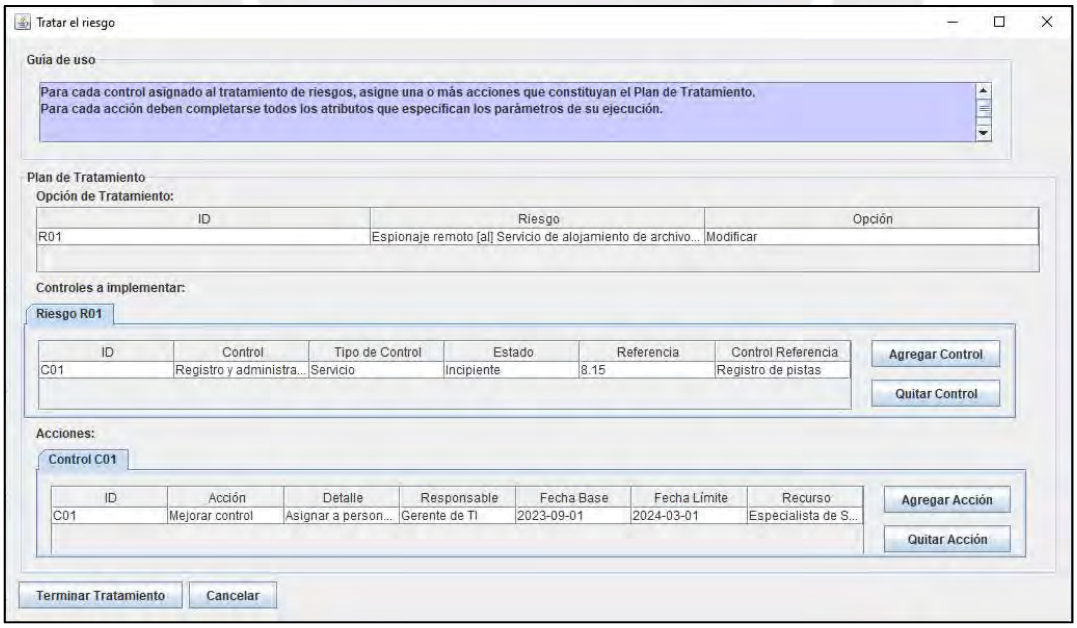
Fuente: Elaboración propia.

Figura 34. Interfaz del módulo "Evaluar el Riesgo"



Fuente: Elaboración propia.

Figura 35. Interfaz del módulo "Tratar el Riesgo"



Fuente: Elaboración propia.

6.3. Prueba de la solución

De manera similar al capítulo 5, se ha considerado validar la adecuada funcionalidad y los resultados obtenidos al usar el aplicativo a través del método Delphi. Se ha aplicado una adaptación, considerando nuevamente la metodología la propuesta por Reguant [82], con las etapas de definición (objetivos y alcance), conformación del grupo (especialistas), ejecución de rondas (iteraciones) y resultados.

Definición. Se han establecido las siguientes condiciones para el análisis de la aplicación:

Tabla 53. Definiciones para la aplicación del método Delphi

Objetivo	Identificar debilidades y errores en las funciones del aplicativo informático y los resultados que muestra.
Alcance	Módulos de contexto, evaluación de riesgos y tratamiento de riesgos en el sistema informático.
Fuentes de información	Cuestionario sobre el uso de las funcionalidades y resultados obtenidos. Copia de archivos: grsi.jar; ejecutable.bat, grsi_final.owl

Fuente: Elaboración propia.

Conformación del grupo. Los requisitos de perfiles de expertos en GRSI han sido los mismos que los utilizados en el capítulo 5, por lo que se ha utilizado el mismo universo de especialistas. Sin embargo, cabe destacar que se les solicitó un requisito adicional, de carácter técnico: contar con equipos que tengan instalada la versión 8 o superior del JRE[4], para ejecutar el archivo de extensión JAR. Debido a que todos confirmaron este requisito, se ha contado con la participación de los 15 especialistas involucrados en el análisis anterior.

