UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE DE RIESGOS PARA APOYAR EN LOS SERVICIOS DE MODELADO NUMÉRICO AMBIENTAL

TESIS PARA OPTAR EL GRADO ACADÉMICO DE
MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR

DAVID GEREMIAS CORREA CHILON

ASESOR

MARIA YSABEL ARANGURI GARCIA

https://orcid.org/0000-0001-9220-5801

Chiclayo, 2020

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE DE RIESGOS PARA APOYAR EN LOS SERVICIOS DE MODELADO NUMÉRICO AMBIENTAL

PRESENTADA POR

DAVID GEREMIAS CORREA CHILON

A la Escuela de Posgrado de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADA POR

Gregorio Manuel Leon Tenorio
PRESIDENTE

Ricardo David Iman Espinoza
SECRETARIO

Maria Ysabel Aranguri Garcia
VOCAL

Dedicatoria

El presente trabajo de investigación es dedicado principalmente a Dios, por haberme dado la motivación de seguir adelante y culminar este proyecto.

A mi familia por haber sido mi apoyo permanente durante esta etapa de mi vida, especialmente a mi esposa Kelly, con quien compartí las clases, los trabajos de grupo y fue mi apoyo incondicional en todo momento.

A mis hijos: Mariejoseph, Dave Francois, Pedro Pablo; A mis queridos padres, Genaro y Gladys; A mí tía Rosa; A mis suegros, Pedro y Teresa, por su apoyo incondicional, fueron parte fundamental durante este periodo.

A todas las personas que me acompañaron en este periodo de mi vida, aportando a mi formación personal y profesional, sus experiencias fueron de gran ayuda.

Finalmente agradezco a mis colegas de maestría, Kelly, Jaime, Diana, Imelda, Leodan, por compartir su tiempo y experiencias, aprendí mucho de ellos, y formamos una gran amistad, quedo agradecidos de haberlos conocido.

Agradecimiento

Agradezco a las empresas que colaboraron y brindaron información, fue muy importante para el desarrollo de la presente investigación,…

Agradezco a mi asesora Mtro María Arangurí García, por su tiempo, paciencia, por sus aportes y sugerencias que fueron claves para la culminación de mi proyecto de tesis.

Así mismo, agradezco los aportes y sugerencias de todas las personas, maestros y doctores a quienes consulté, quienes de una u otra manera me apoyaron desinteresadamente.

Gracias a todos.

Índice

Listas de Tablas

Lista de Figuras

RESUMEN

La “Gestión de la Seguridad de la Información”, cada día asume mayor importancia en las actividades empresariales; aportando valor a los negocios, principalmente cuando confluye la gestión de la información y la infraestructura tecnológica digital, dando lugar a emprendimientos innovadores de alta rentabilidad en diversas actividades económicas, tal es el caso de empresas como UBER, AirB&B, entre otras empresas de servicios altamente tecnológicas. En torno a los Estudios de Impacto Ambiental, se desarrollan servicios complementarios, relacionado a la evaluación se posibles escenarios de Impacto Ambiental ante la instalación de diversos proyectos de inversión, para lo cual se utilizan herramientas de modelado, las mismas que se basan en cálculos numéricos computacionales, que requieren de información ambiental para los fines de evaluación. El servicios de modelado numéricos ambiental, demandan de equipos de cómputo especializado, software, lenguajes de programación y técnicas de procesamiento de información muy específicas, todas ellas necesitan mantener la disponibilidad, integridad y confidencialidad de la información en todas las etapas de los procesos. En este sentido, se propone un modelo de Gestión de Seguridad de la Información basado en normas internacionales de “Gestión de Riesgos”. Llegándose a analizar estándares de Gestión de Seguridad de la Información basado en la Gestión del Riesgos y proponer un modelo de Gestión de Seguridad de la Información, se aplicó; propuesta que fue implementada parcialmente en una empresa, la misma que fue sometida a evaluación de juicio de expertos.

Palabras claves: Gestión de seguridad de la información, Gestión de riesgos, Modelado numérico ambiental

ABSTRACT

The "Information Security Management", each day assumes greater importance in business activities; adding value to businesses, mainly when information management and digital technology infrastructure come together, giving rise to highly profitable innovative ventures in various economic activities, such is the case of companies such as UBER, AirB&B, among other highly-resourced service companies. Technological. Around the Environmental Impact Studies, complementary services are developed, related to the evaluation of possible Environmental Impact scenarios before the installation of various investment projects, for which modeling tools are used, the same ones that are based on numerical calculations. Computational, which require environmental information for evaluation purposes. The environmental numerical modeling services demand specialized computer equipment, software, programming languages and very specific information processing techniques, all of which need to maintain the availability, integrity and confidentiality of information at all stages of the processes. In this sense, an Information Security Management model based on international "Risk Management" standards is proposed. Arriving to analyze Information Security Management standards based on Risk Management and propose an Information Security Management model, it was applied; proposal that was partially implemented in a company, the same one that was submitted to expert judgment evaluation.

Keywords: Information security management, Risk management, Environmental numerical modeling

INTRODUCCIÓN

Desde finales de 1970, el concepto de “medio ambiente” inicio a tomar más importancia, principalmente en los “Estados Unidos de América”, con la creación de la National Environmental Policy Act (NEPA), entidad dedicada a asuntos de “Evaluación de Impacto Ambiental” (EIA), [1]. Mientras que en los países de Latino América, cobro importancia recién en el año 1992, con la declaración de “Río de Janeiro”, Brasil, en la cual 185 países asumieron compromisos de protección de los recursos naturales y del medio ambiente.

Perú, como parte de los países que forman el Grupo de Rio, adopto la declaración de Rio de Janeiro, ese mismo año estableció políticas de regulación ambiental, llegando a crear el “Sistema Nacional de Evaluación de Impacto Ambiental” (SEIA), [2], mientras que en el año 2008 reemplazo al SEIA por el “Ministerio del Medio Ambiente”, dando impulso a la regulación ambiental en el Perú, adoptando carácter obligatorio realizar la EIA antes de la ejecución de cualquier proyecto de inversión. Por otro lado, a partir del año 2015, se creó el “Servicio Nacional de Certificaciones Ambientales para las Inversiones Sostenibles” (SENACE), organismo que viene contribuyendo a la mejora y simplificación de los procesos administrativos relacionados a los EIA en Perú.

La “Gestión de la Seguridad de la Información” (GSI), cada día asume mayor importancia en las actividades empresariales; aportando valor a los negocios, principalmente cuando logran conjugar la gestión de la información con la infraestructura tecnológica digital, como es el caso de emprendimientos innovadores, que con pocos recursos alcanzan a hacerse de un nicho económico, tal es el caso de empresas como UBER, Airbnb y muchas otras empresas servicios altamente tecnológicas.

A nivel internacional, existen diversas iniciativas de proyectos y negocios que giran en torno al uso de información ambiental para el desarrollo de actividades de modelado numérico computacional, algunas de ellas realizan actividades de modelado para fines de investigación científica, tal es el caso de los institutos de investigación.

A nivel local, la empresa FISMATLAB S.A.C. ofrecer servicios de modelado numéricos ambiental para proyectos de ingeniería, además del servicio de desarrollo de aplicativos computacionales para procesamiento de información ambiental. Los servicios de modelado numérico ambiental, demandan de equipos de cómputo, softwares, lenguajes

de programación y técnicas de procesamiento de información muy específicas, todas ellas necesitan mantener la disponibilidad, integridad y confidencialidad de la información que utilizan, ya que la alteración de la información podría producir cambios y afectación de los resultados de los servicios de modelado numérico que ofrece la empresa. En este sentido, es necesario desarrollar e implementar un modelo de GSI basado en normas internacionales, para apoyar la GSI en los servicios de modelado numérico ambiental en la empresa FISMATLAB S.A.C.

Es así que a través de la presente investigación se propusieron alternativas para apoyar los servicios de modelado numérico ambiental a través de la implantación de un modelo de GSI basado en herramientas de "Gestión de Riesgos" (GR). Por lo que se planteó como objetivos específicos, analizar y determinar estándares de GSI basadas en GR aplicables a los procesos asociados a los servicios de modelado numérico ambiental. A partir de estos estándares se propuso un modelo de GSI, se aplicó, como caso de estudio a una empresa en la Chiclayo y finalmente se sometió a opinión de juicio de tres expertos.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1 ANTECEDENTES

Sobre la seguridad de la información

Taopanpa y otros autores, 2020, analizaron diferentes modelos en “Tecnologías de la Información y la Comunicación” (TIC), para la creación de un modelo alternativo para mitigar los riesgos de GSI dentro de empresas de telecomunicaciones. Llegando a definir un prototipo de modelo que usa una matriz de riesgo, [3], los autores propusieron un modelo GSI, basándose en controles de la norma ISO/IEC 27001, con fines de disminuir los riesgos de perdida de información en instituciones educativas para prevenir pérdidas financieras, problemas jurídicos, etc. En este contexto el modelo propuesto indujo al análisis de posibles riesgos sobre los activos críticos y la información importante de la institución educativa, con énfasis en prevenir vulnerabilidades y amenazas en los activos (tanto físicos como lógicos).

Sobre los servicios de modelado numérico ambiental

“A nivel internacional existen informes que dan cuenta de casos de la vulnerabilidad de información, por ejemplo en el Centro Internacional de Administración Oceánica y Atmosférica (NOAA por sus siglas en inglés), encontraron dispositivos móviles no autorizados conectados a plataformas de procesamiento de información satelital ambiental, programas autoejecutables instalados sin autorización, sin controles de habilitación, y/o controles de seguridad. Ante estas situaciones implementaron políticas de seguridad sobre los componentes informáticos y la información desde una perspectiva de gestión del riesgo de la información”, [4] [5].

“A nivel regional existen proyectos que garantizan la accesibilidad a la información a través de plataformas virtuales (SIG, pagina web y link de descarga), denominados observatorios digitales [6] [7], como es el caso de los proyectos hidrológicos EarthCube, TERENO, NEON y CUAHSI” [8], proyectos que son gestionados por universidades e instituciones hidrológicas norteamericanas para la gestión de información hidrológica.

“A nivel local, ocurrieron algunas vulnerabilidades de información importantes, como es el caso de los ciberataques a las agencias bancarias en Perú, ocurrido el día 17 de agosto del 2018, en el que debido a la importancia de la información y la magnitud del riesgo a

los cuales estuvieron expuestos los sistemas informáticos, los bancos se vieron en la necesidad de bajar o apagar sus sistemas informáticos de producción, de los cuales dos bancos (Interbank y Scotiabank) tuvieron que cerrar sus servicios de atención al público, tanto en sus oficinas como en sus plataformas online", [9].

1.2 BASE TEÓRICA CONCEPTUAL

1.2.1 Modelado numérico ambiental

En la actualidad, el Perú cuanta con la "Ley Nº 27446: Ley del Sistema Nacional de Evaluación del Impacto Ambiental" y el "Decreto Supremo Nº 019-2009 MINAM", que establece que todo proyecto de inversión público o privado debe contar con la aprobación de un certificado ambiental, [10].

En este contexto, surgen empresas que ofrecen servicios de desarrollo de EIA, que tienen por finalidad determinar el estado de línea base del lugar donde se ejecutaría un determinado proyecto, llegando a establecer sus posibles impactos sobre medio ambiente, para lo cual hacen uso de herramientas de simulación numérica. El modelado numérico computacional, es una herramienta cada vez más utilizada en los EIA de los proyectos.

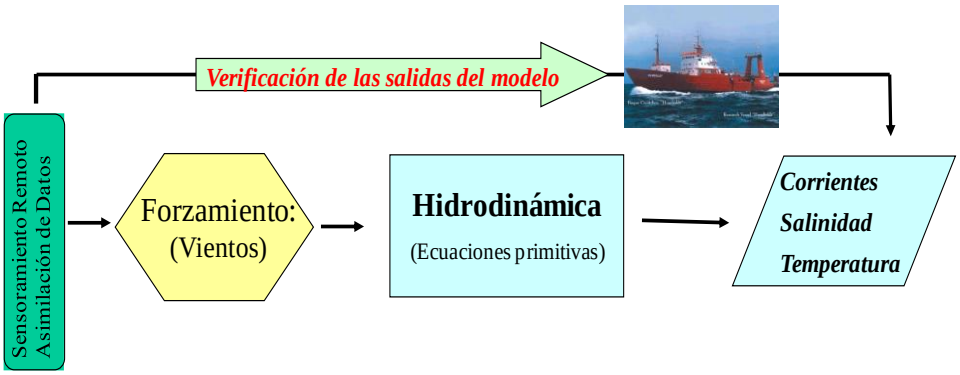
El proceso de modelado numérico ambiental, consiste en reproducir las características y procesos de interacción del medio real en un ambiente digital representado a través de la solución de un sistema de ecuaciones matemáticas, empleando métodos numéricos especiales, y conlleva a realizar las siguientes actividades:

- ✓ Definir el contexto del medio físico ambiental a evaluar.
- ✓ Recolectar información necesaria para evaluar el medio físico ambiental.
- ✓ Definir el modelo conceptual (simplificaciones, aproximaciones, hipótesis).
- ✓ Establecer un modelo físico - matemático (ecuaciones) del modelo conceptual.
- ✓ Resolver el modelo físico - matemático a través de métodos numéricos.
- ✓ Validar los resultados del modelo físico - matemático con información real.
- ✓ Interpretar los resultados bajo diversos escenarios de riesgo de impacto ambiental.
- ✓ Sugerir planes de adaptación y mitigación de riesgos de impacto ambiental para la ejecución de un determinado proyecto.

La Figura Nº 1, muestra el proceso de implementación de un modelo de simulación numérica de parámetros marinos, como temperatura, salinidad y corrientes marinas, a

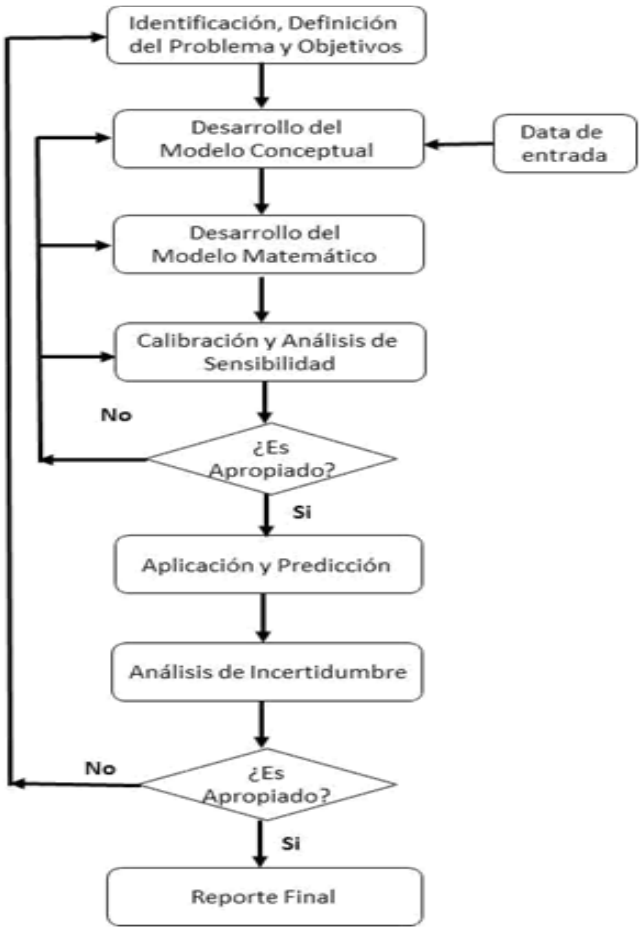
través de un modelo oceánico denominado ROMS (Regional Ocean Model System), que inicia con el análisis de la información marina (temperatura, salinidad y corrientes), para establecer condiciones iniciales (valores para inicializar los cálculos), condicione de fronteras laterales (valores que definen las condiciones del medio marino en el tiempo), condiciones de forzamiento superficial (como el viento) y condiciones de fondo marino; en una segunda instancia se realizan los cálculos a través de la solución de un sistema ecuaciones; finalmente se verifica la información generada por el modelo con la real, Figura Nº 1.

Figura Nº 1: Esquema de ejecución del modelo numérico marino



Fuente: Informe de tesis [11]

Figura Nº 2: Diagrama proceso de modelado numérico ambiental



Fuente: Ingol [12]

1.2.1.1 Ciclo de vida de la información

El ciclo de vida de la información abarca desde su generación o captura hasta su almacenamiento y como su posterior explotación, y poniendo énfasis en las diversas características que componen todo el contexto de los datos desde un enfoque empresarial y técnico, incluye el diseño de la arquitectura, el desarrollo de una base de datos, la gestión de los datos y medidas de seguridad.

Figura Nº 3: Ciclo de vida de los datos

Fuente: https://www.clase10.com

El ciclo de vida de los datos se compone de cuatro fases:

1. Fase 01: Creación y captura

   Aborda el cómo se crean, reciben o capturan datos que entran a formar parte de toda la información del negocio. Los datos pueden crearse a partir de operaciones con personas y/o sistemas con el uso de equipos de medición. Los datos pueden ser reutilizados, distribuidos, almacenados y analizados, se realiza:

   Agregación: es el proceso de combinar la entrada de datos procedentes de diferentes herramientas, equipos o sistemas.

   Categorización: organización de los datos, documentos, u otros en agrupaciones lógicas, basándose en el contenido de la información.

   Indexación: identificación de atributos específicos de un documento o registro de base de datos de cara a facilitar la recuperación.

2. Fase 02: Transmisión, almacenamiento y seguridad

   Como parte del ciclo de vida de los datos, da respuesta a preguntas como:

   ¿Dónde se almacena la información?

   ¿Cómo se podría acceder a la información después?

   ¿Cómo mover o transmitir la información entre sistemas internos y/o externos?

   ¿Cómo se puede garantizar la GSI?

En esta fase, se pueden define el sistema de ficheros, como se van a nombrar los fichero, la lógica de almacenamiento (árbol) y recuperación de la información.

3. Fase 03: Gestión, acceso y compartición

   Esta fase da respuesta a cómo conseguir la información adecuada para las personas o sistemas adecuados en el dispositivo correcto, integrando el sistema de gestión de los datos con el resto de aplicaciones de la empresa u organización.

4. Fase 04: Análisis de información

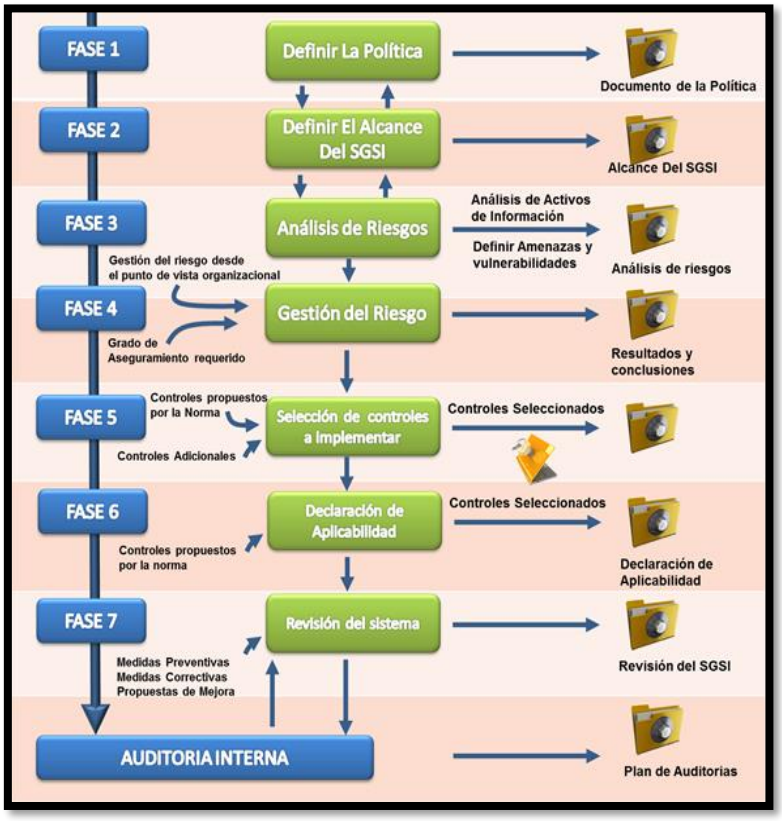
   Esta fase implica el análisis, explotación y uso de los datos para el desarrollo de un servicio, generándose:

   - ✓ Informes, consultas y reportes.
   - ✓ Optimizaciones de procesos.
   - ✓ Análisis estadísticos.
   - ✓ Indicadores de gestión.
   - ✓ Patrones o tendencias
   - ✓ Previsiones.
   - ✓ Control de procesos y costes

1.2.2 La GSI

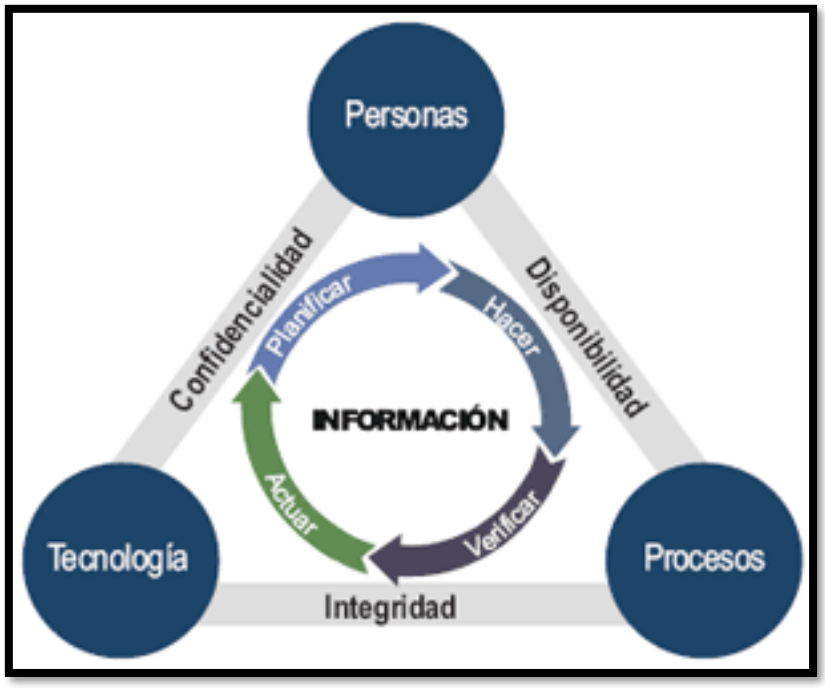
De acuerdo a la norma internacional “ISO/IEC 27001:2013”, la GSI comprende el diseño, implantación y mantenimiento de un conjunto de procesos que gestionan y brindan protección a los elementos que garantizan la confidencialidad, integridad y disponibilidad de la información, a partir de la interacción de tres elementos (procesos, tecnologías y personas de la empresa u organización). La ISO 27001 se organiza en 14 dominios, 114 controles y se estructura en 7 fases, y se basan en el ciclo de mejora continua.

