ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA DE SISTEMAS

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CENTROS DE INVESTIGACIÓN, DIAGNÓSTICO Y PREVENCIÓN DE DESASTRES NATURALES, APLICADO A UN CASO DE ESTUDIO, BASADO EN BUENAS PRÁCTICAS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAESTRÍA DE GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

SANTIAGO DANIEL ARRAIS DIAZ

santiago_arrais@hotmail.com

DIRECTOR: ING. JHONATTAN BARRIGA MSC.

jhonattan.barriga@epn.edu.ec

Quito, Enero 2016

DECLARACIÓN

Yo, Santiago Daniel Arrais Díaz, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Santiago Daniel Arrais Díaz

C E R T IF IC A C IÓ N

Certifico que el presente trabajo fue desarrollado por el Ing. Santiago Daniel Arrais Díaz bajo mi supervisión.

Ing. Jhonattan Barriga, M Sc.

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Mis agradecimientos, más sentidos a:

A mi Director de Tesis Ing. Jhonattan Barriga, MSc., por sus sabios consejos y apoyo en el desarrollo del presente proyecto.

A todos quienes conforman el Instituto Geofísico, por los conocimientos y experiencia adquirida en la ardua labor y cumplimiento de las metas propuestas

Ing. Santiago Arrais

DEDICATORIA

Dedico este proyecto de titulación a mi familia por su respaldo, comprensión y motivación para lograr este objetivo.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Los centros de investigación, diagnóstico y prevención de desastres naturales en el Ecuador son entidades en donde se generan datos continuos, que son almacenados, procesados, su información es transferida a entidades de toma de decisión local, estatal, regional, medios de difusión y comunidades de investigación mundial. La problemática se hace evidente en el ámbito de seguridad de la información, en donde los esfuerzos por aplicar técnicas y métodos en seguridad de la información no son suficientes, lo que conlleva a tener sistemas de información vulnerables a amenazas por ello, se debe establecer un modelo que integre normas y metodologías aplicadas por comunidades sismológicas internacionales y contribuir al tratamiento de la información y mejoramiento en sus operaciones.

El presente estudio plantea la identificación conjunta de normas de seguridad de la información de la Serie ISO/IEC 27000 y metodologías de gestión de riesgos Magerit, NIST SP 800, Octave, Coras, para desarrollar un modelo de gestión de seguridad de la información orientado a estos centros de investigación. La estructura del modelo propuesto contempla procesos de gestión enmarcados en el mejoramiento continuo del modelo, que van desde la preparación del entorno, establecimiento de objetivos, análisis y gestión de riesgos, selección y aplicación de controles, tratamiento del riesgo, operación del sistema de gestión de seguridad y evaluación de la funcionalidad del modelo propuesto.

Los resultados obtenidos de la aplicación del modelo en dos procesos centrales de un caso de estudio han sido la identificación de todos los elementos del sistema de información, se efectuó las etapas de: Preparación, Establecimiento del modelo SGSI e Identificación de riesgos. Respecto a las etapas de Gestión de riesgos, Componentes de gestión de gestión de seguridad y Operación del SGSI que dependen de la revisión y aprobación de la alta dirección, se realizó el planteamiento de lineamientos en caso la institución decida continuar hacia la implementación del modelo propuesto.

PRESENTACIÓN

El presente documento contiene la propuesta de un modelo de gestión de seguridad de la información, apoyado en normas de la serie ISO 27000 y metodologías de gestión de riesgos, aplicado a centros de investigación de desastres naturales en el Ecuador.

El Capítulo 1 presenta la situación actual de los centros de investigación de desastres naturales en el Ecuador frente a las medidas de seguridad en sus sistemas de información; sustenta la similitud de los centros de investigación en el manejo de los datos e información comprobando que no existe un modelo de gestión de seguridad de la información adecuado. Se define objetivos y necesidades de seguridad de la información, caracterización y dimensionamiento en un Caso de Estudio.