Ejecución de rondas. Se muestra un resumen del cuestionario, así como también de los resultados de las dos iteraciones realizadas:

Primera Iteración:

Se facilita a los especialistas los archivos “grsi.jar”; “ejecutable.bat”, “grsi_final.owl” y se monitorea que hayan podido ejecutarlos sin inconveniente. Además, un cuestionario relacionado a una “prueba de recorrido” sobre el uso de la aplicación a lo largo de los tres módulos. Se han formulado 25 preguntas en total:

Tabla 54. Resumen de preguntas y resultados de la iteración 1

#	Grupo de consultas	Resultados obtenidos
1	Deficiencias en módulo Contexto – Componente “Establecer los criterios” (3 consultas)	a) La “Gestión” debería ser lo primero en definirse, antes que los criterios. Además, los criterios son parámetros de la gestión y podrían estar en una ventana aparte, porque confunden al usuario. b) Los criterios de probabilidad e impacto deberían tener una descripción que defina que es “muy bajo” o “muy alto”, sino la calificación puede ser ambigua.
2	Deficiencias en módulo Contexto – Componente “Establecer el contexto” (4 consultas)	c) La matriz de información y sus activos es demasiado densa para visualizarla. Debería desdoblarse en dos paneles “Contexto” (para la información) y “Contexto detallado” (para los activos).
3	Deficiencias en módulo Evaluar – Componente “Identificar riesgos” (4 consultas)	d) La matriz de identificación de riesgos no muestra claramente sus contenidos, podría mejorarse su presentación o dividirse en dos bloques. e) Debería mostrarse un identificador del riesgo a manera de código, que permita correlacionarlo con las siguientes etapas del formulario.

[4] Java Runtime Environment

#	Grupo de consultas	Resultados obtenidos
4	Deficiencias en módulo Evaluar – Componente "Analizar riesgos" (4 consultas)	f) La probabilidad y el impacto deberían mostrar también el valor numérico que tienen asignado, de manera que se pueda corroborar que el nivel de riesgo es el adecuado. g) Los íconos de los botones "+" y "-" no son claros, deberían mostrarse "agregar control" y "quitar control".
5	Deficiencias en módulo Evaluar – Componente "Valorar riesgos" (4 consultas)	h) Debería mostrarse el "umbral de riesgos" que fue definido previamente, ya que el usuario no sabría por qué su riesgo es aceptable o inaceptable. i) No es necesario volver a poner el nombre del riesgo, podría usarse un código o identificador de riesgo, para utilizarlo como referente en esta fase.
6	Deficiencias en módulo Tratar – Componente "Tratar riesgos" (4 consultas)	j) Para cada opción de tratamiento riesgo pueden existir varios controles y cada control puede requerir varias acciones, no es práctico modelarlo en una única matriz, deberían dividirse en: opciones, controles y acciones, por separado. k) Los íconos de los botones "+" y "-" pueden generar dudas, deberían mostrarse "agregar control" / "quitar control" y "agregar acción" / "quitar acción".
7	Oportunidades de mejora generales. (2 consultas)	l) No todos los conceptos usados son intuitivos para un usuario no especializado, debería contarse con una funcionalidad de ayuda que oriente a los usuarios respecto a los pasos a seguir y los atributos que registrar.
8	Beneficios no esperados del uso de la herramienta. (1 consulta)	m) Reducción del tiempo de identificación de amenazas, vulnerabilidades y controles. n) Independencia del uso de base de datos como repositorio de información.

Fuente: Elaboración propia.

Como resultado de esta iteración se han realizado mejoras sobre el sistema. Cabe destacar que todos los cuestionamientos corresponden a mejoras funcionales, pero ninguno corresponde a errores en los resultados mostrados.

Segunda Iteración:

Se facilitó a los especialistas los archivos de sistema actualizados ("grsi.jar"; "ejecutable.bat", "grsi_final.owl) y se han formulado nuevas preguntas (55), derivadas de las anteriores:

Tabla 55. Resumen de preguntas y resultados de la iteración 2

#	Grupo de consultas	Referencia Iteración 1	Resultados obtenidos
1	Propuesta de mensajes orientativos para usuarios de la sección "Guía de uso" (14 consultas).	l)	Recomendaciones para mejorar la redacción (7 comentarios)
2	Propuesta de descripciones que acompañen a los parámetros definidos en la sección "Criterios" (15 consultas).	b)	Recomendaciones para mejorar la redacción (3 comentarios)
3	Consultas sobre la usabilidad de las funciones y la visibilidad de la información (22 consultas).	a), c) – k)	Sin correcciones.
4	Consulta sobre la conformidad de los resultados obtenidos (2 consultas).	-	Conformidad sobre la evaluación de riesgos (total) Conformidad sobre el tratamiento de riesgos (total)
5	Consulta sobre si la solución informática propuesta mitiga errores en el proceso de GRSI, en las etapas de evaluación y tratamiento de riesgos (2 consultas).	-	Calificación en etapa evaluación (4/5). Calificación en etapa tratamiento (4/5).