Figura Nº 4: Estructura de la ISO/IEC 27001:2013



Fuente: elaboración propia

Figura Nº 5: Principios, procesos y actores según ISO 27001:2013



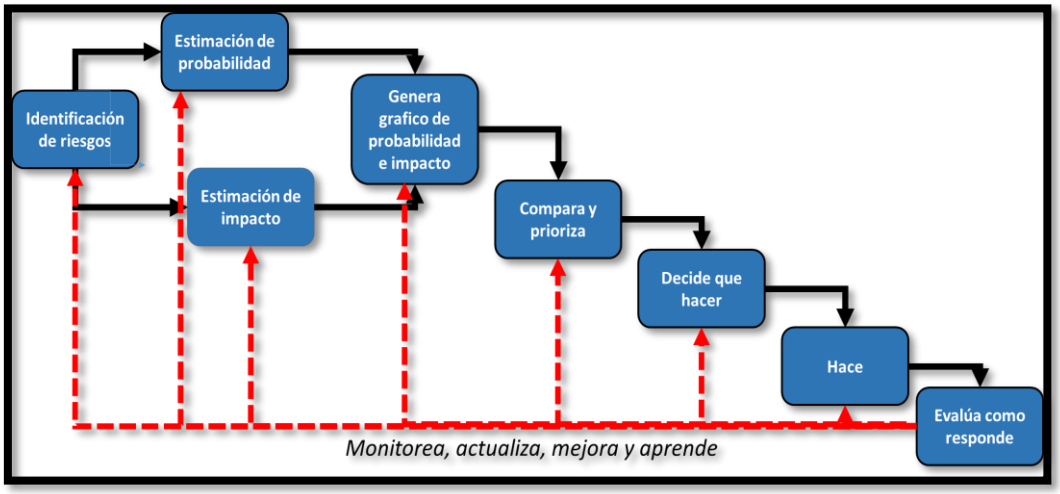
Fuente: elaboración propia

1.2.3 La gestión del riesgo de la información

Comprende principalmente los siguientes elementos para la gestión de riesgos:

- ✓ Identificación del riesgo.
- ✓ Evaluación de riesgos (Estima probabilidad e impacto).
- ✓ Tratamiento de Riesgos (compara, prioriza y decide que hacer).
- ✓ Admisión de Riesgos Seguridad de la información.
- ✓ Evalúa como responde a la gestión del riesgo (monitorea).
- ✓ Revisa, actualiza, mejora y aprende sobre el riesgo.
- ✓ Comunicación de la gestión del riesgo.

Figura Nº 6: Gestión de riesgos de seguridad de la información (ISO 27005)



Fuente: elaboración propia

CAPÍTULO II MATERIALES Y MÉTODOS

2.1 DISEÑO DE INVESTIGACIÓN

El tipo y nivel de investigación es cuantitativa – experimental. Cuantitativa, debido a que es un tipo de investigación concluyente en su propósito al buscar la medición del problema, basado en la lógica empírico – deductiva a partir de procedimientos rigurosos, métodos experimentales y el uso de técnicas de recolección de datos estadísticos, que permiten proyectar los resultados de la investigación hacia un grupo mayor, en este caso hacia otras empresas, [13]. Experimental, debido a que existe un cierto grado de incidencia, por parte de quien investiga, sobre las variables independientes, [13]. De tal forma que el modelo a plantear contiene como variable independiente, al modelo de gestión de seguridad de la información con enfoque de riesgos, que conlleva generar cambios, variable dependiente, en los servicios de modelado numérico ambiental.

En cuanto a diseño de investigación es de tipo Pre test/ Post test, el investigador analiza la situación actual de un grupo de empresas que ofrecen servicios de modelado numérico ambiental, como actividad principal, en ellas se analiza la gestión de la seguridad de la información, basado en la ISO/IEC 27000, 27001 y 27005, llegando a proponer un modelo para la gestión de la seguridad de la información con un enfoque en riesgos, propuesta que implementada y valida a través de juicio de experto, ver Tabla 1.

Variable independiente: X1: El Modelo de Gestión de la seguridad de la información con enfoque en riesgos.

Variable dependiente: X2: El apoyo a los servicios de modelado numérico ambiental.

Tabla 1: Secuencia de tratamiento de la investigación

Secuencia	**Descripción de tratamiento O_1 X O_2**
Pretest	**O_1**: Observación inicial, antes de la aplicación del tratamiento en la variable dependiente (variable dependiente: Apoyo a los servicios de modelado numérico ambiental).
Tratamiento	**X**: Tratamiento (variable independiente: Modelo de gestión de seguridad de la información con enfoque de riesgos)
Postest	**O_2**: Observación registrada después de la aplicación del tratamiento en la variable dependiente (variable dependiente: Apoyo a los servicios de modelado numérico ambiental).

Fuente: elaboración propia

2.2 POBLACIÓN Y MUESTRA

La población de estudio estuvo conformada por cuatro empresas, una con sede en Chiclayo, mientras que tres radican en la ciudad de Lima. Todas las empresas ofrecen servicios de modelado numérico ambiental como parte de servicios generales y asesoramiento ingenieril, tienen cobertura nacional, en sectores comerciales como hidrocarburos, vivienda, infraestructuras marinas.

2.3 CRITERIOS DE SELECCIÓN

Las empresas seleccionadas para el presente estudio cumplen con el criterio, de desarrollar actividades relacionadas a servicios hidrográficos u oceanográficos, estando registradas como empresas prestadoras de servicios hidro-oceanográficas en la Dirección de Hidrografía y Navegación de la Marina de Guerra del Perú (www.dhn.mil.pe/empresas_hidro), además de ofrecer servicios de modelado numérico ambiental como actividad principal, contando con profesionales dedicados a tal fin.

2.4 MÉTODOS Y TÉCNICAS DE RECOLECCIÓN DE DATOS

Las técnicas e instrumentos de recolección de datos e información fuero a través de encuestas, entrevistas y documentación, además se utilizó modelado de procesos y técnicas de validación, ver Tabla 2.

Tabla 2: Métodos y técnicas utilizados en la investigación

Métodos	Técnica
Entrevista	Se realizó a través de comunicación telefónica, realizando preguntas, principalmente a los gerentes o responsables de las empresas.
Encuesta	Se realizó a través de la aplicación de cuestionarios de preguntas de respuestas múltiples, destinado principalmente a personal de las empresas.
Modelado	Se utilizó para el proceso de implementación y análisis de casos de estudio, a través del modelado de procesos de negocios, específicamente se utilizó Bizagi.
Documental	Se revisó diversos documentos relacionados a la gestión de la seguridad de la información de TI y gestión de riesgos.
Validación	Se utilizó la escala de Likert, el alfa de crombach y juicio de experto, estos estadísticos se describen en la sección siguiente

Fuente: elaboración propia

2.5 INSTRUMENTOS DE VALIDACIÓN

2.5.1 Escala de Likert

Se utilizó para medir actitudes y opiniones de los encuestados, de tal forma que se pueda capturar información específica e importante para el estudio. Para la aplicación de las encuestas se utilizó una escala de Linkert de cinco categorías: a) totalmente en desacuerdo, b) en desacuerdo, c) ni de acuerdo ni en desacuerdo, d) de acuerdo, e) totalmente de acuerdo.

2.5.2 Alfa de Cronbach

Se utilizó para evaluar el grado de confiabilidad de las encuestas como instrumentos de recolección de información, coeficiente Alfa de Cronbach, podría variar entre 0 y 1, mientras más se aproxime a su valor máximo, la escala propuesta es más fiable, un valor superior a 0.7 garantiza la confiabilidad de la escala, y se define a través de la siguiente ecuación.

$$\alpha = \left(\frac{K}{k-1}\right)\left[1 - \frac{\sum Vi}{Vt}\right]$$

Donde:
$\alpha = alfa\ de\ crombach$
$K = numero\ de\ preguntas\ (ítem)$
$Vi = varianza\ de\ cada\ ítem$
$Vt = varianza\ total$

2.5.3 VALIDACIÓN POR JUICIO DE EXPERTOS

El juicio de experto es una técnica valida, confiable y aceptada como medio de validación. Se define como una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en el tema, y que pueden dar información, evidencia, juicios y valoraciones. Skjong, en el 2001, [14], propuso diversos criterios de selección de expertos, entre los que destacan a) la experiencia en realizar juicios y toma de decisiones basada en evidencias o experticia (grados, investigaciones, publicaciones, posición, experiencia y premios entre otras), b) reputación en la comunidad, (c) disponibilidad y motivación para participar, y d) imparcialidad y cualidades inherentes como confianza en sí mismo y adaptabilidad.

Autores como Skjong, en [14], propusieron diversos pasos para realizar el juicio de expertos, de los cuales destacan: a) Preparar instrucciones y planillas, b) seleccionar los expertos y entrenarlos, c) explicar el contexto, d) posibilitar la discusión, y e) establecer el acuerdo entre los expertos por medio del cálculo de consistencia

El estadístico Kendall, es una medida que permite evaluar el nivel de concordancia entre los expertos, generando un valor entre cero y uno. El valor de 1 significa una concordancia de total acuerdo entre los expertos, mientras que el valor de 0, representa un total desacuerdo [14].

CAPÍTULO III RESULTADOS Y DISCUSIÓN

3.1 DIAGNÓSTICO DE LAS EMPRESAS DE MODELADO NUMÉRICO

En la actualidad, en el Perú existe un número reducido de empresas especializadas en servicios de modelado numérico, debido que requieren personal altamente técnico y especializado. En su mayoría las empresas grandes que realizan EIA subcontratan los servicios de modelado numérico a empresas especializadas, más pequeñas. En el mercado, existe una variedad de empresas que ofrecen los servicios de modelado numérico para proyectos de ingeniería, principalmente asociadas a proyectos de hidrocarburos, construcción de infraestructuras marino portuarias, transporte de sedimentos marinos, dispersión de sustancias sobre el medio marino entre otros.

3.1.1 Empresas de modelado numérico ambiental

En su mayoría, los servicios de modelado numérico, son desarrollados por empresas especializadas y/o por profesionales independientes en forma de consultorías, la mayoría se ubican en la ciudad de Lima, desarrollan sus actividades bajo un enfoque empírico de gestión de seguridad y riesgos de la información, con controles mínimos en cuanto a disponibilidad, confidencialidad e integridad de la información, se identifican a empresas:

A) DELIMAR S.A.C., empresa especializada en brindar servicios de monitoreo y modelado numérico marinos costeros, oceánicos, fluvial e hidrológicos. Para el desarrollo de los servicios cuenta con personal técnico especializado, con capacidad de análisis e interpretación de información ambiental, con experiencia en el desarrollo de estudios de modelado numérico en el Perú y el extranjero. Tiene como objetivo estratégico, liderar personal y recursos, bajo un enfoque de cuidar la seguridad, la salud y el medio ambiente; tiene como valores fundamentales la responsabilidad, dedicación y colaboración; como visión estratégica, aspira a ser una empresa con alta responsabilidad social y ambiental.

B) INBIOMA S.A.C., empresa dedicada a la prestación de servicios de consultoría ambiental con experiencia en estudios de ingeniería en medios marinos, fluviales y lacustres, cuenta con personal especializado en la gestión de recursos humanos, con capacidad de manejo eficiente de subcontrataciones de diversos servicios relacionados a ingeniera. Tiene como objetivo estratégico generar alternativas con la ventaja de disponer de información primordial para la gestión del medio marino y fluvial; sus valores estratégicos son la responsabilidad, la colaboración, y el compromiso; como visión espera

ser una empresa líder en el campo de la consultoría, especializada en el sector ambiental, acuático, biológico, microbiológico, defensa y agrario.

C) GAPASH CONSULTORÍA INTEGRAL E.I.R.L., empresa que brinda soluciones de ingeniería y consultoría ambiental con un enfoque de soluciones integrales y sostenibles al proyecto de inversión o actividad económica en curso, tiene como objetivo estratégico desarrollar soluciones en ingeniería y consultoría ambiental con innovación, y alineada a una estrategia de gestión consensuada con los clientes; sus valores estratégicos son la honestidad, compromiso, creatividad; como visión espera desarrollar un servicio de ingeniería de consulta ambiental de alta calidad y de satisfacción de sus clientes coadyuvando a que estos alcancen el objetivo deseado al demandar sus servicios.

D) FISMATLAB S.A.C., empresa que ofrece servicios de desarrollo de aplicativos computacionales para procesamiento y análisis de información ambiental, este tipo de servicios está orientado a empresas, organizaciones gubernamentales, y a personas particulares, que usen o gestionen datos o información ambiental, por otro lado brinda servicios de modelado numérico ambiental a empresas consultoras que realizan EIA, como parte del inicio, desarrollo y operación de nuevos proyectos de ingeniería, estos servicios son ofrecidos a distintas empresas consultoras a nivel regional y/o nivel nacional. Tiene como objetivo estratégico, llegar a ser un socio estratégico en el desarrollo de soluciones informáticas y estudios de evaluación ambiental; sus valores estratégicos son la responsabilidad, profesionalismo, honestidad y compromiso; tiene como visión de negocio llegar a ser una empresa de alta capacidad técnica, con estándares internacionales para el desarrollo de soluciones informáticas y estudios de evaluación ambiental.

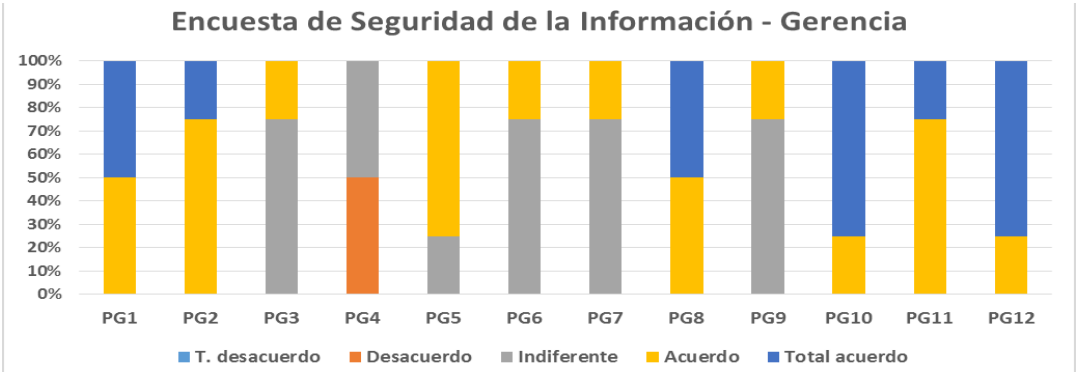
3.1.2 Situación actual de la actividad de modelado numérico ambiental

Para conocer la situación actual de la actividad de modelado numérico ambiental, se recurrió a cuatro empresas, las mismas que por motivos de confidencialidad son mencionadas como empresa 01, 02, 03 y 04, a las cuales se consultó a través de una encuesta dirigida a sus directivos y profesionales sobre la gestión de la seguridad de la información durante el desarrollo de sus servicios, llegándose a obtener que:

A nivel directivo, se tiene que todos ellos se encuentran comprometidos con la seguridad de la información de sus clientes en sus empresas, los resultados se muestran en la Figura Nº 7. Respecto a aprobar e implementar políticas de Seguridad de la Información, el 75%

de los directivos se muestran indiferentes a aprobar y comunicar políticas de seguridad de la información. El 50% se muestra indiferente a contratar personal, mientras que el 50% restante se muestra en desacuerdo en contratar personal para la gestión de la seguridad de la información. Estos resultados muestran que los directivos tienen conocimientos limitados sobre la gestión de la seguridad de la información en sus empresas y más aún en los servicios que ofrecen. Respecto a la gestión de riesgos, el 75% de los encuestados manifiestan estar de acuerdo en la gestión de los riesgos de la seguridad de la información, pero a su vez son indiferentes a implementar sist de gestión.

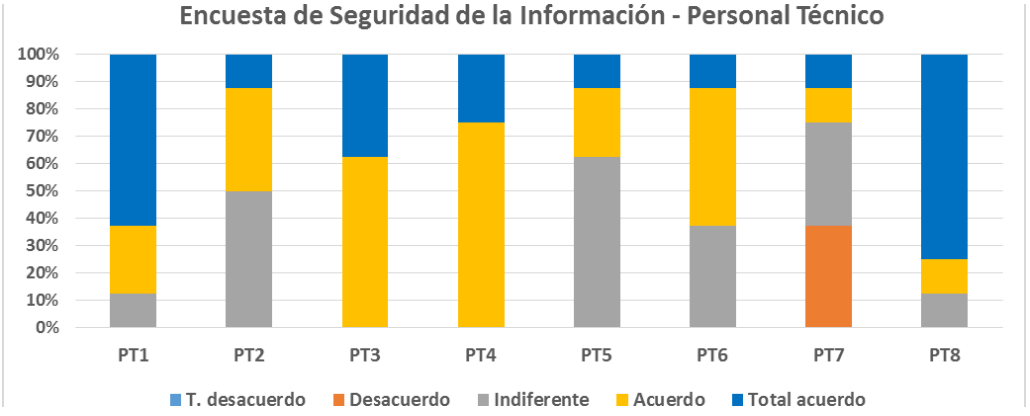
Figura Nº 7: Resultado de encuesta a directivos de empresas



Fuente: elaboración propia

A nivel del personal técnico, más de 60% de los encuestados se encuentran disponibles a seguir metodologías asociadas a seguridad de la información y consideran importante llevar un control de cambio (pregunta 03 y 04 de la encuesta), sin embargo al ser consultados sobre la disponibilidad de documentar incidentes de seguridad de la información, se manifiestan indiferentes, Figura Nº 8

Figura Nº 8: Resultado de encuesta aplicada a personal técnico de empresas



Fuente: elaboración propia

3.2 ARMONIZACIÓN DE ESTANDARES Y PROPUESTA DE MODELO

A continuación se analiza la estructura y contenido de estándares de gestión de la seguridad de la información, y gestión de riesgos, así como metodologías de análisis de gestión de la seguridad de la información y gestión de riesgos. Llegándose a realizar la armonización de los estándares basado en los principios de cada estándar, los conceptos y directrices que definen la seguridad de la información en TI, la evaluación de riesgos de TI, y la valoración de los activos de TI, principalmente basado en la ISO/IEC 27005 y MAGERIT, listado a continuación:

ISO/IECE 27000:2018.- vocabulario estándar para sistemas de gestión de seguridad de la información

ISO/IEC 27001:2013.- Requisitos para la implantación de un sistema de gestión de seguridad de la información.

ISO/IEC 27004:201l.- Requisitos para la implantación de un sistema de gestión de seguridad de la información.

ISO/IEC 27005:2018.- Guía y técnicas para la gestión de riesgos en seguridad de la información

ISO/IEC 31000:2018.- Directrices para la gestión de riesgos

Margerit v3.0.- Metodología de análisis y gestión de riesgos de los sistemas de información.

El análisis de los estándares y metodologías se detallan en el Anexo 04.

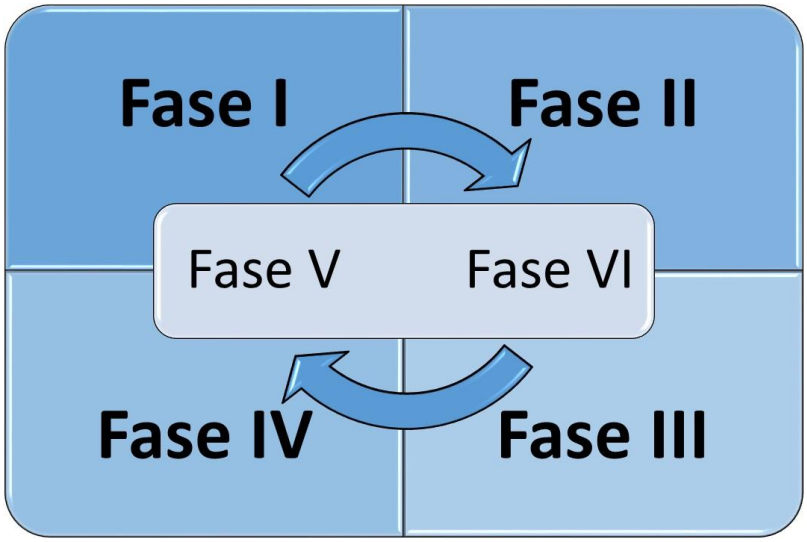
La propuesta de modelo de gestión de seguridad de información con enfoque en riesgos, sigue el ciclo de mejora continua de Planificar, Hacer, Verificar y Monitorear, es el resultado del análisis e integración de estándares internacionales y metodologías de análisis de gestión de seguridad de la información y riesgos, descritas en la sección anterior. Se basa principalmente en el estándar ISO/IEC 27005:2018 y la metodología de análisis y gestión de riesgos de los sistemas de información, denominado MAGERIT.

El modelo busca garantizar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de la información. Independientemente del

estado en que se encuentre, dentro de los procesos del negocio (sea almacenada, procesada o transmitida) o el medio que lo contenga; de tal manera que las amenazas puedan ser contrarrestadas o minimizar, reduciendo la probabilidad de impacto y mejorando la recuperación.

El modelo propuesto consta de seis fases, ver Figura Nº 9, se desagrega en actividades e instrumentos que buscan dar respuestas al qué y cómo gestionar la seguridad de la información desde un enfoque de riesgos:

Figura Nº 9: Modelo de gestión de la seguridad de la información basado en gestión de riesgo



Fuente: Elaboración propia

Fase I: Alcance y contexto
Fase II: Análisis de activos
Fase III: Análisis de riesgos
Fase IV: Tratamiento de riesgos
Fase V: Comunicación
Fase VI: Evalúa y mejora

Tabla 3: Propuesta de modelo de Gestión de Seguridad de la Información

MODELO PROPUESTO PARA LA GSI Y APORTES DE LOS ESTÁNDARES Y METODOLOGÍA DE ANÁLISIS		
Fases	**Actividades**	**Estándar o metodología utilizada**
FASE I: Contexto de la empresa y alcance de la gestión de la seguridad de la información Objetivo: Definir alcance de la gestión de la seguridad de la información	1.1 Comprender a la empresa y su actividad comercial	**ISO/IEC 27001:2013** Sección 4.1: Entiende a la organización, describe la consideraciones a tener en cuenta para comprender a la empresa u organización.
	1.2 Captura las necesidades y expectativas de las partes interesadas	**ISO/IEC 27001:2013** Sección 4.2: Entiende las necesidades de la organización, describe la consideraciones a tener en cuenta para comprender las necesidades de la empresa u organización.
	1.3 Define el alcance de la gestión de la seguridad de la información	**ISO/IEC 27001:2013** Sección 4.3: Determina el alcance del sistema de gestión de la seguridad de la información.
	1.4 Establece el contexto interno y externo Análisis FODA Contexto interno Estructura organizacional Capacidades Procesos del servicio de modelado Contexto Externo Contexto normativo y regulatorio Relación con los clientes Alianzas estratégicas Contexto económico Contexto tecnológico Contexto socio-cultural Relación con proveedores	**ISO/IEC 27001:2013** Sección 4.1: Entiende a la organización y su contexto describe la consideraciones a tener en cuenta para comprender a la empresa u organización dé la empresa u organización, en el contexto interno y externo en que desarrolla sus actividades comerciales.
FASE II: Análisis de activos	2.1 Identificación de procesos de negocio asociados al servicio de modelado numérico	MAGERIT V3.0 Libro II: Catalogo de elemento

MODELO PROPUESTO PARA LA GSI Y APORTES DE LOS ESTÁNDARES Y METODOLOGÍA DE ANÁLISIS		
Fases	**Actividades**	**Estándar o metodología utilizada**
Objetivo: Identificar y valor los activos asociados a la seguridad de la información asociada al servicio.		Sección 2: Define a la información y los servicios como elementos esenciales para la gestión de la seguridad de la información
	2.2 Identificación de activos	MAGERIT V3.0 Libro II: Catalogo de elemento Sección 2.1, 2.2, 2.3, 2.5, 2.6, 2.7, 2.9, 2.10, 2.12: Categorías de activos
	2.3 Valorización de activos (D, I, C)	MAGERIT V3.0 Libro II: Catalogo de elemento Sección 3: Dimensiones de valoración y Sección 4: criterios de valoración
FASE III: Análisis de riesgos Objetivo: identificar y valorar las amenazas asociadas a la información asociada al servicio	3.1 Identificación de amenazas y vulnerabilidades por procesos de servicios	MAGERIT V3.0 Libro II: Catalogo de elemento Sección 5: Amenazas, se toma como base el catálogo de amenazas descrito en la sección 5 de MAGERIT.
	3.2 Valorización de la probabilidad de ocurrencia	V MAGERIT V3.0 Libro II: Catalogo de elemento Sección 5: Amenazas, se toma como base el catálogo de amenazas descrito en la sección 5 de MAGERIT.
	3.3 Valorización del impacto del riesgo	ISO 31000:2018 Sección 6.4.2: identificación del riesgo, encontrar, reconocer y describir los riesgos que ayuden o impidan el logro de la gestión de la información. Sección 6.4.4: Valoración del riesgo.
	3.4 Evaluación del Riesgo Riesgo = Probabilidad x Impacto	ISO/IEC 27005:2018 Sección 8: Evaluación de seguridad de la información. ISO/IEC 31000:2018 Sección 6: Proceso de análisis de riesgo
	3.5 Genera informe de impacto de información sobre servicios de modelado	SO/IEC 27004:2016 Sección 10.2: identificación del criterio de evaluación de medición de la seguridad de la información.