El capítulo 2 muestra la normativa legal vigente en el Ecuador en el área de seguridad de la información. Se realiza un estudio exploratorio de metodologías de gestión de riesgos, normas ISO 27001 e ISO 27005, con ello se define el Alcance y Límites del modelo de gestión de seguridad. Se realiza el diseño y estructuración del modelo SGSI conformando seis etapas: 1) Fase de Preparación, 2) Establecimiento del Modelo de Gestión de Seguridad de la Información, 3) Identificación de los riesgos, 4) Metodología de gestión de riesgos, 5) Componentes de gestión de seguridad de la información de los centros de investigación, 6) Operación del SGSI.

El Capítulo 3 contiene las etapas desarrolladas para el modelo SGSI e implementadas en dos procesos de Gestión de datos sísmicos y volcánicos y Gestión del acceso a la información relacionada al monitoreo sísmico y volcánico, con lo cual se valida el diseño del SGSI propuesto.

El Capítulo 4, contempla las conclusiones y recomendaciones del presente estudio, refleja los resultados obtenidos durante la aplicación del modelo propuesto al caso de estudio; así como, la labor a futuro para estandarizar el SGSI o aplicarlo como referente en estos centros de investigación.

CAPÍTULO 1. SISTEMATIZACIÓN DEL PROBLEMA

1.1. Problemática de la Seguridad de Información relacionada con la Investigación de Desastres Naturales.

Los datos e información generados en los centros de investigación, diagnóstico y prevención de desastres naturales en el Ecuador como el Instituto Geofísico IG de la Escuela Politécnica Nacional, Instituto Oceanográfico de la Armada del Ecuador INOCAR e Instituto Nacional de Meteorología e Hidrología INAMHI, implican volúmenes importantes de almacenamiento en el orden de los Terabytes al año que deben perdurar en el tiempo; por ello, se requiere de equipos especializados y sistemas tolerables a fallos para almacenamiento, procesamiento, respaldos y transferencia de la información a entidades de toma de decisión local, estatal y regional, así también a otros medios de difusión y comunidades internacionales de investigación. Esta transferencia incrementa la vulnerabilidad de la información al presentar diferentes niveles de acceso y niveles de control hacia las redes de información de domino público, dominio privado y estratégico interconectados de manera permanente a redes públicas que ahora son blanco de ataque de virus, malware, troyanos, phishing entre otros.

Los medios para la adquisición de datos basados en varios tipos de redes de estaciones de monitoreo y sistemas en tiempo real han implicado inversiones muy altas. La valía e importancia de los datos sísmicos, volcánicos, oceanográficos y meteorológicos radica en que “contienen” la información que permitirá un mejor entendimiento de la realidad sísmica, volcánica, meteorológica y tectónica-oceánica del país. Estos son datos que no pueden perderse, y la integridad de la información debe estar disponible ya que siempre habrán nuevas investigaciones que realizar con ellos. De la misma manera los sistemas de tiempo real permiten brindar información oportuna a las autoridades y comunidad sobre los fenómenos monitoreados, por tanto,

el almacenamiento de los datos y la información generada deben ser tratados dentro de un marco estandarizado, sostenible y rápido en distintos niveles de acceso.

Los servicios en la nube [3], [27], [28] y centros de datos [2] pueden brindar seguridad en la información pero pueden ser muy costosos por el volumen de datos, la recuperación de datos puede involucrar tiempos muy altos, cadenas de intermediarios, dependencia hacia el proveedor de servicios de cloud computing, problemas en la migración de servicios y en el desarrollo de aplicaciones para procesamiento y análisis de datos; por lo que es imprescindible contar con equipo a nivel de país, formar parte de comunidades sismológicas internacionales y mantener un sistema adecuado de la seguridad de la información.

Los centros de investigación de desastres naturales deben proteger los sistemas de información de la organización bajo los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad [4] manteniendo el riesgo bajo el nivel asumible por la propia organización, mediante un modelo de gestión de seguridad de la información que se ajuste a estándares internacionales utilizados por redes mundiales dedicadas a la prevención de desastres naturales y contribuir al intercambio de información y cooperación internacional.