Fuente: Elaboración propia.

En la tabla anterior, se destaca el grupo de consultas número 5, donde se solicitó a los usuarios que, para las etapas de evaluación y tratamiento de riesgos, indiquen si la solución les ha ayudado a mitigar la posibilidad de errores, según la siguiente escala:

- (1) Ninguno. No existe ningún beneficio.
- (2) No significativo. Se previenen errores, pero no son relevantes.
- (3) Perceptible. Se previenen algunos errores relevantes.
- (4) Significativo. Se previenen la mayoría de los errores posibles.
- (5) Absoluto. Se evita completamente la posibilidad de error.

El resultado de las consultas referidas en ambos casos (evaluación y tratamiento) ha sido el nivel (4) "Significativo".

Tras esta iteración se han recopilado algunas mejoras de forma; además, se ha validado que los resultados mostrados por el sistema son correctos en todos los casos probados.

Resultados. Como resultado de las dos iteraciones realizadas se han obtenidos los siguientes resultados:

- Sistema informático actualizado, aplicando las mejoras recogidas de ambas iteraciones.
- Registros de las conformidades funcionales y de resultados, sobre las pruebas realizadas por los usuarios especialistas.

6.4. Discusión de resultados

El sistema informático que utiliza la ontología, para soportar un proceso de GRSI, ha sido diseñado, implementado y probado; y como resultado de estas actividades, se realizan las siguientes precisiones:

- La arquitectura de la solución informática ha sido diseñada de manera análoga a las del proceso de GRSI; es decir, los módulos de la aplicación corresponden al contexto, evaluación y tratamiento de riesgos.
- Respecto a la implementación, se han atendido las especificaciones detalladas en el numeral 2.4. (“Métodos y sus procedimientos”) de esta investigación, utilizando el lenguaje de programación JAVA y empleando como soporte de datos el formato de archivo OWL.
- Las pruebas al sistema se han realizado mediante la aplicación del método Delphi, con un equipo de especialistas en el ámbito del proceso de GRSI. Como resultado de estas interacciones se han podido recopilar algunas mejoras sobre el diseño del sistema.
- Durante la primera iteración, los usuarios refirieron dos beneficios del uso de la aplicación: la reducción del tiempo de indagación respecto a las amenazas, vulnerabilidades y controles; así como también, la facilidad de no depender de la instalación de una base de datos, al trabajar en un archivo OWL, que permite la persistencia de la información.
- Durante la segunda iteración ha sido posible validar, con todos los especialistas involucrados en el análisis Delphi, que los resultados obtenidos desde la aplicación son adecuados. Además, que los mecanismos ontológicos implementados, aunque no evitan de manera absoluta los errores durante el proceso de GRSI, sí mitigan significativamente su ocurrencia.

7. Conclusiones y trabajos futuros

A continuación, se presentan las conclusiones extraídas del proceso de Gestión de Riesgos de Seguridad de Información (GRSI) implementado utilizando una ontología. Asimismo, se plantean algunas propuestas de investigaciones futuras en planos que no han sido cubiertos por la presente investigación:

7.1. Conclusiones

Como resultado del trabajo realizado se concluyen los siguientes hechos, relacionados a los objetivos general y específicos de la investigación:

Resultados del logro del objetivo específico 1 (Recopilación).

Se han recopilado los conceptos y relaciones alrededor del dominio semántico de un proceso de GRSI, para construir su base ontológica. En adición, se han identificado los siguientes hechos:

Divergencias de términos equivalentes en las fuentes de información. De la revisión sistemática, se han identificado investigaciones relacionadas que proponen modelos ontológicos propios. Sin embargo, algunas presentan conceptos afines, pero con denominaciones distintas. Por ejemplo, el concepto "Propiedad de Seguridad de Información" [54] es mencionado en algunos trabajos como "Atributo de Seguridad" [73] o como "CIA"[5][73]. Por ese motivo, se ha optado por no utilizar como fuente ontológica a las investigaciones, sino a las normas que estas han utilizado como fuente, y en su idioma original. En consecuencia, se han seleccionado los estándares ISO de la familia 27000, cuyas normas no presentan contradicciones entre sí.