MODELO PROPUESTO PARA LA GSI Y APORTES DE LOS ESTÁNDARES Y METODOLOGÍA DE ANÁLISIS		
Fases	**Actividades**	**Estándar o metodología utilizada**
FASE IV: Tratamiento de riesgos Objetivo: Proponer planes de tratamiento de seguridad de la información	4.1 Tratamiento de riesgos	ISO/IEC 31000:2018 Sección 6.5: Tratamiento de riesgo, opciones de tratamiento de riesgos.
	4.2 Plan de tratamiento de riesgo	ISO/IEC 27005:2018 Sección 6.5: Tratamiento de riesgo, opciones de tratamiento de riesgos.
FASE V: Comunicación Objetivo: proponer estrategias de comunicación	5.1 Comunicación	ISO/IEC 27005:2018 Sección 11. Comunicación y consulta de gestión de la seguridad de la información. Describe la importancia del intercambio de información con quienes toman decisiones otras partes interesadas.
	5.2 Consulta	
FASE VI: Seguimiento y revisión Objetivo: Monitorear los planes de tratamiento propuestos	6.1 Seguimiento y revisión	ISO/IEC 27004:2016 Sección 10.3. Seguimiento, control, revisión y evaluación de la medición de la seguridad de la información.
	6.2 Cumplimiento de planes de tratamiento propuestos	

Fuente: Elaboración propia

3.3 APLICACIÓN DE CASO DE ESTUDIO

3.3.1 Fase I: Contexto de la empresa y alcance de la GSI

3.3.1.1 Comprende a la empresa y su actividad comercial

FISMATLAB S.A.C., es una empresa que ofrece servicios de desarrollo informático y asesoramiento en ingeniería de mecánica de fluidos. La empresa, por su facturación y número de trabajadores (6 personas) se categoriza como una microempresa, se ubica en la ciudad de Chiclayo con operación a nivel nacional. La empresa, ofrece dos tipos de servicios: 1) **servicios de desarrollo de aplicativos informáticos**, que consiste en la elaboración de programas, script, funciones, librerías, paquetes, Interfaces Graficas de Usuario, ejecutables, Toolboxs u otros, orientado principalmente al procesamiento de información ambiental (con énfasis en hidrología, meteorología y marina costera); **2) servicios de modelado numérico ambiental**, que consiste en la elaboración de estudios para evaluación de parámetros ambientales (físicos y biológicos), en medios acuáticos, terrestres, lacustres y aéreos, asociados a Estudios de Impacto Ambiental (EIA), a través de herramientas de modelado numérico computacional.

Misión

Brindar servicios especializados en soluciones informáticas y modelado numérico a través de TI para crear soluciones innovadoras y agiles acorde a la necesidad del cliente.

Visión

Llegar a ser una empresa que soporte sus servicios en las TI y el conocimiento técnicas de su personal, desarrollando soluciones que generen valor al cliente.

Objetivos Estratégicos

- ✓ Entregar servicios que generen valor, logrando la satisfacción del cliente.
- ✓ Ser un socio estratégico de los clientes.

Valores

Sus valores son:

- ✓ Responsabilidad,
- ✓ Profesionalismo,
- ✓ Honestidad y compromiso.

Situación actual del área de TI

Cuenta con un personal técnico que se encarga de controlar y dar soporte TI a las áreas de la empresa, priorizando la atención al área de desarrollo de aplicativos y modelado numérico, que son el Core del negocio.

3.3.1.2 Captura las necesidades y expectativas de las partes interesadas

A mediano plazo, la gerencia de la empresa se proyecta ser un socio estratégico de sus clientes para el desarrollo de estudios de modelado numérico como herramienta complementaria para la evaluación ambiental; siguiendo estándares que permitan gestionar la información y datos que confían los clientes a la empresa, especialmente en el desarrollo de servicios de modelado.

Por parte de los trabajadores de la empresa, desean seguir directivas claras en cuanto a procesamiento, resguardo y uso de la información y datos como parte de los servicios que desarrollan.

Por parte de los clientes, desean que información utilizada y generada por los estudios de modelado numérico, no sean cuestionado por las entidades evaluadoras, por lo cual requieren que se generen las evidencias necesarias.

Por parte de las instituciones evaluadoras, requieren que los estudios ambientales y sus estudios complementarios contengan información que refleje las condiciones ambientales reales y que se empleen herramientas de modelado numérico estandarizadas, de uso internacional, que utilicen información fidedigna y sin alteraciones, con las evidencias necesarias, para constatación por las instituciones estatales evaluadoras.

3.3.1.3 Define el alcance de la implementación de la GSI

- ✓ Se centra principalmente en la gestión de la seguridad de la información del área que desarrolla servicios de modelado numérico ambiental.
- ✓ Cubrirá los procesos relacionados al servicio de modelado numérico.
- ✓ La ejecución estará a cargo del personal del área y será supervisado por la gerencia de la empresa.

3.3.1.4 Establece el contexto interno y externo

Debilidades

- Presupuesto restringido para el desarrollo de proyectos internos.
- Los procesos de negocios no se encuentran bien definidos.
- Cuenta con pocos clientes.
- Limitado número de personal para el desarrollo de los servicios
- Frecuentes cambios en la temática de los proyectos a desarrollar, lo cual reduce la especialización en desarrollo un determinado servicio.
- Inadecuada gestión del tiempo y prioridades.
- Aceptación de cambios del cliente, hasta en etapas avanzadas del servicio.
- Sigue una política reactiva antes que preventiva.

Fortalezas

- Por el número de personas y tamaño de la empresa, se podría adaptar fácilmente al cambio.
- La empresa cuenta con el personal técnico especializado.
- El personal de TI capaz de ofrecer soluciones al área de modelado.
- La captación de clientes se da a través de recomendación directa.
- Amplia experiencia en temas de modelado numérico.
- Utilizar herramientas de programación y TI.
- Genera soluciones de acorde a las necesidades del cliente.

Amenazas

- Riesgo de pérdida de información
- Surgimiento de nuevas empresas en el mismo rubro
- La inconformidad de los clientes por servicios o productos que no han llenado sus necesidades.
- Aparición de nuevas tecnologías de información que podrían generar una brecha en el uso de las tecnologías.

Oportunidades

- Recientemente se están dando una serie de normativas que generan demanda de servicios de modelado numérico.
- Se está ampliando el nicho de mercado de los servicios de modelado en IEA.
- La gestión de datos e información viene cobrando mayor importancia.

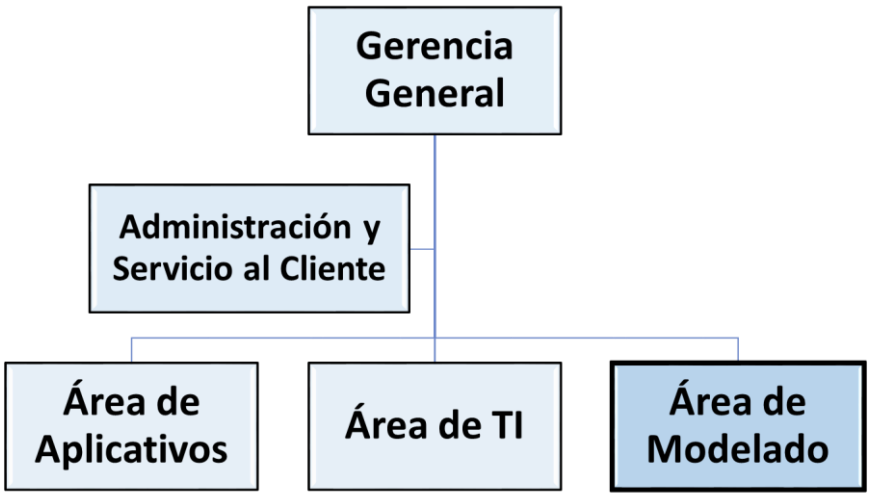
- La empresa se encuentra en un nicho de mercado muy especializado.
- Se espera el incremento de inversiones en diversos sectores económicos.
- Disminución del costo y mayor accesibilidad a las TI.

Contexto interno

La empresa cuenta con cinco área, que abarcan desde la gerencia general hasta las áreas de desarrollo, las cuales se listan a continuación:

1) **Gerencia**: comprende a la gerencia general y directorio de la empresa.
2) **Área Administrativa y Servicio al Cliente:** comprende al área que lleva la parte contable, administrativa y de atención al cliente; entre sus actividades más frecuentes realizan cotizaciones y acuerdo de servicios con los clientes.
3) **Área de Desarrollo de Aplicativos**: comprende al área donde se desarrollan script, funciones, librerías, paquetes, ejecutables, Toolbox (denominados aplicativos) en software como Python, Matlab, Fortran 90; por otro lado se realiza procesamiento de información ambiental, para lo cual se hace uso de software de programación, como Matlab y Python.
4) **Área de TI**: comprende al área que actualiza la información en la plataforma web, realiza soporte de TI, actualiza las licencias de software, lleva el inventario de software y hardware, coordinar servicios con proveedores externo, realiza backup de información.
5) **Área de Modelado Numérico**: comprende al área que elabora estudios para evaluación de parámetros ambientales (físicos y biológicos), en medios acuáticos, terrestres, lacustres y aéreos, asociados a EIA, haciendo uso de herramientas de modelado numérico computacional especializadas.

Figura Nº 10: Organigrama de la empresa FISMATLAB S.A.C.



Fuente: Elaboración propia

La gerencia se proyecta a mediano y largo plazo, llegar a ser un socio estratégico en el desarrollo de soluciones informáticas y estudios de modelado numérico como herramienta complementaria para la evaluación ambiental; su visión de negocio es de llegar a ser una empresa con alta capacidad técnica, y siguiendo estándares que permitan crear soluciones innovadoras y agiles.

Contexto externo

- **Normativo y regulatorio**: diversas instituciones estatales incluyen a las herramientas de modelado numérico como una opción de evaluación de impacto ambiental. El ministerio de la producción en [15, p. 14], menciona, que “en caso no exista información hidrométrica deberá generarse información en base a modelos matemáticos, determinísticos o estocásticos los mismos que serán calibrados con información registrada en la cuenca”.
- **Relación con los clientes**: se mantiene buena relación con los clientes, basado en la confianza y respeto mutuo, aunque los clientes son pocos, esporádicamente demandan de servicios, principalmente porque conocen el trabajo desarrollado y porque a lo largo del tiempo se ha mejorado en la atención a los requerimientos de cada uno de ellos.

- **Alianzas estratégicas**: se mantiene compromisos de exclusividad con clientes antiguos.
- **Contexto económico**: actualmente la economía peruana se encuentra en recesión por los efectos de la pandemia COVID-19, que viene afectando a nivel global, situación que perduraría durante el 2020, sin embargo el Banco Mundial, proyecta "una fuerte recuperación de la economía peruana post-pandemia, retomando una tasa de crecimiento promedio del PBI de 3.1% (promedio anual entre 2014 a 2019)" [16], lo cual impulsaría la inversión privada en el país y la región Lambayeque e incrementaría los requerimientos de estudios de modelado numéricos para EIAs.
- **Contexto tecnológico**: de acuerdo a IDC, consultora de prestigio internacional que analiza la tendencia de la industria de TI, en su reporte de finales del 2019, proyectó para el 2020 un crecimiento del 4.8% de la industria de TI en América Latina, impulsado principalmente por las inversiones en Cloud, Inteligencia Artificial, seguridad de la información, hardware y servicios" [17], está proyección se vio suspendida por la pandemia COVID-19, pero sería retomada post-pandemia.
- **Competencia**: existe competencia principalmente en la ciudad de Lima, donde operan la mayoría de empresas que se dedican al desarrollo de EIAs, por otro, se conoce que gran parte de los trabajos de modelado numérico es desarrollado por profesionales de diversas temáticas (ing. civiles, ing. mecánicos de fluidos, ing. ambientalistas, hidrógrafos, meteorólogos, físicos, biólogos, químico, matemáticos entre otras profesiones), en su mayoría como prestación de servicios no personales.
- **Social y cultural**: Mantiene relación de participación y apoyo con algunas asociaciones civiles y colegios profesionales a nivel regional, principalmente a través de impartir charlas.
- **Relación con proveedores**: algos servicios se terciarizan, como el servicio de hosting, a cargo de la empresa Bluehosting (https://www.bluehosting.pe), el servicio espacio en la nube con la empresa AWS (https://aws.amazon.com)

Discusión de la FASE I

Se analizó el contexto interno y externo que influye sobre el servicio de negocios de modelado numérico que se desarrolla en la empresa, así mismo se analizó las fortalezas,

debilidades, amenazas y oportunidades bajo las cuales opera el servicio, llegándose a determinar que los datos e información, son elementos claves para para el desarrollo del servicio. En este sentido se plantea que la gestión de la seguridad de la información se centra principalmente en el área de desarrollo de servicios de modelado numérico, su ejecución estará a cargo del personal de la misma área y será supervisado por la gerencia de la empresa.

3.3.2 Fase II: Identificación de activos en la empresa

3.3.2.1 Identificación de procesos asociados al servicio de modelado numérico

La empresa por su organización cuenta con dos áreas de desarrollo, pero la aplicación de caso de estudio se centra en el servicio de modelado numérico, este servicio comprende nueve procesos de negocios, que se detallan en la Tabla 4.

Tabla 4: Principales procesos de negocio asociados al servicio de modelado

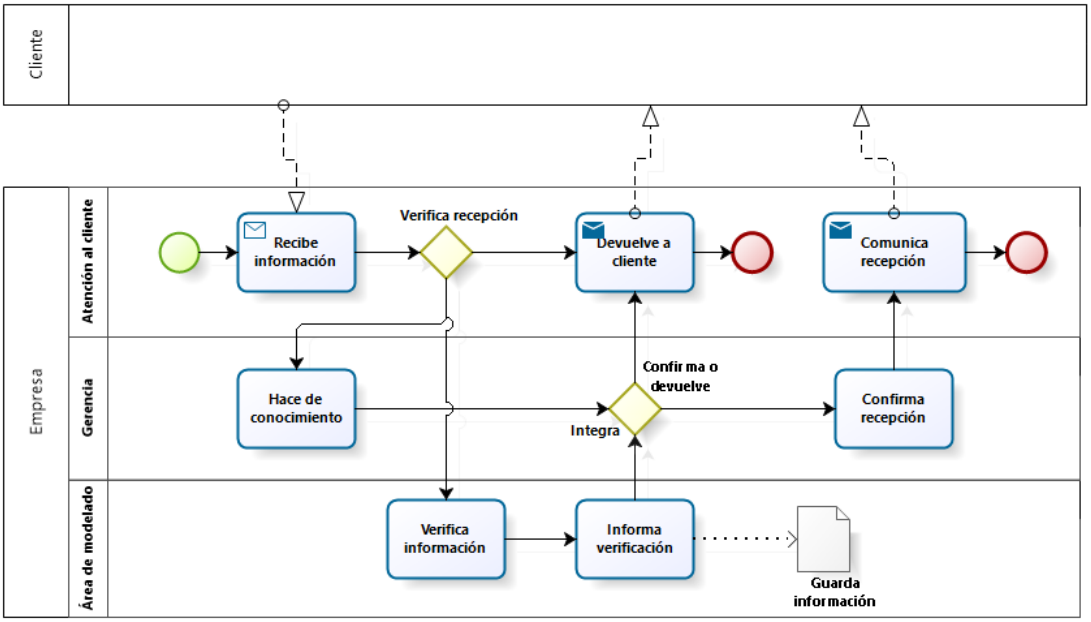
Código	Procesos de negocio
PN_01	Atención de requerimientos de servicios
PN_02	Recibe información para servicio (ver Figura Nº 11)
PN_03	Entrega información de avance (ver Figura Nº 12)
PN_04	Procesamiento de información (ver Figura Nº 13: Esquema de proceso negocio (PN_04)
PN_05	Ejecución de modelado numérico (ver Figura Nº 14)
PN_06	Actualiza y mantiene herramientas de TI
PN_07	Mantiene inventario de información y datos
PN_08	Genera informes, reportes u opiniones técnicas
PN_09	Asiste y coordina reuniones

Fuente: Elaboración propia

En la Figura Nº 11, se muestra el esquema del proceso de negocio que se sigue en la empresa para la recepción de la información que es entregada por parte del cliente para el desarrollo del servicio de modelado. En este proceso, el personal técnico es quien verifica e informa que la información recibida es la necesaria para realizar el servicio solicitado; la gerencia se mantiene informado y confirma la recepción de la información;

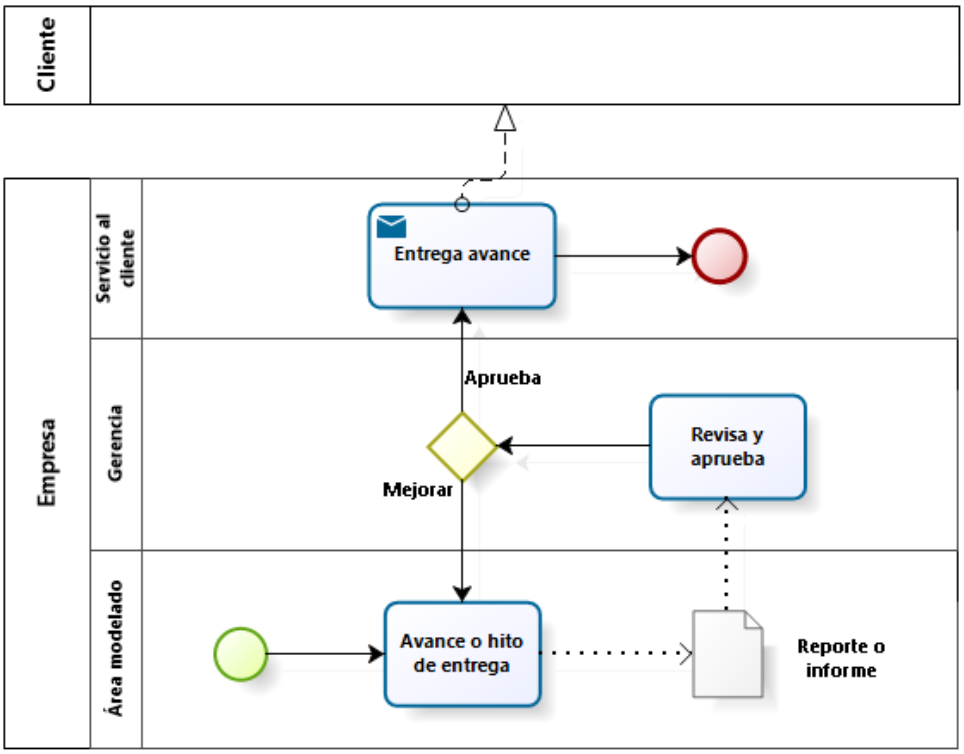
mientras que el personal de atención al cliente es el encargado de mantener comunicación con el cliente, ya sea para devolver la información o confirmar la recepción de la misma. En la Figura Nº 12, se muestra el esquema del proceso de entrega de información o avance de entregable de parte de la empresa al cliente, este proceso inicia en el área técnica con la generación de un reporte de avance, un informe preliminar o muestras de resultados preliminares (que podría ser imágenes o información); la gerencia revisa y aprueba o solicita mejoras el entregable del área técnica, para luego pasa a atención al cliente; el personal de atención al cliente se encarga de hacer llegar el entregable al cliente, vía correo electrónico.

Figura Nº 11: Esquema de proceso negocio (PN_02)



Fuente: Elaboración propia en Bizagi

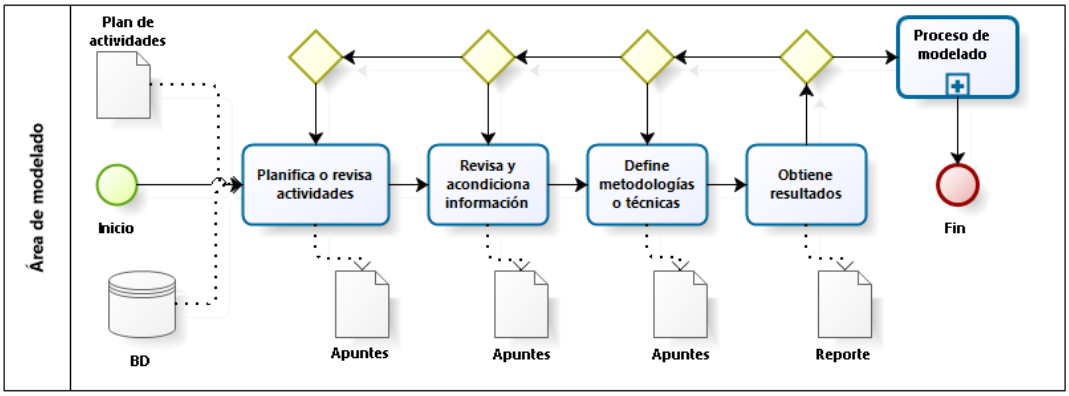
Figura Nº 12: Esquema de proceso negocio (PN_03)



Fuente: Elaboración propia en Bizagi

En la Figura Nº 13, se muestra el esquema del procesamiento de información ambiental, que consisten en un conjunto de actividades secuenciales que se realizan exclusivamente en área de modelado numérico, que inician con la planificación de actividades y consulta a la Base de datos. Posteriormente se revisa y acondiciona la información, en algunos casos es necesarios realizar conversión de unidades de medidas pasando al sistema internacional (para volumen es frecuente convertir galones, pies cúbicos, barriles a metros cúbicos; para longitud es frecuente convertir pies, brazas a metros o millas marinas a kilómetros). El procesamiento secuencial de la información genera resultados, en caso los resultados no sean los apropiados para el proceso siguiente (proceso de modelado), se vuelve a algunas de las etapas preliminares, cabe precisar que cada una de las etapas se toman apuntes que serán utilizados en la generación de reportes.

Figura Nº 13: Esquema de proceso negocio (PN_04)



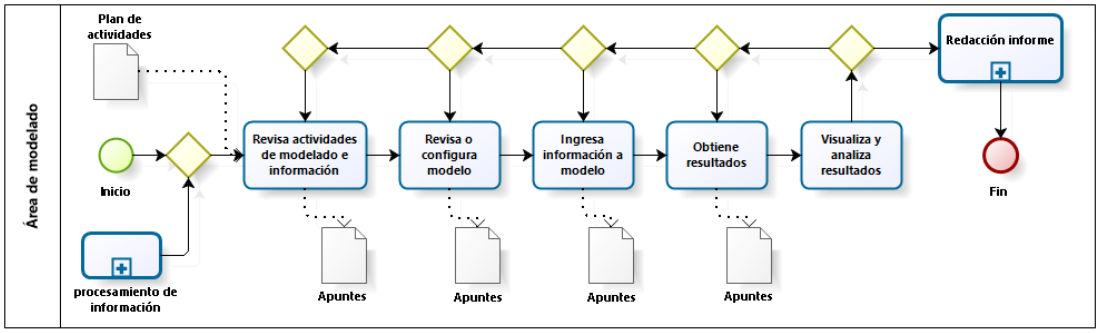
Fuente: Elaboración propia en Bizagi

En la Figura Nº 14, se muestra el esquema de ejecución del proceso de modelado numérico, este proceso consisten en un conjunto de actividades secuenciales que se realizan exclusivamente en área de modelado numérico, inician con la planificación de actividades y revisión de la información disponible (Figura Nº 13).

Una vez que se haya revisado el plan de trabajo a desarrollar, se procede a revisar la operatividad del modelo numérico, en algunos caso será necesario realizar la configuración o reconfiguración del modelo numérico. Posteriormente se ingresa la información al modelo y ejecuta, llegándose a obtener los resultados, los cuales son analizados con herramientas de visualización grafica (2D y/o 3D). Una vez visualizado los resultados, es posible que se identifiquen alguna información inconsistente, por lo cual será necesarios volver a algunas de las etapas preliminares, cabe precisar que cada una de las etapas se registra apuntes que serán utilizados en la generación de reportes.

Los resultados del modelado numérico sirven de insumos para la redacción de informe preliminares o finales.