A continuación se realiza una breve revisión exploratoria de la estructura organizacional de estos centros de investigación para comprender sus funciones y aspectos relacionados a la gestión de la información.

1.1.1. Descripción organizacional de los Centros de Investigación, diagnóstico y prevención de desastres naturales en el Ecuador:

Las instituciones encargadas de la investigación, diagnóstico y prevención de desastres naturales en el Ecuador han fomentado la seguridad individual y colectiva frente a los riesgos provocados por fenómenos naturales; a través del conocimiento de las amenazas sísmicas, volcánicas, de hidrometeorología y oceanográficas,

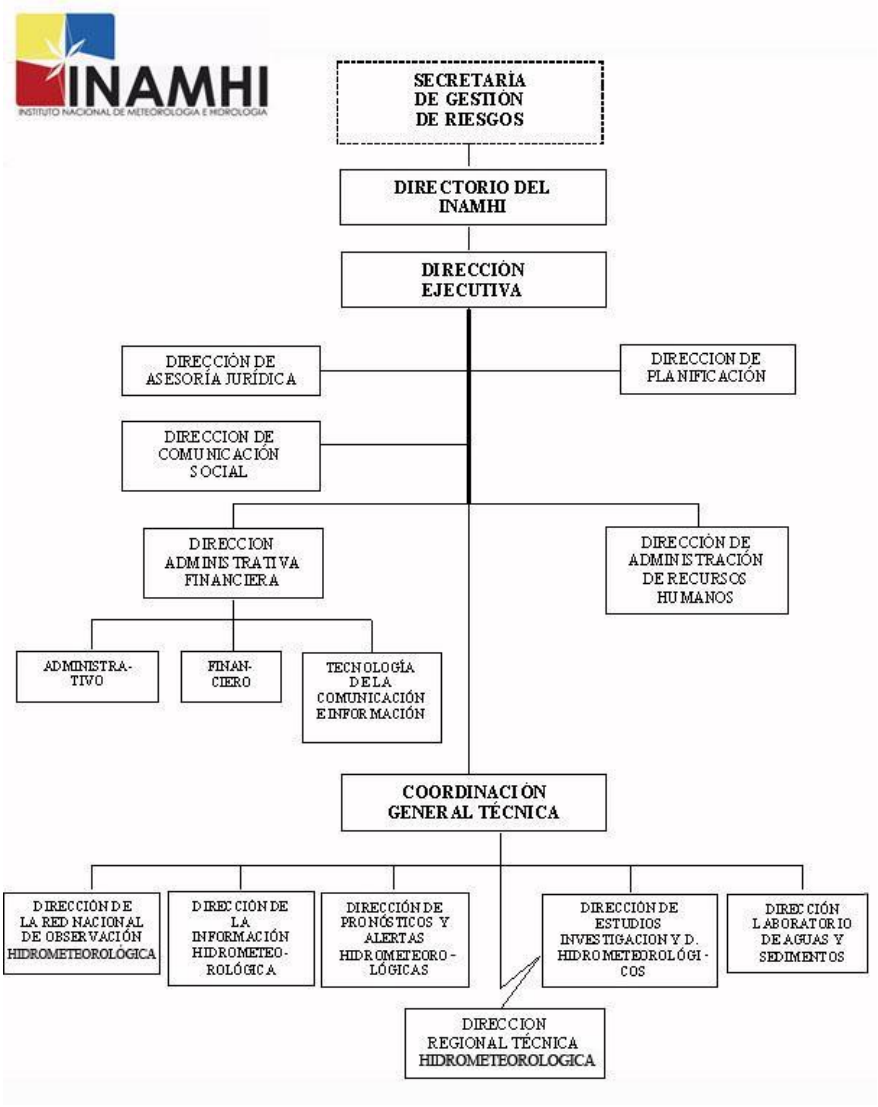
mediante el monitoreo continuo y la investigación científica, contribuyendo a la creación de una cultura de prevención y al desarrollo sostenible y sustentable del país [10]. A continuación se presenta un resumen de las funciones que realizan estas entidades públicas y la estructura organizacional con el objetivo de determinar el rol de las unidades de TI e identificar sus procesos en el campo de gestión de seguridad de la información.