No infalibilidad respecto a la integridad del contenido de las normas. Se ha señalado que las normas ISO, en su idioma de origen, son las fuentes de mayor confianza para la investigación. Sin embargo, algunas de estas presentan ligeros errores de forma en su contenido. Por ejemplo, el estándar ISO/IEC 27002:2022 [19], en su numeral 6.6 "Acuerdos de confidencialidad o no divulgación", refiere por error la capacidad operacional llamada "#Supplier_relationships", en lugar de "#Supplier_relationships_security". Por ello, se ha realizado una revisión y corrección manual de estos estándares, antes de su traducción.

Política de uso y traducción de fuentes de información. La mayoría de las fuentes usadas en la investigación son normas internacionales, cuya edición original está en el idioma inglés. Se ha tenido acceso a traducciones oficiales de países hispanoamericanos o a normas técnicas peruanas. Sin embargo, en algunos casos estas aplican traducciones literales que limitan la semántica de la fuente. En consecuencia, para utilizar estos estándares, se ha optado por tomar las fuentes en inglés, traducirlas con la herramienta DEEPL TRANSLATE al español y validar el resultado mediante una verificación con profesionales especialistas en seguridad de información, antes de utilizarlos.

[5] CIA: Acrónimo en inglés de las propiedades de seguridad de información: "Confidentiality" "Integrity" y "Availability".

Resultados del logro del objetivo específico 2 (Modelado).

Se ha modelado una ontología, en base a la información recopilada, incorporando los conceptos y sus relaciones, de manera que se constituya en el soporte de datos del proceso de GRSI. Además, se ha identificado lo siguiente:

Limitaciones semánticas de los estándares ISO de seguridad de información. Durante el modelado de la etapa del "contexto" (subetapa de "inventario de información y sus activos") se ha identificado que, para esta parte de la ontología, existe información limitada en las normas ISO. Por ello, mediante el uso del método Delphi, aplicado en el capítulo 5, se ha identificado la metodología española MAGERIT como una fuente ontológica, que aporta semántica para cubrir la brecha referida a la categorización de activos de información.

Cabe destacar que, además, ha sido necesario aplicar una recategorización de las clases "amenaza", "vulnerabilidad" y "control", a fin de poder producir relaciones semánticas con otros conceptos, ya que las categorías que el estándar ISO/IEC 27005:2022 [20] no permitían explotar la información contenida en ellas.

Limitaciones en el acceso a Bancos de Datos de Seguridad de Información a nivel local e internacional. Como parte del proceso de modelado, se ha indagado sobre bancos de datos relacionados al tema de GRSI. Sin embargo, dado el carácter confidencial que suele tener esta información en las organizaciones, no ha sido posible tener acceso formal a una de estas fuentes. Por ello, se ha optado por utilizar las normas ISO, como referencias. Cabe destacar que, en una indagación local, se ha identificado que existen 12407 conjuntos de datos publicados en la "Plataforma Nacional de Datos Abiertos"[6], que contienen información principalmente recopilada del Estado Peruano. Si bien 58 de ellos han sido etiquetados como relacionados al tópico de "seguridad de información", en la práctica no contienen conjuntos de datos que se relacionen a este tópico.

Método Delphi como herramienta frente a problemas con limitada información. Debido a que existe una baja disponibilidad de información objetiva en el campo del proceso estudiado, se han indagado alternativas que permitan validar la propuesta del modelo. En consecuencia, se ha revisado la literatura y, considerando las afirmaciones de Reguant [82] respecto a situaciones en las que un problema está asociado a falta de información disponible, se ha optado por utilizar el método Delphi, como un mecanismo que permite validar y refinar el modelo ontológico del proceso investigado.

[6] Publicada como datosabiertos.gob en cumplimiento del D.S. 157-2021-PCM, y consultada el 12 de octubre de 2023.

Resultados del logro del objetivo específico 3 (Aplicación).