Figura Nº 14: Esquema de proceso negocio (PN_05)



Fuente: Elaboración propia en Bizagi

3.3.2.2 Identificación de activos

Entrada: Lista categorizada de activos de TI.

Salida: Tabla de identificación de activos de TI.

Procedimiento: La identificación de los activos se realizó a través de entrevista al personal encargado del área de modelado numérico y al gerente general de la empresa. Para el registro de la información se utilizó la plantilla del anexo 5.1: identificación de activos.

De acuerdo a MAGERIT v 3.0, dentro de la gestión de la seguridad de la información se identifica a los activos de TI de la empresa, los cuales se encuentran definidos en la Tabla 13 del anexo 5.1, y asociados al servicio de modelado en la empresa.

En la Tabla 5 se muestra el listado de activos de TI agrupados por cada tipo de activo y asignado a cada proceso de negocio al que está relacionado, todos estos activos se asocian al servicio de modelado numérico en la empresa.

En cuanto al proceso de atención de requerimientos de servicios de modelado numérico, se encontró mayor asociación con los siguientes activos de TI: información de los servicios de modelado numérico, información de los clientes (de carácter reservada y privada), software y hardware informático, equipos auxiliares (como fuentes de alimentación, impresoras, mobiliarios y estante), personal encargado de la función y clientes con quienes interactúa.

En cuanto al proceso de recepción de información para servicio de modelado numérico, se encontró mayor asociación con los siguientes activos de TI: Base de datos existente en la empresa, Backup de información, información y documentos técnicos de carácter reservado y de uso exclusivo para el servicio, información de acceso a plataformas o software especializados, software y hardware informático, equipos auxiliares (como fuentes de alimentación, impresoras, mobiliarios), y el personal encargado de la función (que involucra al profesional del área de modelado, el gerente de la empresa y el técnico de atención al cliente).

En cuanto al proceso de entrega información y/o entregables de parte de la empresa hacia el cliente, se encontró mayor asociación con los siguientes activos de TI, informes, reporte o entregables producidos por la empresa, Base de datos existente, Backup de información, información y documentos técnicos de carácter reservado y de uso exclusivo para el servicio, información de acceso a plataformas o software especializados, software y hardware informático, equipos auxiliares (como fuentes de alimentación, impresoras, mobiliarios), y el personal encargado de la función (que involucra al profesional del área de modelado, el gerente de la empresa y el técnico de atención al cliente).

En cuanto al proceso de procesamiento de información, se encontró mayor asociación con los siguientes activos de TI: Bases de datos existentes, Backup de información, información y documentos técnicos de carácter reservado y de uso exclusivo para procesamiento de información, información de acceso a software especializados (de cálculo numérico y visualización grafica), equipos auxiliares (como fuentes de alimentación, impresoras, mobiliarios), y el personal encargado del área de modelado numérico.

En cuanto al proceso de ejecución de modelado numérico se encontró mayor asociación con los siguientes activos de TI: Bases de datos existentes, Backup de información, información y documentos técnicos de carácter reservado y de uso exclusivo para modelado numérico, información de acceso a configuración de modelos numéricos, software especializados, equipos auxiliares (como fuentes de alimentación, impresoras, mobiliarios), y el personal encargado del área de modelado numérico.

En cuanto a los procesos de actualización y mantenimiento de herramientas de TI y mantenimiento de inventario de información y datos, se asocian mayormente con los

software y hardware, soporte TI, equipos auxiliares eléctricos, información de licencias de software y en una segunda instancia se asocian con la información que contienen, y el personal del área de TI.

En cuanto al proceso de generación de informes, reportes u opiniones técnicas, se encontró mayor asociación con los activos de TI como Base de datos, documentos e informes técnicos existentes, software y hardware especializado, equipos de recolección de información, modelos numéricos, y el personal encargado del área de modelado numérico.

En cuanto al proceso de asistencia y coordinación de reuniones, se encontró que habría mayor asociación con los activos de TI como: información de la empresa, y el gerente de la empresa (o quien lo represente).

Tabla 5: Activos asociados los procesos de negocio de la empresa

Código	Activo de TI	PN_01	PN_02	PN_03	PN_04	PN_05	PN_06	PN_07	PN_08	PN_09
D01	Bases de datos (marina, ríos, meteorológica, ambiental)		X	X	X	X			X	
D02	Códigos fuentes de programas (> 50)			X	X	X			X	
D03	Información de configuración de modelos numéricos especializados					X	X	X		
D04	Copias de respaldo de servicios de modelado (reportes e informes)		X	X	X	X			X	
D05	Copias de respaldo de desarrollo de aplicativos (código fuentes, plantillas)				X			X		
D06	Información de cotización de servicios	X	X	X						
D07	Informes y/o reportes digitales	X	X	X	X	X	X	X	X	
D08	Información reservada de clientes		X	X					X	
D09	Documentos técnicos personalizados para realizar servicios de negocio.		X	X	X	X	X		X	
D10	Información de licencias, permisos de uso, usuarios y claves de acceso				X	X	X	X		
D11	Listado de servicios	X	X							X

Código	Activo de TI	PN_01	PN_02	PN_03	PN_04	PN_05	PN_06	PN_07	PN_08	PN_09
S01	Acceso a software de desarrollo de aplicativos informáticos			X	X	X		X	X	
S02	Acceso a modelos numéricos				X	X	X	X		
S03	Acceso a plataforma Cloud AWS				X	X	X	X		
S04	Acceso a visualización grafica			X	X	X				
S05	Acceso a correos electrónicos	X	X	X	X	X	X	X	X	X
S06	Consultas a BD		X	X	X	X			X	
S07	Actualización web						X	X		
S08	Soporte de TI						X	X		

Código	Activo de TI	PN_01	PN_02	PN_03	PN_04	PN_05	PN_06	PN_07	PN_08	PN_09
SW01	Software de pre procesamiento			X	X	X			X	
SW02	Software de modelado (marino, meteorológico, ambiental, etc.)				X	X			X	
SW03	Visualizador gráfico (Matlab, SIG)			X	X			X	X	
SW04	Paquete ofimática (Word, Excel,…)	X	X	X	X	X	X	X	X	X
SW05	Sistemas operativos (Windows, Linux)	X	X	X	X	X	X	X	X	X
Sw06	Software de equipos ambientales (sonómetro, estación meteorológica)				X	X	X			
SW07	Correo electrónico	X	X	X	X	X	X	X	X	X
Sw08	Software administrativo	X	X	X					X	
H01	Computadoras (2)				X		X			
H02	Laptops (5)	X	X	X	X	X		X	X	X
H03	Soporte red (2 switch, 1 router)						X	X		
H04	Cableado de red			X	X	X				

Código	Activo de TI	PN_01	PN_02	PN_03	PN_04	PN_05	PN_06	PN_07	PN_08	PN_09
H05	Sonómetro (4), Radiómetro (1), termómetros (4), radiosondas (2),…				X					
H06	Dispositivos móviles	X	X	X	X	X	X	X	X	X
Código	**Activo de TI**	**PN_01**	**PN_02**	**PN_03**	**PN_04**	**PN_05**	**PN_06**	**PN_07**	**PN_08**	**PN_09**
COM01	Internet	X	X	X	X	X	X	X	X	
COM02	Red local (4 equipos conectados)				X	X	X	X		
COM03	Wifi (2 áreas)	X	X	X	X	X	X	X	X	
Código	**Activo de TI**	**PN_01**	**PN_02**	**PN_03**	**PN_04**	**PN_05**	**PN_06**	**PN_07**	**PN_08**	
Media1	Discos duros externos (5 HD x 1TB)				X	X				
Media2	Documentos impresos (informes, reportes, manuales, guías,…)	X	X	X	X	X	X	X	X	X
Media3	Memorias USB (8 x 32 GB)	X	X	X	X	X	X	X	X	X
Código	**Activo de TI**	**PN_01**	**PN_02**	**PN_03**	**PN_04**	**PN_05**	**PN_06**	**PN_07**	**PN_08**	**PN_09**
Aux01	Fuente de alimentación (220 Voltios)	X	X	X	X	X	X	X	X	X
Aux02	Mobiliarios (10)	X	X	X	X	X	X	X	X	X
Aux03	Equipo de ventilación (2)	X	X	X	X	X	X	X	X	X
Aux04	Gabinetes (5)	X	X	X	X	X	X	X	X	X
Código	**Activo de TI**	**PN_01**	**PN_02**	**PN_03**	**PN_04**	**PN_05**	**PN_06**	**PN_07**	**PN_08**	**PN_09**
P01	Ingeniero informático						X	X		
P02	Ingeniero mecánico de fluidos	X	X	X	X	X			X	X
P03	Asistente informático						X	X		
P04	Administrativo y atención al cliente	X	X	X					X	
P05	Gerente	X	X	X	X	X	X	X	X	X
P06	Usuario	X	X	X						X

Fuente: Elaboración propia

3.3.2.3 Valorización de activos (D, I, C)

Entrada: Tabla de identificación de activos de TI.

Salida: Tabla de valoración de activos de TI.

Procedimiento: La identificación de los activos se realizó a través de entrevista al personal encargado del área de modelado numérico y al gerente general de la empresa. Para el registro de la información se utilizó la plantilla del anexo 5.1: identificación de activos.

En la Tabla 6, se muestra el detalle de la valoración de los activos, lo cual se realiza en base a la valoración de las dimensiones de disponibilidad (D), integridad (I) y confidencialidad (C), que se encuentran definidas en el anexo 5.1.

Tabla 6: Valoración de activos asociados al servicio de modelado numérico

Código	Activo asociados al servicio de modelado	Valoración del activo				
		D	I	C	Valor de criticidad	
D01	Bases de datos (marina, ríos, meteorológica, ambiental)	4	4	4	**12**	**Alto**
D02	Códigos fuentes de programas (> 50)	4	4	4	**12**	**Alto**
D03	Información de configuración de modelos numéricos especializados	4	4	4	**12**	**Alto**
D04	Copias de respaldo de servicios de modelado (reportes e informes)	4	4	4	**12**	**Alto**
D05	Copias de respaldo de desarrollo de aplicativos (código fuentes, plantillas)	4	4	4	**12**	**Alto**
D06	Información de cotización de servicios	2	4	4	**10**	**Alto**
D07	Informes y/o reportes digitales	2	4	4	**10**	**Alto**
D08	Información reservada de clientes	4	3	4	**11**	**Alto**
D09	Documentos técnicos personalizados para realizar servicios de negocio.	3	4	4	**11**	**Alto**
D10	Información de licencias, permisos de uso, usuarios y claves de acceso	3	4	4	**11**	**Alto**
D11	Listado de servicios	3	3	2	**8**	**Medio**
S01	Acceso a software de desarrollo de aplicativos informáticos	4	4	4	**12**	**Alto**
S02	Acceso a modelos numéricos	4	4	4	**12**	**Alto**
S03	Acceso a plataforma Cloud AWS	4	4	4	**12**	**Alto**
S04	Acceso a visualización grafica	4	4	4	**12**	**Alto**
S05	Acceso a correos electrónicos	4	4	4	**12**	**Alto**
S06	Consultas a BD	4	4	4	**12**	**Alto**
S07	Actualización web	3	2	2	**7**	**Medio**
S08	Soporte de TI	3	2	2	**7**	**Medio**
SW01	Software de pre procesamiento	4	4	4	**12**	**Alto**

Código	Activo asociados al servicio de modelado	Valoración del activo				
		D	I	C	Valor de criticidad	
SW02	Software de modelado (marino, meteorológico, ambiental, etc.)	4	4	4	**12**	**Alto**
SW03	Visualizador gráfico (Matlab, SIG)	4	4	4	**12**	**Alto**
SW04	Paquete ofimática (Word, Excel,…)	2	3	2	**7**	**Medio**
SW05	Sistemas operativos (Windows, Linux)	4	4	4	**12**	**Alto**
Sw06	Software de equipos ambientales (sonómetro, estación meteorológica)	4	4	4	**12**	**Alto**
SW07	Correo electrónico	2	3	3	**9**	**Medio**
Sw08	Software administrativo	1	3	3	**7**	**Medio**
H01	Computadoras (2)	3	3	3	**9**	**Alto**
H02	Laptops (5)	3	3	3	**9**	**Alto**
H03	Soporte red (2 switch, 1 router)	3	3	3	**9**	**Alto**
H04	Cableado de red	2	2	3	**7**	**Medio**
H05	Sonómetro (4), Radiómetro (1), termómetros (4), radiosondas (2),…	3	4	4	**11**	**Alto**
H06	Dispositivos móviles	2	4	2	**8**	**Medio**
COM01	Internet	2	3	3	**8**	**Medio**
COM02	Red local (4 equipos conectados)	2	3	3	**8**	**Medio**
COM03	Wifi (2 áreas)	2	3	3	**8**	**Medio**
Media1	Discos duros externos (5 HD x 1TB)	3	4	4	**11**	**Alto**
Media2	Documentos impresos (informes, reportes, manuales,…)	3	4	4	**11**	**Alto**
Media3	Memorias USB (8 x 32 GB)	3	4	4	**11**	**Alto**
Aux01	Fuente de alimentación (220 Voltios)	4	4	4	**12**	**Alto**
Aux02	Mobiliarios (10)	2	2	2	**6**	**Medio**
Aux03	Equipo de ventilación (2)	1	1	3	**5**	**Medio**
Aux04	Gabinetes (5)	1	1	3	**5**	**Medio**
P01	Ingeniero informático	4	4	4	**12**	**Alto**
P02	Ingeniero mecánico de fluidos	4	4	4	**12**	**Alto**
P03	Asistente informático	4	4	4	**12**	**Alto**
P04	Administrativo y atención al cliente	4	4	4	**12**	**Alto**
P05	Gerente	4	4	4	**12**	**Alto**
P06	Usuario	4	4	4	**12**	**Alto**

Fuente: Elaboración propia

3.3.3 Fase III: Análisis de riesgos

3.3.3.1 Identificación de amenazas y vulnerabilidades por procesos de servicio

Entrada: procesos de negocios e identificación de amenazas y vulnerabilidades

Salida: Tabla de identificación de amenazas y vulnerabilidades

Procedimiento: La identificación de las amenazas y vulnerabilidades se realizó a través de entrevista al personal encargado del área de modelado numérico y al gerente general de la empresa. Durante este proceso se tuvo en cuenta los tipos de amenazas de origen industrial, errores y fallos no intencionados, y ataque intencionado, definidas en el anexo 5.4. Para el registro de la información se utilizó el formato de identificación de amenazas sobre activos del anexo 5.4.
De acuerdo a la ISO 27001, las amenazas son las "situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de los activos de información", mientras que las vulnerabilidades se definen como la debilidad de un activo o control que ser explotada por una o más amenazas.

En la Tabla 7, se detallan las amenazas y vulnerabilidades que podrían verse afectados en cada uno de los procesos asociados al servicio de modelado numérico

En cuanto al proceso de atención de requerimientos de servicios y recepción de información se podría ver afectada la confiabilidad de la empresa, principalmente por seguir procedimientos inadecuados. Mientras que en cuento a entrega de información se podría afectada la disponibilidad de productos y entregables, generando una afectación a la confiabilidad de la empresa.

En cuanto a los procesos de procesamiento de información y ejecución de modelos numéricos, entre las principales afectación se tendría la disponibilidad de la servicios de modelado, como consecuencia de la indisponibilidad de las herramientas de TI, y la desconfianza de la integridad de la información procesada e incluida en el modelo numérico, produciendo de esta forma afectación a la confiabilidad de los procedimiento utilizados y de la empresa en su conjunto.

En cuanto a los procesos de actualización y mantenimiento de herramientas de TI y mantenimiento de inventario de información y datos, se podría ver afectada la continuidad de la prestación del servicio, como consecuencia de no utilizar procedimientos adecuados. En cuanto al proceso de generación de informes, reportes u opiniones técnicas, se podría ver afectada la confiabilidad de la empresa, sobre todo por el uso de procedimientos inadecuados, viéndose también afectada la confidencialidad de la información, y la capacidad técnica de la empresa.

Tabla 7: Identificación de amenazas y vulnerabilidades por proceso de negocio

Proceso de negocio	Amenazas	Vulnerabilidades
PN_01	- Error en atención de requerimientos de servicio	- Inconformidad por parte del cliente. ***"Afecta la confiabilidad de la empresa en cuanto a uso de procedimientos adecuados".***
PN_02	- Inadecuada recepción de información. - Recepción de información incompleta o insuficiente - Retrasos en la recepción de la información	- Inconvenientes para el desarrollo del servicio. - Retraso en el desarrollo del servicio. - Afectación al cronograma de desarrollo del servicio. ***"Afecta la confiabilidad de la empresa en cuanto a uso de procedimientos adecuados".***
PN_03	- Retraso en entrega de información, reportes o informes (parcial o final). - Inadecuada verificación de información a entregar. - Entrega de información no autorizada,	- Penalidad por retraso de entrega de información o informes. - Inconformidad por parte del cliente, devolución y revisión de la información - Afectación a la reputación de la empresa. ***"Afecta la confiabilidad de la empresa en cuanto disponibilidad de productos y/o entregables".***
PN_04	- No seguir procedimientos adecuados y estandarizados - No generar las evidencias necesarias para mostrar el procesamiento de la información. - Usar información no autorizada. - Hacer un mal uso de la información, - Pérdida y alteración de la información.	- Genera inconformidad de servicio. - Afecta al desarrollo del servicio. - Se difunde información reservada o privada. - Se pierde información. - Afecta a la reputación de la empresa, ***"Afecta la confiabilidad de la empresa en cuanto a confiabilidad de información generada".***

Proceso de negocio	Amenazas	Vulnerabilidades
	- Modificación, destrucción, o divulgación deliberada de información. - Manipulación inadecuada o malintencionada de programas, técnicas y/o metodologías de procesamiento de información.	
PN_05	- Desconfiguración de modelo numérico, - No seguir procedimientos adecuados y estandarizados - No generar las evidencias adecuadas. - Usos no previstos, no autorizados, o de la forma no adecuado de un modelo. - Uso inadecuado de un modelo numérico, causando observaciones y hasta desaprobación de proyectos de IEA. - Acceso no permitido a la configuración o difusión a terceros de información reservada de modelos numéricos.	- Genera retraso en el desarrollo del servicio. - Genera información inadecuada o innecesaria. - Genera inconformidad del servicio - Volver a hacer el trabajo. - No aprobación de informes por parte de las autoridades evaluadoras. - Espionaje de detalles técnicos de modelos numéricos. - Afecta la reputación de la empresa. ***"Afecta la confiabilidad de la empresa en cuanto a uso de procedimientos adecuados y confiabilidad de información generada".***
PN_06	- Indisponibilidad de herramientas de TI. - Software desactualizados - Realizar mantenimientos no autorizados o no programados. - No seguir los procedimientos adecuados. - Habilitación de servicios innecesario. - Usar software o controladores no confiables o spyware. - Deterioro de equipos de TI por falta de mantenimiento. - Alteración de secuencia de ejecución de programas o software. - Abuso de privilegios de accesos.	- Retrasa el desarrollo del servicio de modelado. - Afectar el desarrollo de un servicio de modelado. - Generar acceso no permitido a piratas informáticos. - Dar lugar a la difusión de información privada o reservada. - Ingreso de virus u otros similares - Inhabilitación de equipos de TI. ***"Afecta la confiabilidad de la empresa en cuanto a uso de procedimientos adecuados y disponibilidad de herramientas de TI y confidencialidad de la integridad de la información".***
PN_07	- No tener registros de equipos e información existente. - Desactualización de registros temporales y por áreas de equipos e información existente. - No generar o no comunicar reportes de incidentes o mantenimiento de equipos de TI.	- Desconocimiento de que la situación actual de equipos e información. - Registro desactualizado de estado de equipos e información existente en la empresa. - No contar con evidencia y no comunicar a los responsables.

Proceso de negocio	Amenazas	Vulnerabilidades
		"Afecta la continuidad de los servicios por uso de procedimientos inadecuados".
PN_08	- No aceptación de informes y/o reportes porque no cubren el requerimiento establecido, - Divulgación de informes, reportes o información no autorizada. - Entrega de informes u otros documentos con deficiente revisión. - Desaprobación u observación a informes por parte de entidades evaluadoras, - Desaprobación de informes por parte del cliente, por controversias en interpretación de requerimientos.	- Volver a realizar parte del servicio, genera aumento de costo, por de tiempo de ejecución - Divulgación de información reservada o privada. ***"Afecta la confiabilidad de la empresa en cuanto a uso de procedimientos adecuados, así mismo se podría afectar la confidencialidad de información y capacidad técnica del personal".***
PN_09	- No disponibilidad de personal o representante de la empresa para asistir a reuniones. - Toma de decisiones o compromisos no autorizados por la empresa. - Difusión no intencional de información, metodologías o procedimientos que generen perjuicio a la empresa. - Inadecuado manejo o gestión de coordinación de reuniones	***"Afecta la confiabilidad de la empresa en cuanto a uso de procedimientos adecuados, así mismo se podría afectar la confidencialidad de información y capacidad técnica del personal".***

Fuente: Elaboración propia

Una vez identificadas las amenazas y vulnerabilidades por cada uno de los procesos el negocio, se procedió a asignar la valoración del impacto y probabilidad del riesgo a cada una de las dimensiones asociadas a la seguridad de la información (Disponibilidad, Integridad y Confidencialidad), considerando la afectación en cada uno de los procesos del servicio de modelado numérico, Tabla 8.

Tabla 8: Valoración de criticidad, probabilidad e impacto de riesgos

Código	Valoración de criticidad			Impacto del riesgo			Probabilidad del riesgo		
	D	I	C	D	I	C	D	I	C
D01	4	4	4	4	4	4	4	4	4
D02	4	4	4	4	4	4	4	4	4
D03	4	4	4	4	4	4	4	4	4
D04	4	4	4	3	4	4	4	4	4
D05	4	4	4	3	4	4	4	4	4
D06	2	4	4	1	3	4	2	4	4
D07	2	4	4	2	3	4	2	4	4
D08	4	3	4	4	4	4	4	3	4
D09	3	4	4	3	3	3	3	4	4
D10	3	4	4	4	4	4	3	4	4
D11	3	3	2	1	2	2	3	3	3
S01	4	4	4	3	4	4	4	4	4
S02	4	4	4	4	4	4	4	4	4
S03	4	4	4	4	4	4	4	4	4
S04	4	4	4	2	2	4	4	4	4
S05	4	4	4	1	1	4	4	4	4
S06	4	4	4	2	2	4	4	4	4
S07	3	2	2	2	2	3	3	2	2
S08	3	2	2	3	2	2	3	2	2
SW01	4	4	4	3	3	2	4	4	4
SW02	4	4	4	4	4	2	4	4	4
SW03	4	4	4	3	3	2	4	4	4
SW04	2	3	2	2	2	2	2	3	2
SW05	4	4	4	3	4	1	4	4	4
Sw06	4	4	4	4	4	4	4	4	4
SW07	2	3	3	1	3	4	3	3	3
Sw08	1	3	3	1	2	3	1	3	3
H01	3	3	3	3	4	3	3	3	3
H02	3	3	3	3	4	3	3	3	3
H03	3	3	3	2	3	2	3	3	3
H04	2	2	3	1	3	2	2	2	3
H05	3	4	4	2	4	4	3	4	4
H06	2	4	2	2	2	2	3	4	4
COM01	2	3	3	2	2	2	2	3	3
COM02	2	3	3	2	2	2	2	3	3
COM03	2	3	3	2	2	2	2	3	3
Media1	3	4	4	3	4	4	3	4	4
Media2	3	4	4	3	3	4	3	4	4
Media3	3	4	4	1	2	4	3	4	4
Aux01	4	4	4	4	4	4	4	4	4
Aux02	2	2	2	2	2	2	2	2	2
Aux03	1	1	3	1	1	1	1	1	3
Aux04	1	1	3	1	1	3	1	1	3

Código	Valoración de criticidad			Impacto del riesgo			Probabilidad del riesgo		
	D	I	C	D	I	C	D	I	C
P01	4	4	4	4	4	4	4	4	4
P02	4	4	4	4	4	4	4	4	4
P03	4	4	4	4	4	4	4	4	4
P04	4	4	4	4	4	4	4	4	4
P05	4	4	4	4	4	4	4	4	4
P06	4	4	4	4	4	4	4	4	4

Fuente: Elaboración propia

A continuación se presenta los mapas de calor de la evaluación del riesgo por cada uno de los activos de TI asociados a los procesos de negocios de modelado numérico ambiental en la empresa, que se encuentran bajo el modelo de GSI propuesto. Los resultados se muestran por cada una de las dimensiones relacionadas de la SI (D, I y C).