1.1.1.1. Instituto Nacional de Meteorología e Hidrología – INAMHI:

Es una institución que proporciona información relacionada al comportamiento de la atmósfera y las aguas interiores, cambios del clima y los recursos hídricos en el tiempo, a través del monitoreo, investigación y tecnología necesarios para la formulación y evaluación de los planes de desarrollo, emisión alertas tempranas que contribuyan a la protección de la vida humana, del medio ambiente, de los bienes materiales y por ende al desarrollo económico y social del país. Es parte de la Organización Meteorológica Mundial, OMM para el intercambio de información de hidrometeorología con otros países, sobre el tiempo, el clima, los recursos hídricos, de acuerdo a las normas aplicadas a nivel internacional. Mantiene el monitoreo de la red nacional de estaciones meteorológicas e hidrológicas: recopila, estudia, procesa, publica, y difunde la información de hidrometeorología a través de los medios de comunicación, (prensa, radio, televisión, correo electrónico, entrevistas) y organismos públicos y privados.

Actualmente el INAMHI en su plan estratégico presenta cuatro ejes, de acuerdo con la página web de la institución [11], donde se puede evidenciar la necesidad y el compromiso de mejorar la Gestión de TI, establecer normativas para el uso de la información, fortalecer la confiabilidad de sus datos repotenciando el sistema nacional de información hidrometeorológica y climática del Ecuador, así como el trabajo conjunto con otros organismos del Estado para elevar su nivel científico y técnico.

Figura 1.1 Orgánico funcional INAMHI



Fuente: INAMHI, [46].

En la Figura 1.1 se identifica a nivel funcional que la unidad TI encargada de la gestión de seguridad de la información debe mejorar su estructura y relacionarse directamente a las unidades de tratamiento de datos y gestión de la información.