Se ha implementado una aplicación informática, que permite explotar el modelo de la ontología, para dar lugar a un proceso de GRSI. Además, se han identificado los siguientes hechos:

Beneficios no planificados de la solución informática y ontológica. Según lo referido por los usuarios especialistas del análisis Delphi, la aplicación ha mostrado algunos beneficios inesperados respecto a la experiencia de realizar el proceso de GRSI. El primero consiste en una mejora en la facilidad de identificar amenazas, vulnerabilidades y controles, agilizando la ejecución del proceso. El segundo, está referido a que, dado que la aplicación trabaja con el formato OWL, existe independencia de la utilización de una base de datos, que es propia de otras soluciones; por ello, su uso es más versátil.

Resultados del logro del objetivo específico 4 (Validación).

Se ha validado que la conjunción del modelo y la aplicación informática implementada mitigan el margen de error humano sobre el proceso de GRSI. Además, se ha identificado lo siguiente:

Limitaciones para superar totalmente la subjetividad en la gestión de riesgos. Si bien se ha demostrado que la aplicación de soluciones basadas en ontologías reduce el margen de error de los actores que participan en el proceso de GRSI, existe un margen de subjetividad intrínseco que no puede ser completamente mitigado ni siquiera mediante una solución informática. Como resultado de la aplicación del método Delphi, los especialistas entrevistados han calificado la reducción de errores con el nivel 4 o “significativa”, no llegando al nivel máximo 5 o “absoluta”. Es decir, la presente investigación mitiga los errores de manera sustancial en un proceso de GRSI, pero no los elimina completamente.

Cumplimiento del objetivo general.

Se ha diseñado e implementado un proceso de GRSI con una solución basada en ontologías. Para ello, se ha realizado un análisis semántico de los estándares relacionados a la GRSI (ISO/IEC 27005:2022 [20]). Luego, se ha estructurado una ontología, que ha sido sometida al escrutinio de especialistas en el dominio, para ser refinada aplicando el método Delphi. Esta ontología ha sido articulada con una solución informática, que también ha sido validada por especialistas; que han certificado que mitiga significativamente la posibilidad de errores en el proceso. Además, se ha identificado lo siguiente:

Singularidades de la investigación. Tras revisar el estado del arte, se ha identificado que la mayoría de las investigaciones se limitan a representar el subproceso de evaluación de riesgos y, solo eventualmente, mencionan la fase posterior de tratamiento. La presente investigación es la primera en cuyo alcance se ha analizado también el proceso de tratamiento de riesgos, en profundidad, incorporando sus componentes en el modelo ontológico.

7.2. Trabajos futuros

A continuación, se proponen algunos temas de investigación que son colaterales o que podrían derivarse de la presente tesis:

Implementación de un proceso de gestión de riesgos bajo un enfoque "basado en eventos". Tal como establece el estándar ISO 27005:2022 [20] (numeral 7.2.1) existen dos métodos para iniciar la evaluación de riesgos (identificación de riesgos). El primer enforque es el "basado en activos", el cual ha sido utilizado en la presente tesis. El segundo, "basado en eventos", podría ser aplicado en una nueva investigación, centrándose en los registros estructurados de eventos preexistentes en una organización.

Generación automatizada de la "Declaración de aplicabilidad". El estándar ISO/IEC 27001:2022 [18] establece en su numeral 6.1.3.d el requisito de preparar una "Declaración de Aplicabilidad" de los controles que son necesarios para la organización. Este documento lista los controles de seguridad de información, referidos en la norma y, para cada uno de ellos, indica y justifica si está implementado en la organización. Sería posible ampliar el alcance de la presente investigación, de manera que se recopilen otros controles existentes en la organización y sus atributos, a fin de atender el requisito referido.

Definición y redacción de observaciones bajo el Manual de Auditoría de Cumplimiento de la CGR, aplicando ontologías. Se ha identificado que existe un proceso similar de la GRSI, que corresponde a la identificación y definición de "observaciones de auditoría de cumplimiento" para las Oficinas de Control Interno (OCI) adscritas a la Contraloría General de la República (CGR). Los términos de esta ontología se encuentran definidos en el "Manual de Auditoría de Cumplimiento de la CGR" [83]. Sería posible elaborar una ontología utilizando los elementos que componen una observación (condición, criterio, efecto y causa), para implementar una solución facilitadora de este proceso, a partir de una base de información de auditorías pasadas.