A través de la evaluación de disponibilidad activos en cuanto a seguridad de la información, se llegó a identificar a los datos e información, servicios de TI, software y personas como los elementos en estado de mayor riesgo, con un impacto de crítico y una probabilidad de ocurrencia de tipo máxima, Figura Nº 15.

A través de la evaluación de integridad de la seguridad de la información, se llegó a identificar a los datos e información, servicios de TI, software, dispositivos de backup, auxiliares y personas como los elementos en estado de mayor riesgo, con un impacto de crítico y una probabilidad de ocurrencia máxima, Figura Nº 16.

A través de la evaluación de confidencialidad de la SI, se llegó a identificar a los datos e información, servicios de TI, software, dispositivos de backup, equipos auxiliares y personas como los elementos en estado de mayor riesgo, con un impacto de crítico y una probabilidad de ocurrencia de tipo máxima, Figura Nº 17.

Figura Nº 15: Riesgos de Disponibilidad de activos

PROBABILIDAD					
	4 Máximo	S05	S04, S06	D04, D05, S01, SW01, SW03, SW05	D01, D02, D03, D08, S02, S03, SW02, Sw06, Aux01, P01, P02, P03, P04, P05
	3 Alto	D11, SW07, Media3	S07, H03, H05, H06	D09, S08, H01, H02, Media1, Media2	D10
	2 Significativo	D06, H04	D07, SW04, COM01, COM02, COM03, Aux02		
	1 Mínimo	Sw08, Aux03, Aux04			
		1 Insignificante	2 Limitado	3 Importante	4 Critico
		IMPACTO			

Fuente: Elaboración propia

Figura Nº 16: Riesgos de integridad de activos

PROBABILIDAD					
	4 Máximo	S05	S04, S06, S09, H06, Media3	D06, D07, D09, SW01, SW03, Media2	D01, D02, D03, D04, D05, D10, S01, S02, S03, SW02, SW05, Sw06, H05, Media1, Aux01, P01, P02, P03, P04, P05, P06
	3 Alto		D11, SW04, Sw08, COM01, COM02, COM03	SW07, H03	D08, H01, H02
	2 Significativo		S07, S08, Aux02	H04	
	1 Mínimo	Aux03, Aux04			
		1 Insignificante	2 Limitado	3 Importante	4 Critico
		IMPACTO			

Fuente: Elaboración propia

Figura Nº 17: Riesgos de confidencialidad de activos

PROBABILIDAD					
	4 Máximo	SW05	SW01, SW02, SW03, H06	D09	D01, D02, D03, D04, D05, D06, D07, D08, D10, S01, S02, S03, S04, S05, S06, Sw06, H05, Media1, Media2, Media3, Aux01, P01, P02, P03
	3 Alto	Aux03	D11, H03, H04, COM01, COM02, COM03	Sw08, H01, H02, Aux04	SW07
	2 Significativo		S08, SW04, Aux02	S07	
	1 Mínimo				
		1 Insignificante	2 Limitado	3 Importante	4 Critico
		IMPACTO			

Fuente: Elaboración propia

3.3.4 Fase IV: Tratamiento de riesgo

En esta etapa se proponen planes de tratamiento de riesgos, que permitan mitigar el riesgo de los activos de TI en cuanto a disponibilidad, integridad y confidencialidad de información de TI. Llegándose a plantear tres proyectos que serán ejecutados por la empresa en conjunto con las partes interesadas, teniendo en cuenta las siguientes consideraciones:

- ✓ El alcance de la propuesta, los objetivos, los beneficios esperados;
- ✓ Las personas o área involucradas
- ✓ Responsables de la implementación
- ✓ Las acciones propuestas;
- ✓ Los recursos necesarios, incluyendo las contingencias;
- ✓ Las medidas de evaluación de desempeño;
- ✓ Las restricciones;
- ✓ La frecuencia de reportes o informes y seguimiento requeridos;
- ✓ El costo y plazo previsto para la realización.

A continuación se describe los tres proyectos planteado para el tratamiento del riesgo en la empresa.

1) Proyecto 01: Implementar firma digital para certificar la integridad de la información digital intercambiada entre la empresa y los clientes, y tendría alcance a la información que maneja la empresa. Este proyecto tendrá por finalidad incrementar la integridad y confiabilidad de la información, mitigando el impacto de la alteración de la información, además generará un sentido de responsabilidad de la información en las diversas etapas del servicio de modelado numérico.

2) Proyecto 02: Implementar un sistema de resguardo de información y ejecución de aplicativos en la nubes, se optará por fortalecer el uso de la plataforma AWS, específicamente en el kit de herramienta OPENFOAM, que cuenta con librería asociadas a dinámica de fluidos computacional que se podría integrar o reemplazar a las herramientas de modelado numérico que se vienen utilizando actualmente en la empresa. Este proyecto permitirá incrementar la disponibilidad de la información y ejecución de aplicativos numéricos asociados a los servicios de modelado numérico ambiental, así mismo favorecerá el acceso a la información y aplicativos especializados desde lugares externos a la empresa.
3) Proyecto 03: Realizar un programa de concientización sobre los beneficios de la gestión de la seguridad de la información y el impacto positivo que tendría en el negocio y empresa, haciendo énfasis en la disponibilidad, integridad y confidencialidad de la información.

3.3.5 Fase V: Comunicación

La empresa comunica los resultados de la evaluación del riesgo de la seguridad de la información y las medidas de mitigación que llevara a cabo (ejecución de tres proyectos de mitigación), la comunicación los hace tanto a nivel interno y externo, para lo cual tiene en cuenta lo siguiente elementos asociados a la comunicación:

- ✓ ¿Qué comunicar?,
- ✓ ¿Cuándo comunicar?,
- ✓ ¿A quién comunicar?;
- ✓ ¿Quién debe comunicar?; y
- ✓ ¿Cómo comunicación?

3.3.6 Fase VI: Seguimiento y revisión

El propósito del seguimiento y la revisión es asegurar la mejorar de la calidad y la eficacia de la implementación del sistema de gestión de la seguridad de la información, realizando el seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo, así como de responsabilidades definidas.

El seguimiento y la revisión deberían tener lugar en todas etapas de los procesos del negocio. Los resultados del seguimiento deberían incorporarse a todas las actividades de la gestión de la seguridad de la información.

Se debería documentar e informar a través de los mecanismos apropiados. Llegándose a comunicar las actividades de la gestión del riesgo y sus resultados a los miembros de la empresa; proporcionar información para la toma de decisiones; mejorar las actividades de la gestión del riesgo; manteniendo la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

La empresa debe mejorar continuamente la conveniencia y efectividad del Sistema de Gestión de Seguridad de la Información, por lo que se sugiere realizar una autoevaluación semestral de los incidentes sucedidos y amenazas materializadas en cuanto a seguridad de la información en el área de modelado numérico.

3.4 VALIDACIÓN DE JUICIO DE EXPERTOS DE MODELO

Luego de haber propuesto el modelo de gestión de seguridad de la información basado en riesgos para empresas de modelado numérico ambiental, y de haber implementado el modelo propuesto a los activos de la empresa FISMATLAB S.A.C., se recurrió a tres expertos para validar el modelo propuesto a través de juicio de expertos. Para la elección de los expertos se siguieron las indicaciones dadas en la sección 2.4 sobre validación de juicio de expertos.

Los expertos calificaron las actividades del modelo propuesto a través de la siguiente calificación: 1 = en total desacuerdo, 2 = en desacuerdo, 3 = Indiferente, 4 = De acuerdo, 5 = en total acuerdo.

Una vez obtenida la calificación de los expertos se procedió a calcular el coeficiente Tau de Kendall, Tabla 9. El cálculo del coeficiente de Kendall se realizó a través de un programa Matlab implementado para tal fin, llegándose a determinar un coeficiente de Kendall de 0.8.

Tabla 9: Resumen de validación de juicio de experto

FASE	ACTIVIDAD	Experto 01				Experto 02				Experto 03				Experto 04				Experto 05				Experto 06			
		SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA
Fase I	Actidad 01	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 02	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 03	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 04	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	3	4	4	4	3	4	4	4
Fase II	Actidad 05	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 06	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 07	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Fase III	Actidad 08	4	4	4	4	4	4	4	3	3	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 09	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 10	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Actidad 11	4	4	4	4	4	4	4	4	4	4	4	4	3	2	3	3	3	2	3	3	3	2	3	3
	Actidad 12	4	4	4	4	4	4	4	4	4	4	4	4	2	3	3	3	2	3	3	3	2	3	3	3
Fase IV	Actidad 13	4	4	4	4	4	4	4	4	2	3	3	3	2	3	3	3	2	3	3	3	2	3	3	3
	Actidad 14	4	4	4	4	4	4	4	4	2	2	2	3	3	2	3	3	3	2	3	3	3	2	3	3
Fase V	Actidad 15	4	4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	3	4	4	4	3	4	4	4
	Actidad 16	4	4	4	4	4	4	4	4	2	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4
Fase VI	Actidad 17	4	4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	3	4	4	4	3	4	4	4
	Actidad 18	4	4	4	4	4	4	4	4	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4
Caso de estudio		3	3	3	3	4	4	4	4	3	3	3	3	3	4	4	4	3	4	4	4	3	4	4	4
Aporte de riesgo		4	4	4	4	4	4	4	4	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4

Fuente: Elaboración propia

CONCLUSIONES

- ✓ Se diagnosticó el sector de servicios de modelado numérico ambiental, determinándose, que la totalidad de los directivos de estas empresas están interesados en gestionar la seguridad de la información pero a su vez invierten pocos recursos económicos para la gestión de la seguridad de la información, lo cual estaría relacionado con el desconocimiento de los beneficios que podrían obtener sobre los servicios que ofrecen.

- ✓ Se analizaron estándares y metodologías de análisis de seguridad de la información aplicables a servicios de modelado numérico, llegándose a realizar la armonización de los estándares desde la perspectiva de los principios de la metodología, los procesos de gestión, la valoración de los activos de TI, la evaluación de los riesgos, el tratamiento, la comunicación y la mejora continua de los procesos de la Gestión de SI, llegándose a plantear una propuesta de modelo de GSI basado en la gestión de riesgos.

- ✓ Se propuso un modelo de gestión de seguridad de la información basado en riesgos, para apoyar en los servicios de modelado numérico, el cual consta de seis fases, dando valoración a los activos de TI y a la identificación de los riesgos asociados a los servicios de negocio.

- ✓ Se implementó el modelo de gestión de seguridad de la información basado en herramientas de riesgos en una empresa local, llegándose a implementar todas las fases del modelos propuesto, se identificaron los procesos asociados a los procesos del servicio de modelado, se valoraron los activos de TI, se identificaron los riesgos asociados a los servicios de negocio y a los activos de TI, identificándose a los actividad de datos, personas y sistemas como los elementos de mayor riesgo, para lo cual se propusieron tres medidas de mitigación en forma de proyectos, 1) Proyecto de firma digital

- ✓ El modelo fue validado por seis expertos, con calificación de aceptable, además de las fases del modelo se validó el caso de estudio y el aporte del riesgo en el modelo propuesto.

DISCUSIÓN

- ✓ La validación del modelo se realizó a través del juicio de experto, para lo cual se recurrió a seis expertos, de los cuales dos fueron expertos en modelado numérico, todos evaluaron las fases y sus actividades del modelo de gestión de seguridad de la información, con una calificación aceptable. La calificación conjunta, alcanzo un coeficiente de Cronbach de 0.95 (α=0.95), lo cual indicaría que el instrumento aplicado para la evaluación de los expertos es confiable, alcanzado una concordancia de Kendal de 0.79.

BIBLIOGRAFÍA

[1] EPA, «EPA,» 30 07 2020. [En línea]. Available: https://espanol.epa.gov. [Último acceso: 15 08 2020].

[2] Ley 27446, *Ley del Sistema Nacional de Evaluación de Impacto Ambiental*, Lima, 1992.

[3] S. M. Toapanta Toapanta, L. E. Mafla Gallegos, M. J. Chévez Morán y J. G. Ortiz Rojas, «Analysis of Models of Security to Mitigate the Risks, Vulnerabilities and Threats in a Company of Services of Telecommunications,» *3rd International Conference on Information and Computer Technologies (ICICT),* pp. 445-450, 2020.

[4] NOAA, «Policy and Procedures for IT Security Risk Management and Conducting Risk Assessments,» NESDIS Quality Procedure, 2013.

[5] NOAA, «Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission,» NOAA, 2014.

[6] B. De Longueville, «ommunitybased geoportals:,» *Computers, Environment and,* pp. 299-308, 2010.

[7] J. S. Horsburgh, A. K. Aufdekampe, E. Mayorga, K. A. Lehnert, L. Hsu, L. Song, A. S. Jones, S. G. Damiano, D. G. Tarboton, I. Zaslavsky y T. Whitenack, «Observations Data Model 2: A community information model for spatially discrete Earth observations,» *Environmental Modelling and Software,* vol. 79, p. 5574, 2016.

[8] K. Beven, W. Buytaert y L. A. Smith, «On virtual observatories and modelled realities (or why discharge must be treated as a virtual variable),» *Hidrologic Processes,* vol. 26, pp. 1905-1908, 2012.

[9] D. E. Comercio, «En qué consistió el ciberataque a los bancos peruanos y cómo se repelió,» Diario El Comercio, Lima, 2018.

[10] Estado Peruano, «Ley Nº 27446: Ley del Sistema Nacional de Evaluación de Impactos Ambientales,» Diario El Peruano, Lima, 2008.

[11] D. G. Correa Chilón, «Simulación Numérica del Sistema de Afloramiento frente a las Costas de Lambayeque,» Lambayeque, 2012.

[12] E. Ingol y M. E. Castañeda Zavaleta, «DIRECTRICES PARA EL MODELAMIENTO DE AGUAS SUBTERRÁNEAS EN PERÚ,» 2017.

[13] R. Hernández Sampiere, C. Fernández Collado y P. Baptista Lucio, Metodología de la investigación, Mexico: Mc Graw Hill, 2014.

[14] R. &. W. B. Skjong, «Expert Judgement and risk perception,» *International Offshore and Polar Engineering Conference*, pp. 17-22, 2001.

[15] PRODUCE, *Guía para la elaboración de estudios de impacto ambiental (eia) en la actividad acuícola de mayor escala,* Lima, 2008.

[16] Banco Mundial, «El Banco Mundial en el Perú,» 16 abril 2020. [En línea]. Available: https://www.bancomundial.org/es/country/peru/overview. [Último acceso: 06 agosto 2020].

[17] IDC, «La industria de TI en Latinoamérica crecerá 1.3% en 2019 y 4.8% para 2020,» IDC, 21 noviembre 2019. [En línea]. Available: https://www.idc.com/getdoc.jsp?containerId=prLA45665419. [Último acceso: 06 agosto 2020].

[18] E. B. Mackay y C. J. A. M. K. B. B. J. P. M. G. M. M. E. Wilkinson, «Digital catchment observatories: A platform for engagement and knowledge exchange between catchment scientists, policy makers, and local communities,» *Water Resource Research,* vol. 51, pp. 4815-4822, 2015.

[19] M. Malathi, «Cloud Computing Concept,» Department od Computer Science, Bangalore, Karnataka, India, 2011.

[20] F. J. Dominguez-Mayo, J. A. Garcia-Garcia, M. J. Escalona, M. Mejias, M. Urbierta y G. Rossi, «A framework and tool to manage Cloud Computing service quality,» *Software Quality Journal,* vol. 23, pp. 259-625, 2015.

[21] Carrasco, Metodología de investigación científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación, Lima: San Marcos, 2009.

[22] M. Rojas, Manual de Investigación y Redacción científica, Lima, 2010.

[23] HYCOM, «Modelo Hidrodinamico de Coordenadas Curvilines,» HYCOM, [En línea]. Available: www.hycom.org. [Último acceso: 2018 08 20].

[24] MERCATOR, «Proyecto de pronostico operacional del mar,» MERCATOR, [En línea]. Available: www.mercator.com. [Último acceso: 2018 08 20].

[25] Jan, Van Bon et al., *Fundamentos de ITIL®V3*, Van Haren Publishing Zaltebommel, 2008.

[26] P. Cooper, «Knowledge and Wisdom,» *Anaesthesia and Intensive Care Medicine,* vol. 1, nº 15, p. 44, 2014.

[27] International Standar Organization, «ISO/IEC 27000,» 07 09 2018. [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en. [Último acceso: 07 09 2018].

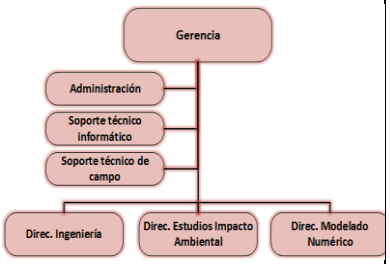
[28] G. M. &. A. A. R. J. Sullivan, «Analyzing and interpreting data from likert-type scales,» *Journal of graduate medical education,* vol. 5, nº 4, pp. 541 - 542, 2013.

[29] ecured, «Coeficiente de Kendall,» [En línea]. Available: https://www.ecured.cu/Coeficiente_de_Kendall. [Último acceso: 25 07 2019].

ANEXOS

Anexo 01: Resumen de empresas participantes

Tabla 10: Información de diagnóstico de empresas de modelado numérico

Concepto	**Empresa 01**	**Empresa 02**	**Empresa 03**	**Empresa 04**
Sector	Servicios de consultoría	Servicios de consultoría ambiental	Asesoramiento empresarial e ingeniería	Servicios de consultoría y tecnología
Fecha de creación	abril del/2007	marzo del 2010	mayo del 2014	mayo del 2015
Organigrama de la empresa		Gerencias, contabilidad, servicios de ingeniería y servicios de modelado	- Gerencia -- Administración -- Servicios --- Servicios EIA --- Servicios de Ingeniería --- Servicios de Modelado	
Misión	Brindar servicios de ingeniería amigables con el medio marino y fluvial.	Crear soluciones integrales y creativas en busca del desarrollo y progreso mediante la aplicación de tecnología moderna para un mejor aprovechamiento racional de los recursos. Llegando, de esta manera a satisfacer los requerimientos de nuestros Clientes mediante la prestación de servicios confiables.	Ser reconocida como una de las 10 principales empresas en ingeniería de consulta ambiental en el mercado nacional, con un paradigma de gestión innovador.	Brindar un servicio de calidad basado en nuestra experiencia.

Concepto	Empresa 01	Empresa 02	Empresa 03	Empresa 04
Visión	Llegar a ser una empresa con alta responsabilidad social y ambiental en el desarrollo de nuestros servicios y de nuestros clientes.	Ser una empresa Consultora, líder en el campo de la consultoría diversificada en los sectores ambiental, acuático, biológico, microbiológico, defensa, agrario y Supervisión	Desarrollar un servicio de ingeniería de consulta ambiental de alta calidad y de satisfacción de nuestros clientes coadyuvando a que estos alcancen el objetivo deseado al demandar nuestros servicios.	Llegar a ser una empresa de alta capacidad técnica, con estándares internacionales para el desarrollo de soluciones informáticas y estudios de evaluación ambiental.
Valores	Responsabilidad, dedicación y colaboración	Responsabilidad, colaboración, compromiso	Honestidad, compromiso, creatividad	Responsabilidad, profesionalismo, honestidad y compromiso
Objetivos estratégicos	Liderar personal y recursos, en áreas de seguridad, salud y medio ambiente, operaciones y logística en la mar y fluvial	Generar alternativas con la ventaja de disponer de información primordial para la gestión del medio marino y fluvial.	Desarrollar soluciones en ingeniería de consulta ambiental con innovación, y alineada a una estrategia de gestión consensuada con nuestros clientes	Ser un socio estratégico en el desarrollo de soluciones informáticas y estudios de evaluación ambiental en general.
Descripción del área de TI	Cuenta con un personal técnico que brinda servicios técnicos de soporte computacional a la empresa. Pero a la vez cada profesional y personal de la empresa se hace cargo y responsable del buen funcionamiento del equipo informático a cargo.	Cuenta con un personal técnico que brinda servicios técnicos de soporte computacional a la empresa. Pero a la vez cada profesional y personal de la empresa se hace cargo y responsable del buen funcionamiento del equipo informático a cargo.	Cuenta con personal técnico offline para el soporte de la infraestructura computacional de la empresa. A mediano plazo espera implementar un área de soporte técnico e informático. Actualmente cada profesional y personal de la empresa se hace cargo y responsable del buen funcionamiento del equipo informático a cargo.	Cuenta con un personal técnico que se encarga de controlar y dar soporte a la infraestructura computacional local y remota (alojado en hosting remoto) que se utiliza para el desarrollo de los diversos servicios que la empresa.

Fuente: Elaboración propia

Anexo 02: Diagnostico de la situación de las empresas

Para el diagnóstico de la importancia que tiene la gestión de la seguridad de la información en las empresas que ofrecen servicios de modelado numérico ambiental, se elaboró dos encuestas, una dirigida a los directivos de las empresas y una segunda encuesta dirigida al personal técnico que realizan los trabajos de modelado numérico en las empresas.

A nivel de gerencia se elaboraron 12 preguntas que buscan determinar el compromiso de los directivos respecto a la gestión de la seguridad de la información respecto a los servicios de modelado ambiental que ofrecen las empresas, ver **Anexo 03**

Las preguntas de las encuestas están dirigidas a evaluar diversos aspectos de la seguridad de la información en cada empresa encuestada, bajo los diversos aspectos de la ISO/IEC 27001:2013: Requisitos para la Gestión de la seguridad de la información.

A nivel técnico se elaboraron 8 preguntas que buscan determinar el grado de compromiso, conciencia y aceptación de parte del personal a usar herramientas, buenas prácticas, y seguir directivas asociadas a la gestión de la seguridad de la información respecto a los servicios de modelado ambiental que desarrollan en sus respectivas empresas, ver **Anexo 03**

Tabla 11: Validación de encuesta aplicada a directivos (ISO/IEC 27001:2013)

Ítem	Aspectos a evaluar	Preguntas
01	Contexto de la organización: ✓ Comprender la organización y su contexto ✓ Comprender las necesidades y expectativas de las partes interesadas ✓ Determinar el alcance del sistema de gestión ✓ de seguridad de la información ✓ Sistema de gestión de seguridad de la información	PG1
02	Liderazgo: ✓ Liderazgo y compromiso ✓ Política ✓ Roles, responsabilidades y autoridades organizacionales	PG2 y PG3
03	Planificación: ✓ Acciones para tratar los riesgos y las oportunidades ✓ Objetivos de seguridad de la información y planificación para conseguirlos	PG5 y PG9
04	Soporte: ✓ Recursos ✓ Competencia ✓ Concientización ✓ Comunicación ✓ Información documentada	PG4 y PG7
05	Operación: ✓ Planificación y control operacional ✓ Evaluación de riesgos de seguridad de la información ✓ Tratamiento de riesgos de seguridad de la información	PG6 y PG11
06	Evaluación del desempeño: ✓ Monitoreo, medición, análisis y evaluación ✓ Auditoría interna ✓ Revisión por la gerencia	PG12
07	Mejoras ✓ No conformidades y acción correctiva ✓ Mejora continua	PG8 y PG10

Fuente: Elaboración propia

Tabla 12: Validación de encuesta aplicada a técnico (ISO/IEC 27001:2013)

Ítem	Aspectos a evaluar	Preguntas
01	Contexto de la organización: ✓ Comprender la organización y su contexto ✓ Comprender las necesidades y expectativas de las partes interesadas ✓ Determinar el alcance del sistema de gestión ✓ de seguridad de la información ✓ Sistema de gestión de seguridad de la información	PT1
02	Liderazgo: ✓ Liderazgo y compromiso ✓ Política ✓ Roles, responsabilidades y autoridades organizacionales	PT5
03	Planificación: ✓ Acciones para tratar los riesgos y las oportunidades ✓ Objetivos de seguridad de la información y planificación para conseguirlos	PT2
04	Soporte: ✓ Recursos ✓ Competencia ✓ Concientización ✓ Comunicación ✓ Información documentada	PT4 y PT7
05	Operación: ✓ Planificación y control operacional ✓ Evaluación de riesgos de seguridad de la información ✓ Tratamiento de riesgos de seguridad de la información	PT3
06	Evaluación del desempeño: ✓ Monitoreo, medición, análisis y evaluación ✓ Auditoría interna ✓ Revisión por la gerencia	PT6
07	Mejoras ✓ No conformidades y acción correctiva ✓ Mejora continua	PT8

Fuente: Elaboración propia

Anexo 03: Aplicación de encuesta a directivos de empresas

Encuesta para evaluar la gestión de la seguridad de la información para apoyar los servicios de modelado numérico ambiental

Responsable: Lic. David Correa Chilón
Maestría de Gestión de Tecnologías de Información
Universidad Católica Santo Toribio de Mogrovejo, Chiclayo

Objetivo:

Recopilar información sobre la gestión de la seguridad de la información y riesgos durante el desarrollo de servicios de modelado numérico ambiental.