1.1.1.2. Instituto Oceanográfico de la Armada del Ecuador INOCAR:

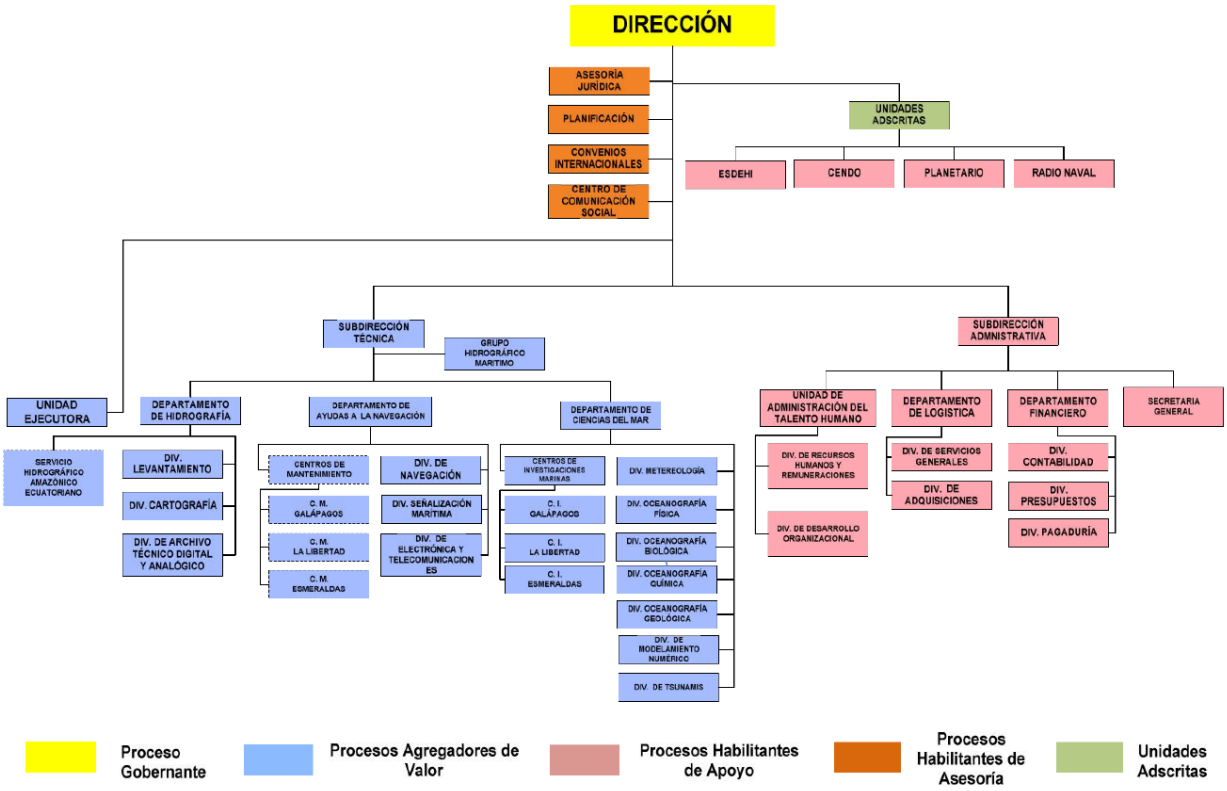
Es un organismo encargado de la investigación y seguridad marítima en el Ecuador, gestiona las actividades técnicas y administrativas relacionadas con el Servicio de Hidrografía, Navegación, Oceanografía, Meteorología, Ciencias del Mar, Señalización Náutica y realiza estudios a nivel científico para colaborar con instituciones nacionales y extranjeras en la protección al medio ambiente marino, la investigación de los recursos minerales y exploración de petróleo costa fuera. Para alcanzar los objetivos propuestos se ha implementado diversos sistemas de monitoreo, levantamiento de información, observación y alerta temprana, a través de equipos y herramientas tecnológicas que han permitido la construcción de un sistema robusto de geoinformación y generación de productos operacionales sobre el estado del mar en tiempo real. Entre estas tecnologías se destacan: La incorporación de sonares multihaz para levantamiento de data hidrográfica, perfilador sísmico, sonares de barrido lateral, piston core, robots submarinos, Sistemas de teledetección oceanográfica y atmosférica e implementación de modelos numéricos de predicción.

Los resultados obtenidos han sido: la elaboración de cartas náuticas del área marítima nacional, investigaciones oceanográficas de los procesos de interacción océano-atmósfera en el Pacífico Ecuatorial-Oriental para determinar el impacto en los recursos vivos, clima, productividad biológica, fenómenos que afectan los puertos y terminales de la zona costera. Finalmente, las expediciones a la Antártica con lo cual la Armada del Ecuador atiende los intereses nacionales en el Continente blanco [5].

El INOCAR al ser una entidad parte de la Fuerza Naval [6], [7], las directrices relacionadas a seguridad de la información son dispuestas por el COGMAR (Comandancia General de la Marina), en donde se encuentra la DIRTIC (Dirección de TICs) [8], que es la unidad encargada de la gestión y operación de los sistemas de información. Se puede evidenciar que existen políticas de seguridad de la información orientadas a la administración de la red y servicios de TI, con personal responsable de verificar el cumplimiento de las normas y procedimientos establecidos. Sin embargo, se pudo evidenciar que en los centros tecnológicos de la información existentes dentro

de la Fuerza Naval, el INOCAR aplica procedimientos relacionados a la gestión de seguridad de la información parcialmente, para la monitorización y tratamiento de datos relacionados a Hidrografía, Navegación, Oceanografía y Meteorología, que son los procesos agregadores de valor como se indica en la Figura 1.2 que se indica a continuación:

Figura 1.2 Organigrama Estructural - INOCAR



Fuente: INOCAR, [47].