Implementación de una plataforma de gamificación para la enseñanza de la gestión de riesgos de seguridad de información. La disponibilidad de la ontología y de la solución informática que soporta al proceso de GRSI, permite contar con una herramienta operacional de gestión de riesgos. Sin embargo, si esta fuera conjugada con casos ficticios que propongan escenarios de riesgos en organizaciones, podría ser utilizadas para la formación de gestores de riesgos en seguridad de información. Es decir, podría realizarse una investigación respecto a la efectivad de la presente herramienta como software educativo para la capacitación en gestión de riesgos.

8. Referencias bibliográficas

[1] International Organization for Standardization & International Electrotechnical Commission. (2000). ISO/IEC 17799:2000 Information technology — Code of practice for information security management. Geneva, Switzerland: ISO.

[2] International Organization for Standardization & International Electrotechnical Commission. (2005). ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice for information security management. Geneva, Switzerland: ISO.

[3] International Organization for Standardization & International Electrotechnical Commission. (2005). ISO/IEC 27001:2005 Information security management systems. Requirements. Geneva, Switzerland: ISO.

[4] International Organization for Standardization & International Electrotechnical Commission. (2005). ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management. Geneva, Switzerland: ISO.

[5] International Organization for Standardization & International Electrotechnical Commission. (2008). ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management. Geneva, Switzerland: ISO.

[6] International Organization for Standardization & International Electrotechnical Commission. (2009). ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: ISO.

[7] International Organization for Standardization. (2009). ISO 31000:2009 Risk management — Principles and guidelines. Geneva, Switzerland: ISO.

[8] International Organization for Standardization & International Electrotechnical Commission. (2011). ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management. Geneva, Switzerland: ISO.

[9] International Organization for Standardization & International Electrotechnical Commission. (2012). ISO/IEC 27000:2012 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: ISO.

[10] International Organization for Standardization & International Electrotechnical Commission. (2013). ISO/IEC 27001:2013 Information security management systems. Requirements. Geneva, Switzerland: ISO.

[11] International Organization for Standardization & International Electrotechnical Commission. (2013). ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. Geneva, Switzerland: ISO.

[12] International Organization for Standardization & International Electrotechnical Commission. (2014). ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: ISO.

[13] International Organization for Standardization & International Electrotechnical Commission. (2016). ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: ISO.

[14] International Organization for Standardization & International Electrotechnical Commission. (2016). ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. Geneva, Switzerland: ISO.

[15] International Organization for Standardization & International Electrotechnical Commission. (2018). ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, Switzerland: ISO.

[16] International Organization for Standardization & International Electrotechnical Commission. (2018). ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. Geneva, Switzerland: ISO.

[17] International Organization for Standardization. (2018). ISO 31000:2018 Risk management — Guidelines. Geneva, Switzerland: ISO.

[18] International Organization for Standardization & International Electrotechnical

Commission. (2022). ISO/IEC 27001:2022 Information security management systems. Requirements. Geneva, Switzerland: ISO.
[19] International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Geneva, Switzerland: ISO.
[20] International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva, Switzerland: ISO.
[21] International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process. Geneva, Switzerland: ISO.
[22] Comisión de Reglamentos Técnicos y Comerciales - INDECOPI. (2004). NTP-ISO/IEC 17799:2004 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. Lima, Perú: INDECOPI.
[23] Comisión de Reglamentos Técnicos y Comerciales - INDECOPI. (2007). NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. Lima, Perú: INDECOPI.
[24] Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias – INDECOPI. (2008). NTP-ISO/IEC 27001:2008 EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Lima, Perú: INDECOPI.
[25] Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias – INDECOPI. (2009). NTP-ISO/IEC 27005:2009 Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información. Lima, Perú: INDECOPI.
[26] Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias - INDECOPI. (2011). NTP-ISO 31000:2011 Gestión del riesgo. Principios y directrices. Lima, Perú: INDECOPI.
[27] Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias - INDECOPI. (2014). NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. Lima, Perú: INDECOPI.
[28] Instituto Nacional de Calidad. (2017). NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. Lima, Perú: INACAL.
[29] Instituto Nacional de Calidad. (2019). NTP-ISO/IEC 27035-1:2019 Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1: Principios de la gestión de incidencias. Lima, Perú: INACAL.
[30] Instituto Nacional de Calidad. (2018). NTP-ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información. Lima, Perú: INACAL.
[31] Instituto Nacional de Calidad. (2018). NTP-ISO 31000:2018 Gestión del riesgo. Directrices. Lima, Perú: INACAL.
[32] Instituto Nacional de Calidad. (2022). NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. Lima, Perú: INACAL.
[33] Instituto Nacional de Calidad. (2022). NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. Lima, Perú: INACAL.
[34] Instituto Nacional de Calidad. (2022). NTP-ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. Lima, Perú: INACAL.
[35] Resolución Ministerial N° 224-2004-PCM, del 23 de julio de 2004. Aprueban uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 17799:2004 EDI”.
[36] Resolución Ministerial N° 246-2007-PCM, del 22 de agosto de 2007. Aprueban uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición” en todas las entidades integrantes del Sistema Nacional de Informática.
[37] Resolución Ministerial N° 129-2012-PCM, del 23 de mayo de 2012. Apruébese el uso

obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información.
[38] Resolución Ministerial N° 004-2016-PCM, del 8 de enero de 2016. Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
[39] Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid, octubre de 2012.
[40] Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos. Madrid, octubre de 2012.
[41] Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Catálogo de Técnicas. Madrid, octubre de 2012.
[42] Resolución SBS N° 504-2021, del 19 de febrero de 2021, Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
[43] Nist, & Aroms, E. (2012). NIST SP 800-100 Information Security Handbook: A Guide for Managers.
[44] Santos, D. (2016). Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001: 2013, para una empresa de consultoría de software.
[45] Slovic, P. (1999). Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. Risk analysis, 19, 689-701.
[46] Horridge, M., Brandt, S. (2011). A practical guide to building owl ontologies using protégé 4 and co-ode tools edition1.3. The university of Manchester, 108.
[47] Von Solms, B. (2001). Corporate governance and information security. Computers & Security, 20(3), 215-218.
[48] Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS, 11(5), 23-29.
[49] Kitchenham, B. A. & Charters, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. Engineering, 2:1051, 2007.
[50] Kitchenham, B. A., Mendes, E., & Travassos, G. H. (2007). Cross versus within-company cost estimation studies: A systematic review. IEEE Transactions on Software Engineering, 33(5), 316-329.
[51] M. Petticrew, and H. Roberts, ³Systematic Reviews in the Social Sciences: A Practical Guide, Malden, USA, Blackwell Publishing, 2006.
[52] Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. Intentional Perspectives on Information Systems Engineering, 289-306.
[53] Torrellas, G. S. (2004, September). A framework for multi-agent system engineering using ontology domain modelling for security architecture risk assessment in e-commerce security services. In Third IEEE International Symposium on Network Computing and Applications, 2004. (NCA 2004). Proceedings. (pp. 409-412). IEEE.
[54] Kiesling, E., Strausß, C., & Stummer, C. (2012, August). A multi-objective decision support framework for simulation-based security control selection. In 2012 Seventh international conference on availability, reliability and security (pp. 454-462). IEEE.
[55] Pereira, T., & Santos, H. (2012). An Ontological Approach to Information Security Management. In 7th International Conference on Information Warfare and Security. Seattle. University Washington (pp. 368-375).
[56] Fenz, S. (2011, March). An ontology-and bayesian-based approach for determining threat probabilities. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 344-354).
[57] Pereira, T. S. M., & Santos, H. M. D. (2012). An Ontology Approach in Designing Security Information Systems to Support Organizational Security Risk Knowledge. In KEOD (pp. 461-466).
[58] Talens, G., Delorme, G., & Disson, E. (2022, October). • An ontology for data regulation. In 14th International Conference on Knowledge Engineering and Ontology Development.