Se define a la *Seguridad de la Información*, como el conjunto de medidas preventivas y reactivas, que las empresas implementan en sus respectivas áreas o direcciones a fin de reducir la probabilidad e impacto de riesgos interno y externos. En este caso se buscaría mantener la confidencialidad, disponibilidad e integridad de los datos e información que utilizada para el desarrollo de los servicios de modelado numérico ambiental.

Nota: Para responder cada una de las preguntas, considere la calificación de 1 a 5, en donde 1 equivale a la calificación más baja o a estar totalmente en desacuerdo y 5 equivale a la calificación más alta o total de acuerdo.

1	2	3	4	5
Totalmente en desacuerdo	En desacuerdo	Es indiferente	De acuerdo	Totalmente de acuerdo

1) SECCIÓN DIRIGIDA A LA GERENCIA DE LAS EMPRESA

ÍTEM	PREGUNTAS	CALIFICACIÓN
PG1	¿Qué tan comprometida esta la dirección o gerencia con la seguridad de la información y datos que genera su empresa?	
PG2	¿Qué tan comprometida esta la dirección o gerencia con la seguridad de la información y datos que entregan sus clientes a su empresa para el desarrollo de los servicios?	
PG3	La dirección o gerencia cuenta con políticas de seguridad de la información, son debidamente aprobadas y comunicadas a los empleados y clientes externas.	
PG4	La empresa cuenta o tiene interés en contratar personal para gestionar la seguridad de la información de los servicios de modelado numérico	
PG5	Que tanta importancia da la gerencia a la gestión de los riesgos con fines de preservar la confidencialidad, disponibilidad e integridad de los datos e información que utiliza para el desarrollo de los servicios de modelado numérico.	
PG6	La gerencia, direcciones y/o jefes de área son conscientes y promueven el valor que tendría la gestión de la seguridad de la información en los servicios de la empresa y del impacto que tendría en la confianza y satisfacción de los clientes	
PG7	Se informa a los clientes sobre las políticas, estrategias y buenas prácticas de gestión de seguridad de la información y riesgos de la información y datos que utiliza la empresa para brindar los servicios	
PG8	¿Qué tan importante o necesario considera, incluir cláusulas de seguridad de la información y riesgos en los cuerdos de niveles de servicios?	
PG9	La empresa promueve políticas de desarrollo e implementación de seguridad de la información para reducción de riesgos asociado al resguardo de la información y datos de la empresa y clientes	

PG10	¿Qué tanto podría impactar la gestión de seguridad de la información y mitigación de riesgos en el prestigio de su empresa?	
PG11	¿La empresa prioriza las políticas de seguridad de la información y riesgos para la sub contratación de servicios de proveedores o terceros?	
PG12	¿Qué tan importancia debería tener el monitoreo, revisión y la auditoria de la gestión de la seguridad de la información en la entrega de los servicios asociados al modelado numérico ambiental?	

Fuente: Elaboración propia

Nota: La encuesta fue validada con los controles de la ISO/IEC 27001:2013.- Requisitos para la Gestión de la seguridad de la información

2) SECCIÓN DIRIGIDA AL ÁREA TÉCNICA

ÍTEM	PREGUNTAS	CALIFICACIÓN
PT1	¿Qué tan comprometido está usted y sus colegas en seguir políticas, estrategias o buenas prácticas de gestión de seguridad de la información?	
PT2	¿Con que frecuencia recibe capacitación sobre el valor de la información y los datos de la empresa?	
PT3	En el desarrollo de su trabajo, aplica metodologías asociadas a la seguridad de la información, por ejemplo aplica copias de seguridad, usa cadenas de custodia, copias en la nube, o cualquier otro mecanismo de protección de datos.	
PT4	¿Qué tanta importancia da a los procedimientos de control de cambios, a solicitud de nuevos requerimientos de parte de los clientes externos o internos?	
PT5	Lleva un control de los errores o actividades que ponen en riesgo la seguridad de la información o datos en el trabajo que realiza.	
PT6	Utiliza un sistema de gestión o sigue buenas prácticas de seguridad de la información en el trabajo que realiza	
PT7	Considera burocrático u obstruccionista realizar la documentación detallada o reportar a sus superiores sobre diversas ocurrencias de eventos de riesgos de la información y datos de la empresa y los clientes.	
PT8	El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información le permite reducir la probabilidad o el impacto de incidentes futuros.	

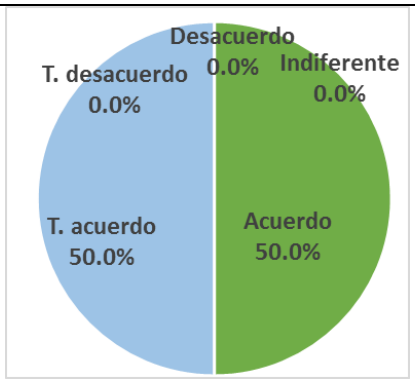
Fuente: Elaboración propia

Nota: La encuesta fue validada con los controles de la ISO/IEC 27005:2018.- Requisitos para la Gestión de la seguridad de la información.

Resultados de encuestas dirigida a gerentes de negocio

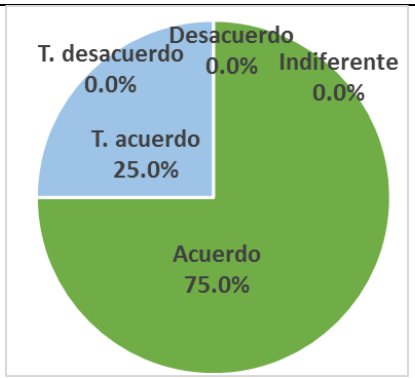
PG01. ¿Qué tan comprometida esta la dirección o gerencia con la seguridad de la información y datos que genera su empresa?

Respuesta		Encuestados	Porcentaje
	En total desacuerdo	0	0%
	En desacuerdo	0	0%
	Indiferente	0	0%
	De acuerdo	2	50%
	En total acuerdo	2	50%
	Total	4	100%



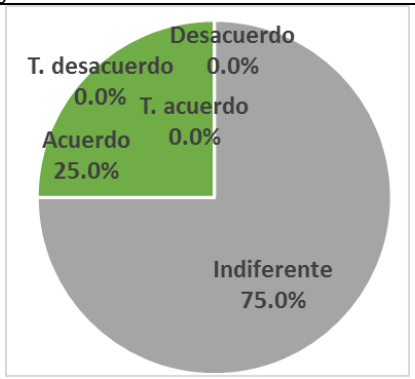
PG02. ¿Qué tan comprometida esta la gerencia con la seguridad de la información y datos que entregan sus clientes a su empresa para el desarrollo de los servicios?

Respuesta		Encuestados	Porcentaje
	En total desacuerdo	0	0%
	En desacuerdo	0	0%
	Indiferente	0	0%
	De acuerdo	2	50%
	En total acuerdo	2	50%
	Total	4	100%



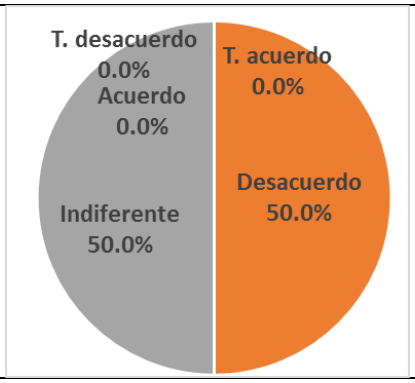
PG03. La dirección o gerencia cuenta con políticas de seguridad de la información, son debidamente aprobadas y comunicadas a los empleados y clientes externas.

Respuesta		Encuestados	Porcentaje
	En total desacuerdo	0	0%
	En desacuerdo	0	0%
	Indiferente	0	0%
	De acuerdo	2	50%
	En total acuerdo	2	50%
	Total	4	100%



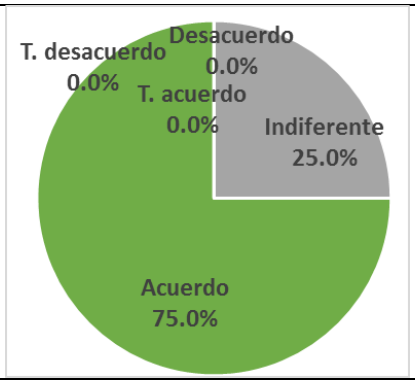
PG04. La empresa cuenta o tiene interés en contratar personal para gestionar la seguridad de la información de los servicios de modelado numérico

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



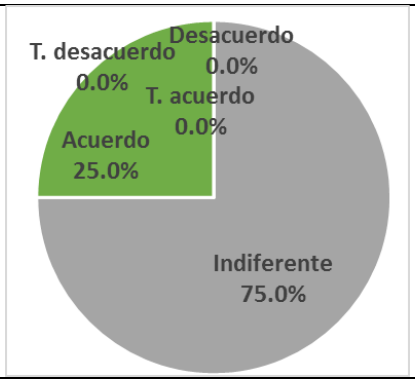
PG05. Que tanta importancia da la gerencia a la gestión de los riesgos con fines de preservar la confidencialidad, disponibilidad e integridad de los datos e información que utiliza para el desarrollo de los servicios de modelado numérico.

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



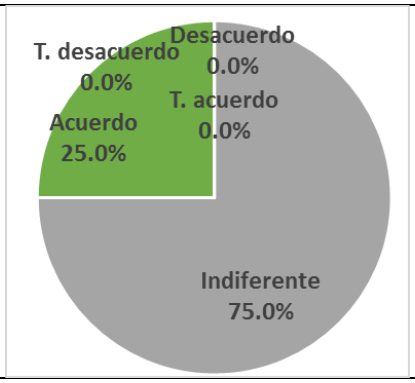
PG06. La gerencia, direcciones y/o jefes de área son conscientes y promueven el valor que tendría la gestión de la seguridad de la información en los servicios de la empresa y del impacto que tendría en la confianza y satisfacción de los clientes.

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



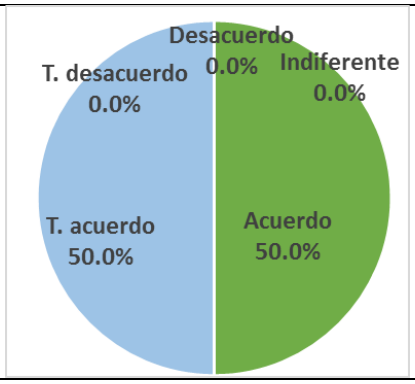
PG07. Se informa a los clientes sobre las políticas, estrategias y buenas prácticas de gestión de seguridad de la información y riesgos de la información y datos que utiliza la empresa para brindar los servicios

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



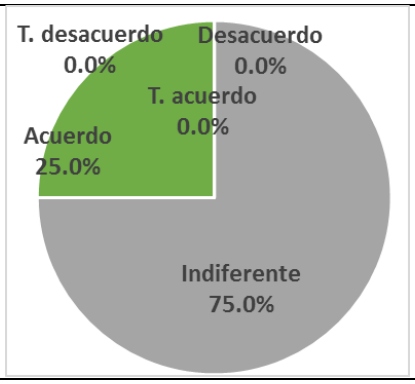
PG08. ¿Qué tan importante o necesario considera, incluir cláusulas de seguridad de la información y riesgos en los cuerdos de niveles de servicios?

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



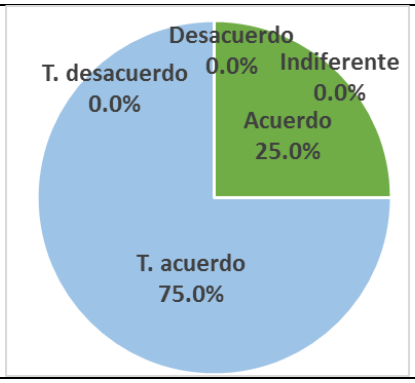
PG09. La empresa promueve políticas de desarrollo e implementación de seguridad de la información para reducción de riesgos asociado al resguardo de la información y datos de la empresa y clientes

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



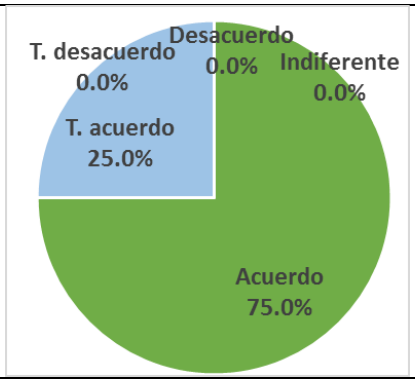
PG10 ¿Qué tanto podría impactar la gestión de seguridad de la información y mitigación de riesgos en el prestigio de su empresa?

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



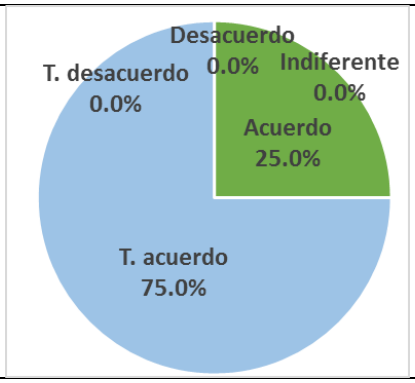
PG11 La empresa promueve políticas de desarrollo e implementación de seguridad de la información para reducción de riesgos asociado al resguardo de la información y datos de la empresa y clientes

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



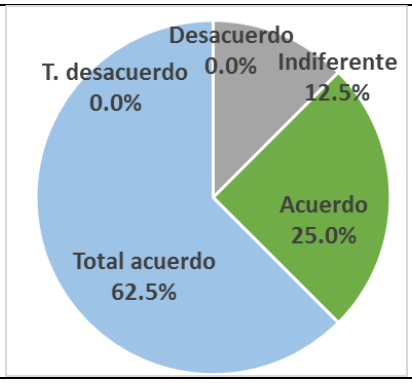
PG11 ¿Qué tan importancia debería tener el monitoreo, revisión y la auditoria de la gestión de la seguridad de la información en la entrega de los servicios asociados al modelado numérico ambiental?

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	2	50%
En total acuerdo	2	50%



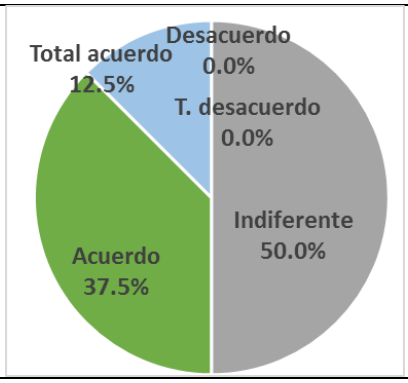
PT01 ¿Qué tan comprometido está usted y sus colegas en seguir políticas, estrategias o buenas prácticas de gestión de seguridad de la información?

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	1	12.5%
De acuerdo	2	25%
En total acuerdo	5	62.5%



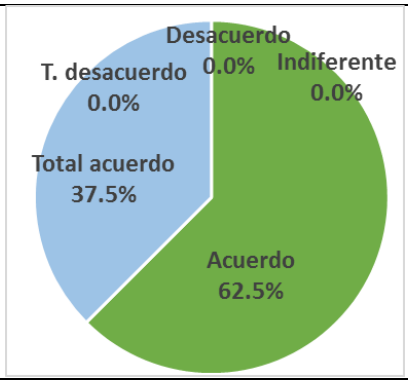
PT02 ¿Con que frecuencia recibe capacitación sobre el valor de la información y los datos de la empresa?

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	4	50%
De acuerdo	3	37.5%
En total acuerdo	1	12.5%



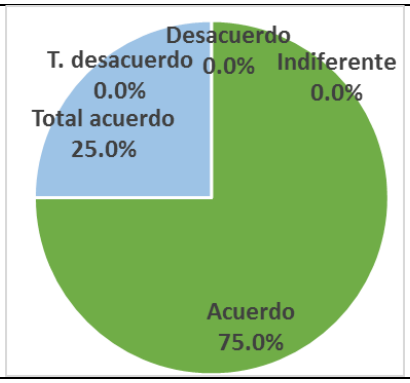
PT03 En el desarrollo de su trabajo, aplica metodologías asociadas a la seguridad de la información, por ejemplo aplica copias de seguridad, usa cadenas de custodia, copias en la nube, o cualquier otro mecanismo de protección de datos.

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	5	62.5%
En total acuerdo	3	37.5%



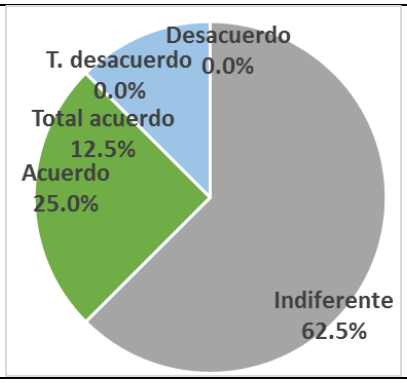
PT04 ¿Qué tanta importancia da a los procedimientos de control de cambios, a solicitud de nuevos requerimientos de parte de los clientes externos o internos?

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	0	0%
De acuerdo	6	75%
En total acuerdo	2	25%



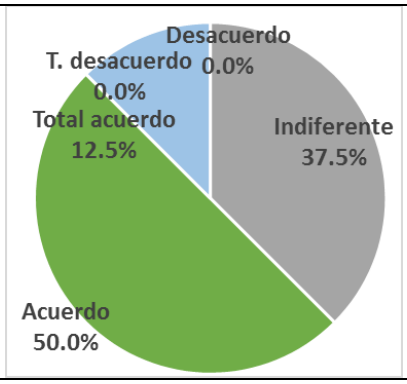
PT05 Lleva un control de los errores o actividades que ponen en riesgo la seguridad de la información o datos en el trabajo que realiza.

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	5	62.5%
De acuerdo	2	25.0%
En total acuerdo	1	12.5%



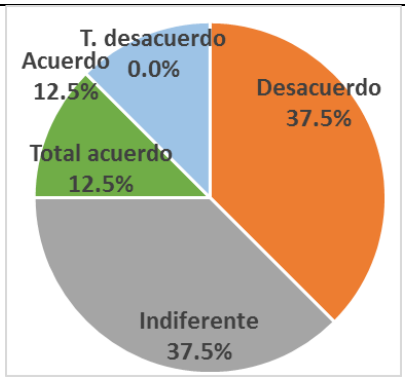
PT06 Utiliza un sistema de gestión o sigue buenas prácticas de seguridad de la información en el trabajo que realiza.

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	3	37.5%
De acuerdo	4	50.0%
En total acuerdo	1	12.5%



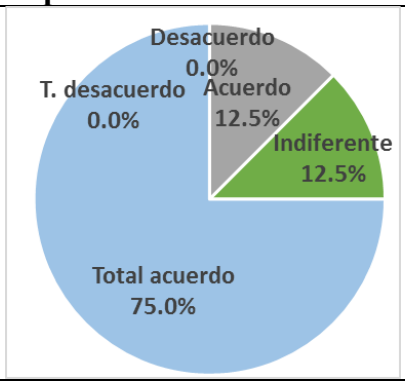
PT07 Considera burocrático u obstruccionista realizar la documentación detallada o reportar a sus superiores sobre diversas ocurrencias de eventos de riesgos de la información y datos de la empresa y los clientes

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	3	37.5%
Indiferente	3	37.5%
De acuerdo	1	12.5%
En total acuerdo	1	12.5%



PT08 El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información le permite reducir la probabilidad o el impacto de incidentes futuros.

Respuesta	Encuestados	Porcentaje
En total desacuerdo	0	0%
En desacuerdo	0	0%
Indiferente	1	12.5%
De acuerdo	1	12.5%
En total acuerdo	6	75%



Anexo 04: Armonización de estándares de gestión de seguridad de la información

	ISO/IEC 27001:2013	ISO/IEC 27004:2016	ISO/IEC 27005:2018	ISO/IEC 31000:2018	MAGERIT V3.0
Propósito del estándar o metodología	**Tecnologías de la información – Técnicas de seguridad – sistema de gestión de la seguridad de la información - requerimientos**	**Tecnologías de la información – Técnicas de seguridad – sistema de gestión de la seguridad de la información – Análisis y Evaluación**	**Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo de la seguridad de la información**	**Directrices para la gestión de riesgos**	**Metodología de análisis y gestión de los sistemas de la información**
Principio	**Objetivo:** Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.	**Objetivo:** Proporcionar pautas destinadas a ayudar a organizaciones a evaluar el rendimiento de la seguridad de la información y la eficiencia de un sistema de gestión con el fin de cumplir los requisitos de la norma ISO/IEC 27001	Objetivo: Suministrar las directrices para gestionar los riesgos que puede sufrir la información de una empresa, principalmente se apoya en el ISO/IEC 27001, centrándose principalmente en los requisitos de seguridad de la información.	Objetivo: Gestionar el riesgo a través de la creación y protección del valor en base a los siguientes principios Integridad, estructurada y exhaustiva, adaptada, incluida, dinámica, mejor información disponible, factores humanos y culturales, mejora continua	Objetivos; 1) Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarla. 2) Ofrecer un método sistemático para analizar los riesgos derivados del uso de las Tecnologías de la Información. 3) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
Proceso de gestión de la seguridad de la información y riesgos	**Contexto de la organización** Se busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información. Adicional a esto, se debe determinar el alcance. Entendiendo la organización y su contexto Entendiendo las necesidades y expectativas de los implicados	El monitoreo y medición del rendimiento de la seguridad de la información. El monitoreo y medición de la efectividad de un Sistema de Gestión de la Seguridad de la Información, incluidos procesos y controles. Análisis y evaluación de los resultados de monitorización y medición.	**Establece el contexto:** **Alcance y límites:** - La organización debe delimitar el alcance del sistema de gestión de riesgos de la seguridad de la información - El alcance necesita definirse para asegurar que todos los activos relevantes de la organización son tomados en cuenta para la evaluación del riesgo. - Los límites necesitan identificarse para abordar aquellos riesgos que surjan dentro del alcance. Establecimiento de contexto:	**Definición del alcance** La organización debería definir el alcance de las actividades ligadas a la gestión del riesgo **Contexto interno y externo** La organización debería establecer el contexto interno y externo. Los contextos hacen referencia a los entornos en que la organización busca definir y lograr sus objetivos	Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. 1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. 2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará

	ISO/IEC 27001:2013	ISO/IEC 27004:2016	ISO/IEC 27005:2018	ISO/IEC 31000:2018	MAGERIT V3.0
	Determinando el campo de aplicación del SGSI Sistema de gestión de la seguridad de la información		Requiere que se establezca el contexto externo e interno para la gestión del riesgo de la seguridad de la información **Criterios:** ✓ Enfoque de gestión de riesgo ✓ Criterio de evaluación de riesgo ✓ Criterio de impacto ✓ Criterio de aceptación de riesgo. Organización para la gestión del riesgo de la seguridad de la información Se requiere que se establezcan la organización y las responsabilidades para el proceso de gestión de riesgos de seguridad de la información.	**Definición de los criterios asociados al riesgo** La organización debería precisar los riesgos que tendrá en cuenta en relación a los objetivos de la gestión de riesgos La organización define los criterios para valorar la importancia del riesgo y para apoyar los procesos de control.	mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad
Proceso de la valoración de los activos			El orden de los activos puede hacerse de dos maneras: • A través del valor de reposición del activo. • A través de las consecuencias para el negocio. » La valoración de los activos y su clasificación por la criticidad • El incidente puede afectar a más de un activo, debido a la interdependencia de los activos. » Las consecuencias se pueden expresar en términos de criterios financieros, técnicos, humanos, del impacto en los negocios, entre otros criterios.		Contiene un catálogo que permite definir: **Tipos de activos**, sabiendo que aparecerán nuevos tipos de activos continuamente. Dimensiones de valoración, sabiendo que en casos específicos pueden aparecer dimensiones específicas; pero en la certidumbre de estar recogido lo esencial. **Criterios de valoración**, con un fuerte componente de estimación por los expertos; El ánimo es relativizar el valor de los diferentes activos en sus diferentes dimensiones de valoración.