De acuerdo a la página web de la institución [5], [6], [47] respecto a la Base Legal, regulaciones y procedimientos internos aplicables a la entidad INOCAR se puede evidenciar que las siguientes, no son normativas relacionadas a la seguridad de la información:

- Normas de creación: Ley de Creación del Instituto Oceanográfico de la Armada, Decreto Nº 940
- Normas de regulación: Leyes convexas, Código Civil, Decreto Nº 959, Ley de faros y boyas, Registro Oficial 235 - Hora Oficial
- Matriz de normatividad

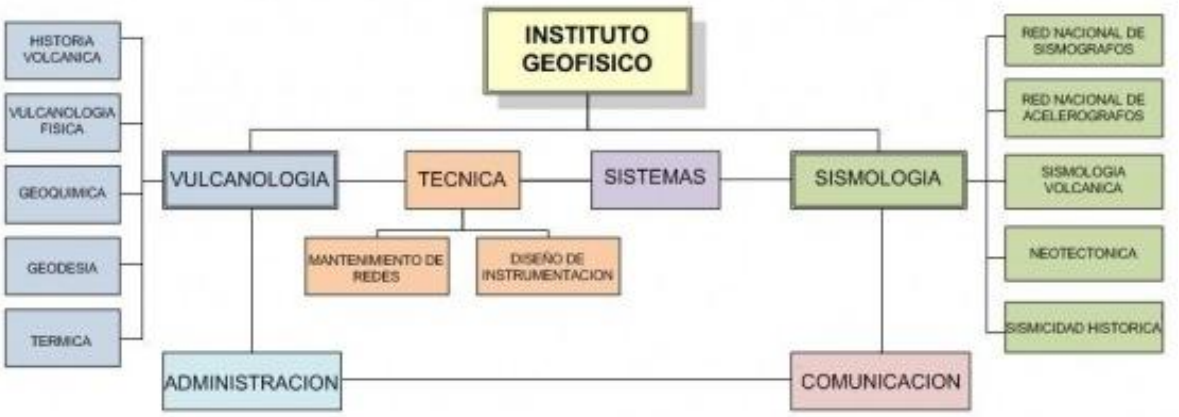
El INOCAR inició en el año 2015 el proyecto de implementación del esquema de gubernamental de seguridad de la información EGSI en la herramienta GPR (Gobierno por resultados) [35], que promueve la SNAP (Secretaría de Administración Pública), en donde se ha planteado como objetivo incrementar a nivel administrativo la eficiencia, operatividad, calidad, capacidad en los departamentos y unidades del INOCAR.

1.1.1.3. Instituto Geofísico IG-EPN:

Es una organización encargada de la investigación científica y monitoreo instrumental permanente de los fenómenos sísmicos y volcánicos, contribuyendo a través del conocimiento de amenazas sísmicas y volcánicas a la reducción de su impacto negativo en el Ecuador [10]. Así también, a la generación continua de publicaciones y artículos técnicos, formación académica de alto nivel, desarrollo y aplicación tecnológica con el fin de asegurar la óptima adquisición y archivo de datos e información necesaria para el monitoreo sistemático y evaluación de los fenómenos; promoviendo la creación de una cultura de prevención y mejoramiento de la seguridad individual y colectiva. Su participación activa con asociaciones científicas ha fortalecido sus alianzas a nivel nacional e internacional a través de Proyectos de investigación que aportan a una efectiva reducción del riesgo.

En la Figura 1.3, se identifica que el área de Sistemas es donde se concentran los procesos de seguridad de la información y está relacionada directamente a las áreas de Vulcanología, Sismología y Técnica involucradas en el transporte de datos, adquisición, procesamiento, análisis e interpretación y comunicación.

Figura 1.3 Organigrama Instituto Geofísico EPN



Fuente: IG-EPN, [48].