[59] Oliveira, Í., Sales, T. P., Baratella, R., Fumagalli, M., & Guizzardi, G. (2022, October). An ontology of security from a risk treatment perspective. In International conference on conceptual modeling (pp. 365-379). Cham: Springer International Publishing.
[60] Montesino, R., & Fenz, S. (2011, September). Automation possibilities in information security management. In 2011 European Intelligence and Security Informatics Conference (pp. 259-262). IEEE.
[61] Buerle, S. (2012). BioONT: Improving Knowledge Organization and Representation in the Domain of Biometric Authentication. In Proceedings of the 7th International Conference on Information Warfare and Security: ICIW (p. 56). Academic Conferences Limited.
[62] Liu, F. H., & Lee, W. T. (2010). Constructing enterprise information network security risk management mechanism by ontology. Journal of Applied Science and Engineering, 13(1), 79-87.
[63] Iqbal, M., & Matulevičius, R. (2020). Corda Security Ontology: Example of Post-Trade Matching and Confirmation. Baltic Journal of Modern Computing, 8(4).
[64] Delorme, G., Talens, G., & Disson, E. (2022). Data Regulation Ontology. In SEKE (pp. 503-506).
[65] Fenz, S., & Ekelhart, A. (2009, March). Formalizing information security knowledge. In Proceedings of the 4th international Symposium on information, Computer, and Communications Security (pp. 183-194).
[66] Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S., & Muck, T. (2008, January). Integration of an ontological information security concept in risk aware business process management. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 377-377). IEEE.
[67] Peng, W., Yingwu, C., Sen, C., & Guoqing, Y. (2011, May). ISRMDSS: An information security risk management oriented multi-agent system. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 356-359). IEEE.
[68] Adán, B. G., Cristhian, L. C., Mario, C. L., Sonia, O. S., Yaneth, C. C., & Jairo, G. (2016). Knowledge base for an intelligent system in order to identify security requirements for government agencies software projects. In MATEC Web of Conferences (Vol. 76, p. 03012). EDP Sciences.
[69] Riesco, R., & Villagrá, V. A. (2019). Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL). International Journal of Information Security, 18(6), 715-739.
[70] Dos Santos Moreira, E., Andréia Fondazzi Martimiano, L., José dos Santos Brandão, A., & César Bernardes, M. (2008). Ontologies for information security management and governance. Information Management & Computer Security, 16(2), 150-165.
[71] Satybaldina, D., Muratkhan, R., & Kabenov, D. Ontology and Fuzzy Measures Based System for Information Security Risk Assessment. In WOSIS—9th International Workshop on Security in Information Systems, June (Vol. 28, pp. 77-85).
[72] Ekelhart, A., Fenz, S., & Neubauer, T. (2009, March). Ontology-based decision support for information security risk management. In 2009 Fourth International Conference on Systems (pp. 80-85). IEEE.
[73] Fenz, S., & Neubauer, T. (2018). Ontology-based information security compliance determination and control selection on the example of ISO 27002. Information & Computer Security, 26(5), 551-567.
[74] Muratkhan, R., & Satybaldina, D. Z. (2014). Quantitative method of information security risk assessment by multicomponent threats. Life Science Journal, 11(11), 372-375.
[75] Sarala, R., Vijayalakshmi, V., Zayaraz, G., & Priyanka, E. (2014, December). Risk intelligence retrieval based on ontology. In 2014 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-4). IEEE.
[76] Kurylets, A., & Goranin, N. (2023). Security Ontology OntoSecRPA for Robotic Process Automation Domain. Applied Sciences, 13(9), 5568.
[77] Solic, K., Ocevcic, H., & Golub, M. (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. Computers & security, 55, 100-112.
[78] Mace, J. C. (2017). Tools and techniques for analysing the impact of information security (Doctoral dissertation, Newcastle University).
[79] Solic, K., Ocevcic, H., Fosic, I., Horvat, I., Vukovic, M., & Ramljak, T. (2017, May). Towards overall information security and privacy (IS&P) taxonomy. In 2017 40th

International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1298-1301). IEEE.
[80] Agrawal, V. (2016). Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard. In HAISA (pp. 101-111).
[81] Hammarberg, M., & Sunden, J. (2014). Kanban in action. Manning Publications Co.
[82] Reguant Álvarez, M., & Torrado Fonseca, M. (2016). El método delphi. REIRE: revista d'innovació i recerca en educació.
[83] Resolución de Contraloría N.° 001-2022-CG Aprobar la Directiva Nº 001-2022-CG/NORM “Auditoría de Cumplimiento” y el “Manual de Auditoría de Cumplimiento”, que en Anexos forman parte integrante de la presente Resolución. 9 de enero de 2022.
[84] Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. International Journal of Information Management, 43, 165-172.
[85] International Organization for Standardization & International Electrotechnical Commission. (2012). ISO/IEC 27032:2012 Information technology—Security techniques—Guidelines for cybersecurity. Geneva, Switzerland: ISO.
[86] International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 27032:2023 Cybersecurity— Guidelines for Internet security. Geneva, Switzerland: ISO.
[87] Landeta, J., Barrutia, J., & Lertxundi, A. (2011). Hybrid Delphi: A methodology to facilitate contribution from experts in professional contexts. Technological Forecasting and Social Change, 78(9), 1629-1641.