	ISO/IEC 27001:2013	ISO/IEC 27004:2016	ISO/IEC 27005:2018	ISO/IEC 31000:2018	MAGERIT V3.0
			» Preparación de la lista de consecuencias evaluadas referentes a un escenario de incidente, en relación a los activos y criterios de impacto		**Amenazas**, sabiendo que no todas las amenazas son significativas sobre todos los sistemas; pero con una razonable esperanza de que este catálogo crezca lentamente. **Salvaguardas**, se tratan con un enfoque de "identificación de necesidades" por parte de los responsables de los sistemas de información, mientras que se tratan con un enfoque de "controles de eficacia y eficiencia" por los auditores de sistemas.
Proceso de valoración y evaluación del riesgo	Examinar sistemáticamente los riesgos de seguridad de la información de la organización, teniendo en cuenta las amenazas, vulnerabilidades e impactos; Diseñar e implementar un conjunto coherente e integral de controles de seguridad de la información y / u otras formas de tratamiento de riesgos (como evitar riesgos o transferir riesgos) para abordar los riesgos que se consideran inaceptables	Con el fin de medir y evaluar la eficacia de la seguridad de la información, se siguen las siguientes etapas: Elegir los objetivos y procesos de medición. Describir las líneas principales. Elegir los datos. Desarrollo del sistema de medición. Interpretar los valores medidos. Notificar dichos valores.	**Valoración de riesgo** **Identificación del riesgo** - Identificación de los activos. - Identificación de las amenazas. - Identificación de los controles existentes - Identificación de las vulnerabilidades - Identificación de las consecuencias. **Análisis del riesgo** Metodologías de análisis de riesgo Evaluación de las consecuencias Evaluación de la probabilidad de incidentes	**Identificación del riesgo** El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que puedan ayudar o impedir lograr los objetivos de una organización **Análisis de riesgos** El propósito del análisis de riesgo es comprender la naturaleza del riesgo y sus características, incluyendo si fuera necesario el nivel del riesgo. Las técnicas de análisis de pueden ser cualitativas, cuantitativas o una combinación. **Valoración del riesgo**	**Análisis de riesgos** Caracterización de los activos: basado en los activos relevantes para la organización, su interrelación, y su valor. Caracterización de las amenazas, determinar a qué amenazas están expuestos los activos motivo de análisis. Caracterización de las salvaguardas, que salvaguardas están dispuestas y cuán eficientes son frente a los riesgos. Estimación del estado del riesgo a través de la estimación del impacto sobre los activos.

	ISO/IEC 27001:2013	ISO/IEC 27004:2016	ISO/IEC 27005:2018	ISO/IEC 31000:2018	MAGERIT V3.0
			Determinación del nivel de riesgo. **Evaluación del riesgo** El nivel de los riesgos debe ser comparado con los criterios de evaluación de riesgo y la aceptación del riesgo.	Valora el riesgo para apoyar la toma de decisiones	
Proceso de tratamiento del riesgo			**Tratamiento del riesgo** Modificación del riesgo Retención del riesgo Evasión del riesgo Compartición del riesgo	**Selección de las opciones para el tratamiento del riesgo** La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales derivados del logro de los objetivos asociados al costo, esfuerzo o desventajas de la implementación. **Preparación para la implementación de los planes de tratamiento de los riesgos** El propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementan las opciones elegidas para el tratamiento.	**Gestión del riesgo** Identificación de proyectos de seguridad de la información Planificación de los proyectos de seguridad de la información. Ejecución del plan de seguridad de la información.

	ISO/IEC 27001:2013	ISO/IEC 27004:2016	ISO/IEC 27005:2018	ISO/IEC 31000:2018	MAGERIT V3.0
Proceso de comunicación	Se debe contemplar un plan de comunicación. Quien debe comunicar los aspectos de seguridad. A quienes debe llegar la comunicación. Cuál es el contenido. En qué momento ha de realizarse la comunicación. Que medios utilizaremos.	Se recomienda que el comunicador de la información determine cómo comunicar los resulta-dos de la medición de la seguridad de la información, Se recomienda que los resultados de las mediciones se comuniquen a una variedad de partes interesadas internas incluyendo, como mínimo. La organización puede requerir en algunos casos distribuir informes de resultados de mediciones a partes externas, incluyendo autoridades reguladoras, accionistas, clientes y proveedores. Se recomienda que los informes de los resultados de las mediciones que se distribuyan externamente, contengan sólo datos que sean apropiados para ser entregados externamente, y que sean aprobados por la alta dirección y por las partes interesadas correspondientes antes de su entrega.	Proceso de comunicación y consulta del riesgo de seguridad de la información. Comunicación y consulta del riesgo de seguridad de la información.	**Propósito de asistir a las partes pertinentes a comprender el riesgo.** La comunicación busca promover la toma de conciencia. La consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.	

	ISO/IEC 27001:2013	ISO/IEC 27004:2016	ISO/IEC 27005:2018	ISO/IEC 31000:2018	MAGERIT V3.0
Proceso de seguimiento y revisión	**Evaluación de desempeño** Se debe realizar un seguimiento, una medición, un análisis, una evaluación, una auditoría interna y una revisión por parte de la dirección del sistema de gestión de la información, para asegurar su correcto funcionamiento. Supervisión, medida, análisis y evaluación Auditorías internas Revisiones de la gestión Mejora: Habla sobre el tratamiento de las no conformidades, las acciones correctivas y a mejora continua. Disconformidades y acciones correctivas	Información de seguridad Seguimiento de Riesgos y Revisión. Los riesgos y sus factores (valoración de activos, impactos, amenazas, vulnerabilidades y probabilidad de ocurrencias) deben ser monitoreados y revisados para identificar cualquier cambio en el contexto de la organización en una etapa temprana. Monitorear y revisar los factores de riesgos. Monitorear la gestión, revisión y mejora del Sistema Gestión de Seguridad de la Información.	El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados de procesos de evaluación de riesgo.	Se debe revisar la ejecución del plan de seguridad de la información.	

Fuente: Elaboración propia

Anexo 4.B Aportes de estándares y metodologías a modelo de gestión de seguridad de la información

MODELO PROPUESTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y APORTES DE LOS ESTÁNDARES Y METODOLOGÍA DE ANÁLISIS		
Fases	**Actividades**	**Estándar o metodología utilizada**
FASE I: Alcance y contexto de la gestión de la seguridad de la información Objetivo: Definir alcance de la gestión de la seguridad de la información	1.1 Comprender a la empresa y su actividad comercial	**ISO/IEC 27001:2013** Sección 4.1: Entiende a la organización, describe la consideraciones a tener en cuenta para comprender a la empresa u organización.
	1.2 Captura las necesidades y expectativas de las partes interesadas	**ISO/IEC 27001:2013** Sección 4.2: Entiende las necesidades de la organización, describe la consideraciones a tener en cuenta para comprender las necesidades de la empresa u organización.
	1.3 Define la visión, misión, objetivos y metas de la gestión de la seguridad de la información	**ISO/IEC 27001:2013** Sección 4.3: Determina el alcance del sistema de gestión de la seguridad de la información.
	1.4 Establece el contexto interno y externo Análisis FODA Contexto interno Estructura organizacional Capacidades Procesos del servicio de modelado Contexto Externo Contexto normativo y regulatorio Relación con los clientes Alianzas estratégicas Contexto económico Contexto tecnológico Contexto socio-cultural	**ISO/IEC 27001:2013** Sección 4.1: Entiende a la organización y su contexto describe la consideraciones a tener en cuenta para comprender a la empresa u organización dé la empresa u organización, en el contexto interno y externo en que desarrolla sus actividades comerciales.

MODELO PROPUESTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y APORTES DE LOS ESTÁNDARES Y METODOLOGÍA DE ANÁLISIS		
Fases	**Actividades**	**Estándar o metodología utilizada**
	Relación con proveedores	
FASE II: Análisis de activos Objetivo: Identificar y valor los activos asociados a la seguridad de la información asociada al servicio.	2.1 Análisis de activos	MAGERIT V3.0 Libro II: Catalogo de elemento Sección 2: Tipos de activos, determina a la información y los servicios como elementos esenciales para la gestión de la seguridad de la información
	2.2 Identificación de dependencias	MAGERIT V3.0 Libro II: Catalogo de elemento Sección 2.1, 2.2, 2.3, 2.5, 2.6, 2.7, 2.9, 2.10, 2.12: Categorías de activos
	2.3 Valorización de activos (D, I, C)	MAGERIT V3.0 Libro II: Catalogo de elemento Sección 3: Dimensiones de valoración y Sección 4: criterios de valoración
FASE III: Análisis de riesgos Objetivo: identificar y valore las amenazas asociadas a la información asociada al servicio	3.1 Identificación de amenazas	MAGERIT V3.0 Libro II: Catalogo de elemento Sección 5: Amenazas, se toma como base el catálogo de amenazas descrito en la sección 5 de MAGERIT.
	3.2 Valorización de la probabilidad de ocurrencia	V MAGERIT V3.0 Libro II: Catalogo de elemento Sección 5: Amenazas, se toma como base el catálogo de amenazas descrito en la sección 5 de MAGERIT.
	3.3 Valorización del impacto del riesgo	ISO 31000:2018 Sección 6.4.2: identificación del riesgo, encontrar, reconocer y describir los riesgos que ayuden o impidan el logro de la gestión de la información. Sección 6.4.4: Valoración del riesgo.
	3.4 Evaluación del riesgo R = P x I x V	ISO/IEC 27005:2018 Sección 8: Evaluación de seguridad de la información. ISO/IEC 31000:2018 Sección 6: Proceso de análisis de riesgo

MODELO PROPUESTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y APORTES DE LOS ESTÁNDARES Y METODOLOGÍA DE ANÁLISIS		
Fases	**Actividades**	**Estándar o metodología utilizada**
	3.5 Genera informe de impacto información sobre servicios de modelado	SO/IEC 27004:2016 Sección 10.2: identificación del criterio de evaluación de medición de la seguridad de la información.
FASE IV: Tratamiento de riesgos Objetivo: Proponer planes de tratamiento de seguridad de la información	4.1 Tratamiento de riesgos	ISO/IEC 31000:2018 Sección 6.5: Tratamiento de riesgo, opciones de tratamiento de riesgos.
	4.2 Plan de tratamiento de riesgo	ISO/IEC 27005:2018 Sección 6.5: Tratamiento de riesgo, opciones de tratamiento de riesgos.
FASE V: Comunicación Objetivo: proponer estrategias de comunicación	5.1 Comunicación	ISO/IEC 27005:2018 Sección 11. Comunicación y consulta de gestión de la seguridad de la información. Describe la importancia del intercambio de información con quienes toman decisiones otras partes interesadas.
	5.2 Consulta	
FASE VI: Seguimiento y revisión Objetivo: Monitorear los planes de tratamiento propuestos	6.1 Seguimiento y revisión	ISO/IEC 27004:2016 Sección 10.3. Seguimiento, control, revisión y evaluación de la medición de la seguridad de la información.
	6.2 Cumplimiento de planes de tratamiento propuestos	

Fuente: Elaboración propia

Anexo 05: Formatos de instrumentos a aplicar en el modelo propuesto

Anexo 5.1 Formato para identificación de activos

De acuerdo a Magerit v3 y la ISO/IEC 27001:2013 los activos se definen como aquel recurso tecnológico de una empresa que contribuye a agilizar la gestión, y se utilizan para el cumplimiento de los objetivos de la actividad comercial de la empresa, la Tabla 13 se muestra la definición de los tipos de activos para la gestión de información en la empresa.

Tabla 13: Catálogo para identificación de activos de modelado numérico

Código	Tipo	Descripción	Activos asociados
[D]	Datos / Información	Activo que puede estar almacenado en equipos o soportes de información y que puede ser transferido de un lugar a otro por medios de transmisión de datos	Bases de datos Códigos fuentes Datos de configuración Copias de respaldo Información de cotizaciones Informes y/o reportes digitales Información de clientes Documentos personalizados para desarrollar servicios Licencias y permisos
[S]	Servicios	Se refiere a funciones prestadas por sistemas informáticos que satisfacen las necesidades de los usuarios del servicio	*Acceso a software* de d*esarrollo* Acceso a actualización web Acceso a plataforma Cloud AWS Acceso a correo electrónico Acceso a BD Acceso a modelos numérico Reporte contable Soporte de TI
[SW]	*Software*	*Se refiere a los activos que gestionan, analizan y transforman los datos en información o datos de procesados, permitiendo la explotación de la información para la prestación de los servicios*	*IDE de programación* Modelos Numéricos Visualizadores gráficos Sistema de equipos de medición ambiental

Código	Tipo	Descripción	Activos asociados
			Sistemas de Información Geográfica Kit informático (Word, Excel, Power Point) Página web de la empresa Base de datos Sistema operativo
[H]	*Hardware*	*Se refiere a los medios físicos que almacenan, procesan o transmiten los datos, soportan la ejecución de las aplicaciones informáticas y soportan los servicios prestados a los usuarios*	*Computadoras* Laptops Soporte de red (switches, routers, firewalls) Equipos digitales de medición ambiental (sonómetro, radiómetro) Impresoras
[COM]	*Redes de comunicación*	*Se refiere a los medios que transmiten datos*	*Internet* Red local Wifi
[Media]	*Soportes de información*	*Se refiere a los dispositivos físicos que almacenan información por lagos periodos de tiempo o permanentemente*	*Disco externos* Documentos impresos (reportes, manuales, guías, informes de estudios, técnicas) Memorias USB
[Aux]	*Equipos auxiliares*	*Se refiere a los equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos*	*Fuentes de alimentación de corriente* Equipo de ventilación Gabinetes Mobiliarios
[P]	*Personal*	*Se refiere a las personas que interactúan con los sistemas de información*	*Desarrollador de aplicativos* Modelador numérico Asistentes de desarrollo Soporte informático y TI Atención al cliente Clientes

En el caso de los servicios de modelados, se considera a los recursos humanos (de acuerdo a su conocimiento y nivel de especialización) como el elemento fundamental para el desarrollo de la actividad comercial, seguido de los recursos tecnologías (hardware y software) y en una tercera instancia tenemos a la información (datos históricos e informes técnicos).

Tabla 14: Formato para identificación de activos

Formato 01:		**IDENTIFICACIÓN DE ACTIVOS**			
Clasificación: Especifica la categoría a la que pertenece el activo (Hardware, Software, datos, servicios,…)					
Elaborado por:		Consigne el nombre de la persona encargada del registro de la información		**Fecha**	Indique la fecha en que se recoge la información
Ítem	**Código**	**Nombre**	**Descripción**		**Responsable**
1	Consigna código del activo	Nombre del activo	Describa el activo de forma que se pueda diferenciar entre otros activos, evitar generalidades.		Consignar el nombre de la persona o área responsable del activo
2					
3					
…					

Fuente: Elaboración propia, adaptado de MAGERIT V3.0

Anexo 5.2 Escala de valoración de activos

La empresa debe asignar un valor a los activos de información que pueden ser afectados por la presencia de amenazas. Para la valoración de activos se tendrán en cuenta las siguientes dimensiones:

Disponibilidad (D): es el acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (ISO 27000). Principalmente se define en función de afectación en horas de trabajo de indisponibilidad de la información, ver Tabla 15.

Integridad (I): mantenimiento de la exactitud y completitud de la información. (ISO 27000). Principalmente se define en función al grado de recuperación de la información en caso de ser afectada, ver Tabla 16.

Confidencialidad (C): la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (ISO 27000). Principalmente se define en función del nivel de interacción entre los recursos humanos de la empresa a nivel interno y externo. Ver Tabla 17.

:

Tabla 15: Escala de valoración de activos de acuerdo a la disponibilidad

VALOR	ESCALA	DISPONIBILIDAD (D)
1= Bajo	Menor a 6 horas	La inaccesibilidad o indisposición a la información hasta ¼ día en las actividades asociadas al uso de la información en la empresa. Considerando un tiempo (24/7).
2 = Medio	De 6 a 24 horas	La inaccesibilidad o indisposición a la información, de ¼ a 1 día de actividades asociadas al uso de la información en la empresa.
3 = Alto	De 24 a 72 horas	La inaccesibilidad o indisposición a la información de 1 a 3 días de actividades asociadas al uso de la información en la empresa.
4 = Muy alto	Mayor a 72 horas	La inaccesibilidad o indisposición a la información por más de 3 días de las actividades asociadas al uso de la información en la empresa.

Fuente: Elaboración propia

Tabla 16: Escala de valoración de activos de acuerdo a la integridad

VALOR	ESCALA	INTEGRIDAD (I)
1= Bajo	Integro	La información no fue modificada o la modificación no fue autorizada, pero mantiene la integridad y no pone en cuestionamiento el uso de la información. Podrías representar una unidad de medida equivalente, o porque se encuentran fuera de límites.
2 = Medio	Recuperable	La modificación no autorizada puede repararse aunque podría ocasionar un perjuicio de la empresa en cuanto tiempo (debido a la revisión de etapas anteriores donde se utilizó la información).
3 = Alto	Alterado	La modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo a la empresa, teniendo que hacer de conocimiento a terceros (solicitantes del servicio).
4 = Muy alto	Perdido	La modificación no autorizada no podría repararse bajo ninguna forma, tanto a nivel de la empresa o terceros.

Fuente: Elaboración propia

Tabla 17: Escala de valoración de activos de acuerdo a la confiabilidad

VALOR	ESCALA	CONFIDENCIALIDAD (C)
1= Bajo	Publico	La información es conocida y/o utilizada sin autorización por cualquier persona, dentro y fuera de la empresa sin causar perjuicio a la empresa
2 = Medio	Limitado	La información es utilizada y de conocimiento de un número reducido de personal interno de la empresa, y de personal externo a la empresa (solicitante del servicio), mayormente se asocia a la información que se maneja durante la interacción de la empresa y los clientes.
3 = Alto	Reservado	La información es utilizada y de conocimiento de un número de personas reducido dentro de la empresa, mayormente asociada a la nivel de administrativo y desarrollo (gerencia y administración, gerencia y personal de desarrollo),
4 = Muy alto	Privado	La información es utilizada y de conocimiento de un número de personas bastante reducido dentro de la empresa, mayormente asociada a nivel de gestión (gerencia, gerencia y administración),

Fuente: Elaboración propia

Tabla 18: Valoración del nivel de criticidad de los activos

Rango (resultado de sumatoria de los criterios de disponibilidad, integridad y confidencialidad)	Nivel de criticidad
Entre 1 a 3	Bajo
Entre 4 a 8	Medio
Entre 9 a 12	Alto

Fuente: Elaboración propia

Anexo 5.3: Formato para valoración de activos

Tabla 19: Valoración de los activos

Activos				**Criterios**			**Total**	**Nivel de criticidad**
Ítem	**Clasificación**	**Código**	**Nombre**	**Disponibilidad**	**Integridad**	**Confidencialidad**		
1	Nombre de la clasificación del activo	Código de la asignación al activo	Nombre del activo	Puntuación de acuerdo a la escala del anexo 5.2			Sumatoria de las puntuaciones	Nivel de criticidad de acuerdo a la Tabla 18
2								
3								
…								

Fuente: Elaboración propia

Anexo 5.4; Formato para la identificación de amenazas de activos

Tabla 20: Formato para identificación de amenazas sobre activos

Activos			Amenazas/Vulnerabilidad
ítem	**Clasificación código**	**Nombre**	
1	Clasificación y código del activo	Consigna el nombre del activo.	Describa la amenaza/vulnerabilidad que podría afectar al activo.
2			
3			
…			

Fuente: Elaboración propia

Para la identificación se basa principalmente en la análisis de las amenazas y vulnerabilidades de seguridad de la información a las estarían expuestos los procesos de negocio, y por ende los activos de TI que se relacionan a cada uno de los procesos de negocios. La identificación de las amenazas y vulnerabilidades se basará en la metodología MAGERIT (Libro II, punto 5, "Catálogo de Elementos"), enfocándonos principalmente en las amenazas de origen industrial, errores y fallo no intencionados, y ataque intencionado, los mismos que se detallan a continuación:

Amenazas de origen industrial [I]: hace referencia a los sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada, entre las cuales destacan:

[I.1] Fuego

[I.2] Daños por agua

[I.3] Desastres industriales.

[I.4] Contaminación electromagnética.

[I.5] Avería de origen físico o lógico.

[I.6] Corte de suministro eléctrico.

[I.7] Condiciones inadecuadas de temperatura o humedad

[I.8] Fallo de servicios de comunicaciones.

[I.9] Interrupción de otros servicios y suministros esenciales

[I.10] Degradación de los soportes de almacenamiento de la información.

[I.11] Emanaciones electromagnéticas

Amenazas de origen de errores y fallos no intencionados [E]: hace referencia a fallos no intencionales causados por las personas, entre las cuales destacas:

[E.1] Errores de los usuarios

[E.2] Errores del administrador

[E.3] Errores de monitorización

[E.4] Errores de configuración

[E.8] Difusión de SW dañino

[E.9] Errores de [re]-encaminamiento

[E.10] Errores de secuencia

[E.15] Alteración accidental de la información

[E.18] Destrucción de la información

[E.19] Fugas de información

[E.20] Vulnerabilidades de los programas (SW)

[E.21] Errores de mantenimiento / actualización de programas (SW)

[E.23] Errores de mantenimiento / actualización de equipos (HW)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Pérdida de equipos

[E.26] Indisponibilidad del personal

Amenazas de origen de ataques intencionados [A]: hace referencia a fallos deliberados causados por las personas, entre los cuales destacan:

[A.3]Manipulación de los registros de actividad (log)

[A.4]Manipulación de la configuración

[A.5]Suplantación de la identidad del usuario

[A.6]Abuso de privilegios de acceso

[A.7]Uso no previsto

[A.8]Difusión de software dañino

[A.9] [Re-] encaminamiento de mensajes

[A.10]Alteración de secuencia

[A.11]Acceso no autorizado

[A.12]Análisis de tráfico

[A.13]Repudio

[A.14]Interceptación de información (escucha)

[A.15]Modificación deliberada de la información

[A.18]Destrucción de información

[A.19]Divulgación de información

[A.22]Manipulación de programas

[A.23]Manipulación de los equipos

[A.24]Denegación de servicio

[A.25]Robo

[A.26] Ataque destructivo

[A.27] Ocupación enemiga

[A.28] Indisponibilidad del personal

[A.29] Extorsión

[A.30] Ingeniería social

Anexo 5.5: Identificación y valoración del riesgo

La identificación del riesgo, se realiza sobre cada activo y se evalúa a través de la valoración de la probabilidad y el impacto de las amenazas y vulnerabilidades del riesgo de la Tabla 21.

Tabla 21: Valoración de probabilidad de ocurrencia de riesgo durante la GSI_GR

Valor	Probabilidad	Descripción del evento
1	Mínima	No debería suceder o volver a suceder
2	Significativa	Podría suceder o volver a suceder
3	Alta	Podría ocurrir o volver a ocurrir a corto o mediano plazo.
4	Máxima	Podría ocurrir o volver a ocurrir en algún momento (a largo plazo).

Fuente: Elaboración propia

Tabla 22: Valoración del impacto de riesgo durante la GSI

Escala	Impacto	Descripción
1	Insignificante	No altera la ejecución, ni el rendimiento de las actividades de la empresa. Los impactos son superables sin ninguna dificultad*****.
2	Limitado	Altera la ejecución y rendimiento de las actividades de la empresa. Los impactos serían superados con algunas dificultades.
3	Importante	Altera la ejecución y rendimiento de las actividades de la empresa. Los impactos serían superados con graves dificultades.
4	Critico	Altera la ejecución y rendimiento de las actividades de la empresa. Los impactos no serían superados.

Fuente: Elaboración propia

Se utiliza la valoración de la magnitud del riesgo como el producto de la probabilidad por el impacto, en una escala de 1 a 16.

Riesgo = Probabilidad x Impacto

Tabla 23: Escala de riesgo

VALOR	MAGNITUD
1 – 4	Baja
5 – 8	Media
9 – 12	Alta
13 – 16	Critica

Fuente: Elaboración propia

Evaluación del riesgo

En esta actividad se procede a ubicar los valores asigandos de impacto y probabilidad de riesgo en el mapa de calor.

Tabla 24: Mapa de calor para diagnóstico de la probabilidad e impacto del riesgo

PROBABILIDAD	4 Máximo	4	8	12	16
	3 Alto	3	6	9	12
	2 Significativo	2	4	6	8
	1 Mínimo	1	2	3	4
		1 Insignificante	2 Limitado	3 Importante	4 Critico
		IMPACTO			

Fuente: Elaboración propia

Fase IV: Tratamiento de riesgo

En esta etapa se deben proponer planes de tratamiento de riesgos, los cuales deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas.

La información proporcionada en el plan del tratamiento debería incluir:

- ✓ El alcance de la propuesta, los objetivos, los beneficios esperados;
- ✓ Las personas o área involucradas
- ✓ Responsables de la implementación

- ✓ Las acciones propuestas;
- ✓ Los recursos necesarios, incluyendo las contingencias;
- ✓ Las medidas de evaluación de desempeño;
- ✓ Las restricciones;
- ✓ La frecuencia de reportes o informes y seguimiento requeridos;
- ✓ El costo y plazo previsto para la realización.

Fase V: Comunicación

La empresa u organización debe determinar la necesidad de comunicaciones internas y externas relevantes al sistema de SGI incluyendo:

- ✓ Qué comunicar,
- ✓ Cuándo comunicar,
- ✓ A quién comunicar;
- ✓ Quién debe comunicar; y
- ✓ Los procesos por los cuales la comunicación debe ser efectuada.

Fase VI: Seguimiento y revisión

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

El seguimiento y la revisión deberían tener lugar en todas etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

Los resultados del seguimiento y la revisión deberían incorporarse a todas las actividades de la gestión de la seguridad de la información.

Registro e informe

El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:

- Comunicar las actividades de la gestión del riesgo y sus resultados a lo miembros de la empresa.
- Proporcionar información para la toma de decisiones;
- Mejorar las actividades de la gestión del riesgo;
- Asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

Las decisiones con respecto a la creación, conservación y tratamiento de la información documentada deberían tener en cuenta, pero no limitarse a su uso, la sensibilidad de la información y los contextos externo e interno.

El informe es una parte integral de la gobernanza de la empresa y debería mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección. Los factores a considerar en el informe incluyen, pero no se limitan a:

- Las diferentes partes interesadas, sus necesidades y requisitos específicos de información;
- La pertinencia de la información con respecto a los objetivos de la empresa y la toma de decisiones.

Mejora continua

La empresa debe mejorar continuamente la conveniencia y efectividad del Sistema de Gestión de Seguridad de la Información, por lo que se sugiere realizar una autoevaluación semestral de los incidentes sucedidos y amenazas materializadas en cuanto a seguridad de la información en el área de modelado numérico.

Anexo 6: Ficha de juicio de expertos

Experto 01: Dr. Gilberto Carrión Barco

USAT Universidad Católica Santo Toribio de Mogrovejo

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	14 de agosto del 2020
Nombres y apellidos	GILBERTO CARRIÓN BARCO
Formación académica	**Profesión**: Ingeniero en Computación e Informática **Grado académico**: Doctor en Ciencias de la Computación y Sistemas
Áreas de experiencia profesional:	- Infraestructura tecnológica - Transformación digital - Seguridad de la información
Tiempo de experiencia	Más de 15 años
Cargo actual	Docente Universitario
Institución / Empresa	Universidad Nacional Pedro Ruíz Gallo
Objetivo de la investigación	Proponer un modelo de gestión de seguridad de la información con enfoque de riesgos para apoyar en los servicios de modelado numérico ambiental.
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.
Objetivo de la prueba	Determinar la utilidad del modelo propuesto.

Firma del experto

USAT
Universidad Católica
Santo Toribio de Mogrovejo

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	**1.** No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	**1.** No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA: El ítem tiene relación lógica con	**1.** No cumple con el criterio	El ítem no tiene relación lógica con la dimensión

CATEGORÍA	CALIFICACIÓN	INDICADOR
la dimensión o indicador que está midiendo.	**2.** Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	**1.** No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE I Contexto de la empresa y alcance de la gestión de la seguridad de la información	Comprender a la empresa y su actividad comercial	4	4	4	4	
	Captura las necesidades y expectativas de las partes interesadas	4	4	4	4	
	Define el alcance de la gestión de la seguridad de la información	4	4	4	4	
	Establece el contexto interno y externo	4	4	4	4	
FASE II Análisis de activos	Identificación de procesos de negocio asociados al servicio de modelado numérico	4	4	4	4	
	Identificación de activos	4	4	4	4	
	Valorización de activos (D, I, C)	4	4	4	4	

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

FASE III Análisis de riesgos	Identificación de amenazas y vulnerabilidades por procesos de servicios	4	4	4	4	
	Valorización de la probabilidad de ocurrencia	4	4	4	4	
	Valorización del impacto del riesgo	4	4	4	4	
	Evaluación del riesgo = Probabilidad x Impacto	4	4	4	4	
	Genera informe de impacto de información sobre servicios de modelado	4	4	4	4	
FASE IV Tratamiento de riesgos	Tratamiento de riesgos	4	4	4	4	
	Plan de tratamiento de riesgo	4	4	4	4	
FASE V Comunicación	Comunicación	4	4	4	4	
	Consulta	4	4	4	4	

USAT
Universidad Católica
Santo Toribio de Mogrovejo

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

FASE VI Seguimiento y revisión	Seguimiento y revisión	4	4	4	4	
	Cumplimiento de planes de tratamiento propuestos	4	4	4	4	
Caso de estudio	Implementación parcial de modelo de Gestión de Seguridad de la Información	3	3	3	3	Se evidencia una discusión a la FASE I. Lo recomendable es hacer una crítica a todas las FASES
Aporte de riesgo	Que tanta importancia tiene el riesgo en el modelo propuesto	4	4	4	4	Todo servicio de TI debe contemplar riesgos. En este caso se ha realizado un buen análisis para la empresa seleccionada.
					ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)	ACEPTADO

EL "MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE DE RIESGOS PARA APOYAR EN LOS SERVICIOS DE MODELADO NÚMERICO AMBIENTAL" CONTEMPLA LAS FASES Y ACTIVIDADES APROPIADAS PARA SER CONSIDERADAS VALIDAS, POR LO TANTO, APTOS PARA ALCANZAR LOS OBJETIVOS QUE SE PLANTEAN EN LA INVESTIGACIÓN.

Firma del experto

Experto 02: Dra. Jessie Bravo Jaico

USAT
Universidad Católica
Santo Toribio de Mogrovejo

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	18 de agosto del 2020
Nombres y apellidos	Jessie Leila Bravo Jaico
Formación académica	**Profesión**: Ingeniero en computación y sistemas **Grado académico**: Dra. En ciencias de la computación y sistemas
Áreas de experiencia profesional:	- Gestión de la seguridad de la información de TI - Gestión de riesgos de TI
Tiempo de experiencia	- Gestión de TI: Más de 20 años - Gestión de riesgo de TI: Más de 5 años
Cargo actual	Docente
Institución / Empresa	Universidad Nacional Pedro Ruiz Gallo
Objetivo de la investigación	Proponer un modelo de gestión de seguridad de la información con enfoque de riesgos para apoyar en los servicios de modelado numérico ambiental.
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.
Objetivo de la prueba	Determinar la utilidad del modelo propuesto.

Firma del experto

USAT
Universidad Católica
Santo Toribio de Mogrovejo

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada

CATEGORÍA	CALIFICACIÓN	INDICADOR
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE I Contexto de la empresa y alcance de la gestión de la seguridad de la información	Comprender a la empresa y su actividad comercial	4	4	4	4	
	Captura las necesidades y expectativas de las partes interesadas	4	4	4	4	
	Define el alcance de la gestión de la seguridad de la información	3	4	4	4	Analizar la posibilidad del trabajo remoto como alternativa y debería ser parte del alcance.
	Establece el contexto interno y externo	4	4	4	4	
FASE II Análisis de activos	Identificación de procesos de negocio asociados al servicio de modelado numérico	4	4	4	4	
	Identificación de activos	4	4	4	4	
	Valorización de activos (D, I, C)	4	4	4	4	

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

FASE III Análisis de riesgos	Identificación de amenazas y vulnerabilidades por procesos de servicios	4	4	4	3	Se debería analizar la posibilidad de incluir la situación actual de la pandemia como una amenaza
	Valorización de la probabilidad de ocurrencia	4	4	4	4	
	Valorización del impacto del riesgo	4	4	4	4	
	Evaluación del riesgo = Probabilidad x Impacto	4	4	4	4	
	Genera informe de impacto de información sobre servicios de modelado	4	4	4	4	
FASE IV Tratamiento de riesgos	Tratamiento de riesgos	4	4	4	4	
	Plan de tratamiento de riesgo	4	4	4	4	
FASE V Comunicación	Comunicación	4	4	4	4	
	Consulta	4	4	4	4	

FASE VI Seguimiento y revisión	Seguimiento y revisión	**4**	**4**	**4**	**4**	
	Cumplimiento de planes de tratamiento propuestos	**4**	**4**	**4**	**4**	
Caso de estudio	Implementación parcial de modelo de Gestión de Seguridad de la Información	**4**	**4**	**4**	**4**	
Aporte de riesgo	Que tanta importancia tiene el riesgo en el modelo propuesto	**4**	**4**	**4**	**4**	
				ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)		**Aceptado**

Firma del experto

Experto 03: Dr. Oliver Vásquez Leyva

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	17 de agosto del 2020
Nombres y apellidos	Oliver Vásquez Leyva
Formación académica	**Profesión**: Ingeniero de Sistemas Doctor en Ciencias de la Computación y Sistemas
Áreas de experiencia profesional:	Gestión de la seguridad de la información de TI
Tiempo de experiencia	- Más de 15 años
Cargo actual	Gerente
Institución / Empresa	SOLTI.SAC
Objetivo de la investigación	Proponer un modelo de gestión de seguridad de la información con enfoque de riesgos para apoyar en los servicios de modelado numérico ambiental.
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.
Objetivo de la prueba	Determinar la utilidad del modelo propuesto.

Firma del experto

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	**1.** No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	**1.** No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada

CATEGORÍA	CALIFICACIÓN	INDICADOR
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	**1.** No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	**1.** No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE I Contexto de la empresa y alcance de la gestión de la seguridad de la información	Comprender a la empresa y su actividad comercial	**4**	**4**	**3**	**3**	Aún no se establece la relevancia del riesgo real o potencial para justificar la gestión de los activos.
	Captura las necesidades y expectativas de las partes interesadas	**4**	**4**	**4**	**4**	
	Define el alcance de la gestión de la seguridad de la información	**4**	**4**	**3**	**3**	
	Establece el contexto interno y externo	**4**	**4**	**4**	**4**	
FASE II Análisis de activos	Identificación de procesos de negocio asociados al servicio de modelado numérico	**4**	**4**	**4**	**4**	
	Identificación de activos	**4**	**4**	**4**	**4**	
	Valorización de activos (D, I, C)	**4**	**4**	**3**	**3**	

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

FASE III Análisis de riesgos	Identificación de amenazas y vulnerabilidades por procesos de servicios	**4**	**4**	**4**	**3**	
	Valorización de la probabilidad de ocurrencia	**4**	**4**	**4**	**4**	
	Valorización del impacto del riesgo	**4**	**4**	**4**	**4**	
	Evaluación del riesgo = Probabilidad x Impacto	**4**	**4**	**4**	**4**	
	Genera informe de impacto de información sobre servicios de modelado	**4**	**4**	**4**	**4**	
FASE IV Tratamiento de riesgos	Tratamiento de riesgos	**4**	**4**	**4**	**4**	
	Plan de tratamiento de riesgo	**4**	**4**	**4**	**4**	
FASE V Comunicación	Comunicación	**4**	**4**	**4**	**4**	
	Consulta	**4**	**4**	**4**	**4**	

FASE VI Seguimiento y revisión	Seguimiento y revisión	**4**	**4**	**4**	**4**	
	Cumplimiento de planes de tratamiento propuestos	**4**	**4**	**4**	**4**	
Caso de estudio	Implementación parcial de modelo de Gestión de Seguridad de la Información	**4**	**4**	**4**	**4**	
Aporte de riesgo	Que tanta importancia tiene el riesgo en el modelo propuesto	**4**	**4**	**3**	**3**	
					ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)	**Aceptado**

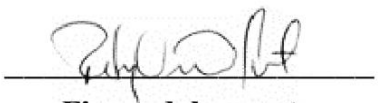
Firma del experto

Experto 04: MSc. Ruby Viviana Ortiz Martínez

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	21 de agosto del 2020
Nombres y apellidos	Ruby Viviana Ortiz Martínez
Formación académica	**Profesión**: Ingeniera de sistemas **Grado académico**: Magister en Dirección estratégica de tecnologías de información
Áreas de experiencia profesional:	Gestión de datos e información
Tiempo de experiencia	Más de 15 años de experiencia profesional
Cargo actual	Coordinadora técnica del Centro Colombiano de Datos Oceanográficos (Cecoldo)
Institución / Empresa	Dirección General Marítima (Dimar)
Objetivo de la investigación	Proponer un modelo de gestión de seguridad de la información con enfoque de riesgos para apoyar en los servicios de modelado numérico ambiental.
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.
Objetivo de la prueba	Determinar la utilidad del modelo propuesto.



Firma del experto

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	**1.** No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	**1.** No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA: El ítem tiene relación lógica	**1.** No cumple con el criterio	El ítem no tiene relación lógica con la dimensión

CATEGORÍA	CALIFICACIÓN	INDICADOR
con la dimensión o indicador que está midiendo.	**2.** Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	**1.** No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE I Contexto de la empresa y alcance de la gestión de la seguridad de la información	Comprender a la empresa y su actividad comercial	**4**	**4**	**4**	**4**	
	Captura las necesidades y expectativas de las partes interesadas	**4**	**4**	**4**	**4**	
	Define el alcance de la gestión de la seguridad de la información	**4**	**4**	**4**	**2**	Desde el punto de vista metodológico, es de considerar que esta actividad hace referencia al resultado esperado de la fase I. Es decir, el análisis y discusión de las demás actividades debería permitir definir el "alcance de la gestión de la seguridad de la información".
	Establece el contexto interno y externo	**3**	**4**	**4**	**4**	El análisis del contexto externo se puede mejorar. Debería poder entrever la oportunidad de negocio, de manera que muestre el retorno de la inversión económica en la que tendría que incurrir la empresa, para implementar la gestión de riesgos de seguridad de la información.

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE II Análisis de activos	Identificación de procesos de negocio asociados al servicio de modelado numérico	**4**	**4**	**4**	**4**	
	Identificación de activos	**4**	**4**	**4**	**4**	
	Valorización de activos (D, I, C)	**4**	**4**	**4**	**4**	
FASE III Análisis de riesgos	Identificación de amenazas y vulnerabilidades por procesos de servicios	**4**	**4**	**4**	**4**	
	Valorización de la probabilidad de ocurrencia	**4**	**4**	**4**	**4**	
	Valorización del impacto del riesgo	**4**	**4**	**4**	**4**	
	Evaluación del riesgo = Probabilidad x Impacto	**4**	**4**	**4**	**4**	
	Genera informe de impacto de información sobre servicios de modelado	**4**	**3**	**4**	**4**	Se recomienda incluir al final una discusión sobre los resultados. para dar mayor claridad sobre los hallazgos y los posibles motivos.

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE IV Tratamiento de riesgos	Tratamiento de riesgos	**4**	**3**	**4**	**4**	Se recomienda mejorar la conexión de la fase anterior con esta, es decir, debe ser claro cómo los resultados de la fase anterior conducen a formular los proyectos propuestos.
	Plan de tratamiento de riesgo	**3**	**4**	**4**	**4**	Si bien se nombran los proyectos propuestos, sería bueno que de acuerdo a las limitaciones de la empresa, explicar cuál de ellos sería prioritario, o si podrían abordarse en el corto o mediano plazo y qué proceso tendría el reto de hacerlo.
FASE V Comunicación	Comunicación	**3**	**4**	**4**	**4**	Se recomienda mejorar la estrategia de comunicación, respondiendo a las preguntas planteadas.
	Consulta	**3**	**4**	**4**	**4**	
FASE VI Seguimiento y revisión	Seguimiento y revisión	**4**	**4**	**4**	**4**	
	Cumplimiento de planes de tratamiento propuestos	**4**	**4**	**4**	**4**	

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Caso de estudio	Implementación parcial de modelo de Gestión de Seguridad de la Información	**4**	**4**	**4**	**4**	
Aporte de riesgo	Que tanta importancia tiene el riesgo en el modelo propuesto	**4**	**4**	**4**	**4**	
					ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)	**Aceptado**

Firma del experto

Experto 05: Dr. Jorge Tam Malaga

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	14 de agosto del 2020
Nombres y apellidos	Jorge Tam Málaga
Formación académica	**Profesión**: Biólogo **Grado académico**: Doctor en Oceanografía
Áreas de experiencia profesional:	- Ecología marina, modelado ecosistémico
Tiempo de experiencia	- Más de 20 años
Cargo actual	Responsable del Laboratorio de Modelado Oceanográfico, Ecosistémico y del Cambio Climático
Institución / Empresa	Instituto del Mar del Perú
Objetivo de la investigación	Proponer un modelo de gestión de seguridad de la información con enfoque de riesgos para apoyar en los servicios de modelado numérico ambiental.
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.
Objetivo de la prueba	Determinar la utilidad del modelo propuesto.

Firma del experto

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	**1.** No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	**1.** No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada

CATEGORÍA	CALIFICACIÓN	INDICADOR
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	**1.** No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	**1.** No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE I Contexto de la empresa y alcance de la gestión de la seguridad de la información	Comprender a la empresa y su actividad comercial	4	4	4	4	
	Captura las necesidades y expectativas de las partes interesadas	4	4	4	4	
	Define el alcance de la gestión de la seguridad de la información	4	4	4	4	
	Establece el contexto interno y externo	3	4	4	3	
FASE II Análisis de activos	Identificación de procesos de negocio asociados al servicio de modelado numérico	4	4	4	4	
	Identificación de activos	4	4	4	4	
	Valorización de activos (D, I, C)	4	4	4	4	

FASE III Análisis de riesgos	Identificación de amenazas y vulnerabilidades por procesos de servicios	4	4	4	4	
	Valorización de la probabilidad de ocurrencia	3	4	4	4	
	Valorización del impacto del riesgo	4	4	4	4	
	Evaluación del riesgo = Probabilidad x Impacto	4	4	4	4	
	Genera informe de impacto de información sobre servicios de modelado	4	4	4	4	
FASE IV Tratamiento de riesgos	Tratamiento de riesgos	3	2	3	3	Especificar o dar alternativas de tratamiento de riesgos
	Plan de tratamiento de riesgo	2	3	3	3	
FASE V Comunicación	Comunicación	2	3	3	3	Especificar o dar alternativas de comunicación de riesgos
	Consulta	3	2	3	3	

FASE VI Seguimiento y revisión	Seguimiento y revisión	3	4	4	4	Especificar responsables y frecuencia
	Cumplimiento de planes de tratamiento propuestos	4	4	4	4	
Caso de estudio	Implementación parcial de modelo de Gestión de Seguridad de la Información	3	4	4	4	
Aporte de riesgo	Que tanta importancia tiene el riesgo en el modelo propuesto	4	4	4	4	
				ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)		Aceptado

Firma del experto

Experto 06: Dr. Adolfo Chamarro Gómez

Maestría en Ingeniería de Sistemas y Computación
Mención en Dirección Estratégica de TI

INFORMACIÓN DEL PROFESIONAL QUE VALIDA A TRAVÉS DE JUICIO DE EXPERTO EL MODELO PROPUESTO

Fecha	18 de agosto del 2020
Nombres y apellidos	Adolfo Vicente Chamorro Gómez
Formación académica	**Profesión**: Físico **Grado académico**: Doctor en Ciencias Ambientales
Áreas de experiencia profesional:	- Interacción oceano-atmósfera, modelado atmosférico
Tiempo de experiencia	- Más de 8 años
Cargo actual	Investigador Científico del Laboratorio de Modelado Oceanográfico Ecosistémico y del Cambio Climático
Institución / Empresa	Instituto del Mar del Perú
Objetivo de la investigación	Proponer un modelo de gestión de seguridad de la información con enfoque de riesgos para apoyar en los servicios de modelado numérico ambiental.
Objetivo del juicio de expertos	Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de las actividades que comprende.
Objetivo de la prueba	Determinar la utilidad del modelo propuesto.

Firma del experto

CRITERIOS DE CALIFICACIÓN A TENER EN CUENTA

De acuerdo a los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	**1.** No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	**1.** No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.

CATEGORÍA	CALIFICACIÓN	INDICADOR
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	**1.** No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	**1.** No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

CUESTIONARIO PARA VALIDACIÓN A TRAVÉS DE JUICIO DE EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
FASE I Contexto de la empresa y alcance de la gestión de la seguridad de la información	Comprender a la empresa y su actividad comercial	**4**	**4**	**4**	**4**	
	Captura las necesidades y expectativas de las partes interesadas	**3**	**4**	**4**	**4**	- Incluir las necesidades de los trabajadores
	Define el alcance de la gestión de la seguridad de la información	**4**	**4**	**4**	**4**	
	Establece el contexto interno y externo	**4**	**4**	**4**	**4**	
FASE II Análisis de activos	Identificación de procesos de negocio asociados al servicio de modelado numérico	**4**	**4**	**4**	**4**	
	Identificación de activos	**4**	**4**	**4**	**4**	

	Valorización de activos (D, I, C)	4	4	4	4	
FASE III Análisis de riesgos	Identificación de amenazas y vulnerabilidades por procesos de servicios	**3**	**4**	**4**	**4**	- Incluir la importancia del respaldo de la información (backup)
	Valorización de la probabilidad de ocurrencia	**4**	**4**	**4**	**4**	
	Valorización del impacto del riesgo	**4**	**4**	**4**	**4**	
	Evaluación del riesgo = Probabilidad x Impacto	**4**	**4**	**4**	**4**	
	Genera informe de impacto de información sobre servicios de modelado	**4**	**4**	**4**	**4**	
FASE IV Tratamiento de riesgos	Tratamiento de riesgos	**2**	**3**	**3**	**3**	- Señalar las personas o áreas involucradas, responsables de la implementación, acciones propuestas, etc, en cada uno de los proyectos planteados
	Plan de tratamiento de riesgo	**2**	**3**	**3**	**3**	

FASE V Comunicación	Comunicación	**3**	**3**	**3**	**3**	- Indicar por cada proyecto que se comunicará, cuando, a quien, etc.
	Consulta	**2**	**3**	**3**	**3**	
FASE VI Seguimiento y revisión	Seguimiento y revisión	**3**	**3**	**3**	**3**	- Indicar cuales serían los mecanimos apropiados
	Cumplimiento de planes de tratamiento propuestos	**3**	**3**	**3**	**3**	
Caso de estudio	Implementación parcial de modelo de Gestión de Seguridad de la Información	**3**	**3**	**3**	**3**	
Aporte de riesgo	Que tanta importancia tiene el riesgo en el modelo propuesto	**3**	**3**	**3**	**3**	
				ESTADO DE MODELO PROPUESTO: (Aceptado/Observado/Disconforme)		**Aceptado**

Firma del experto