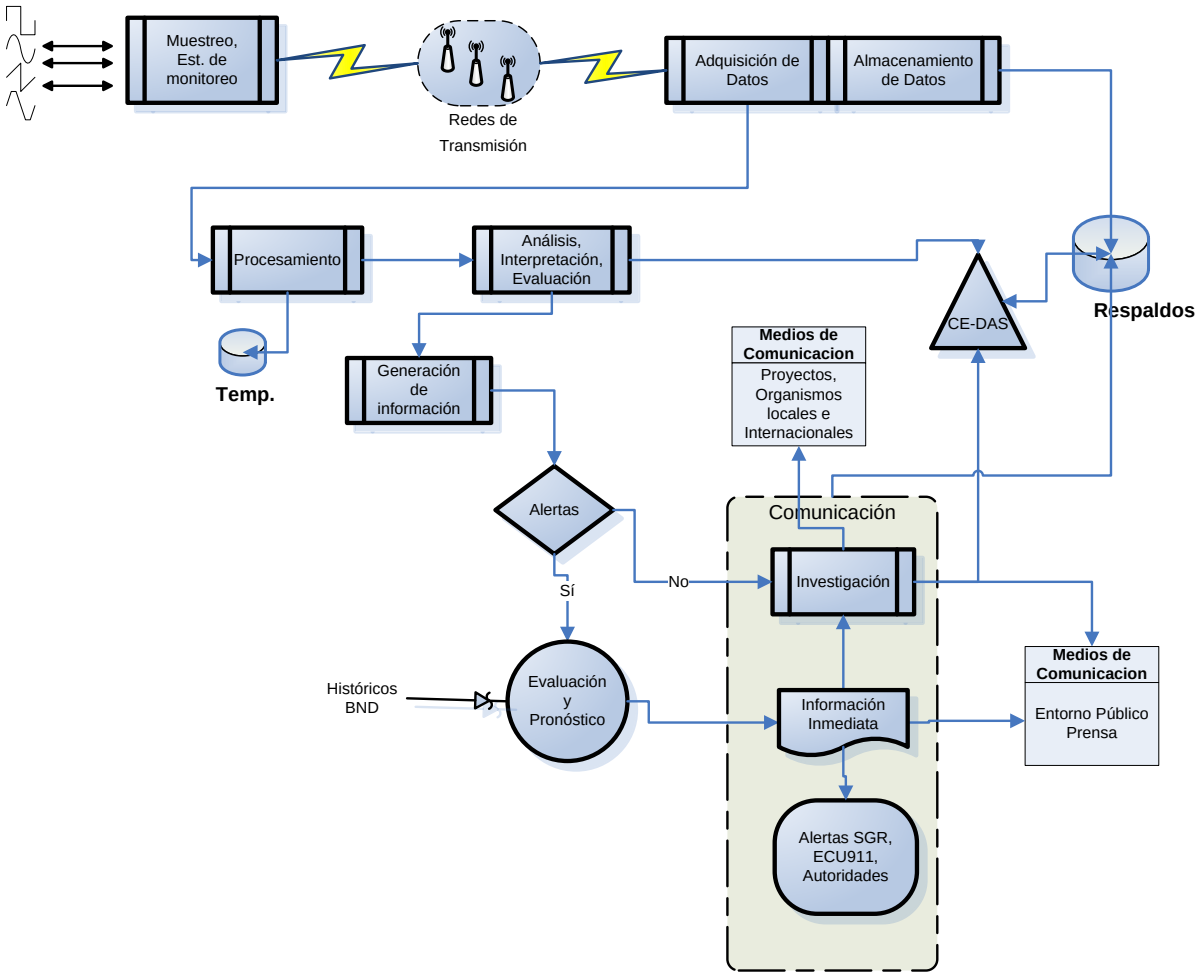
En esta institución IG-EPN se realizó entrevistas al personal de TI, y se pudo concluir que los procedimientos para seguridad de la información no están completamente documentados, las políticas de seguridad se han actualizado parcialmente, se ha hecho énfasis en el control de acceso de usuarios al portal web, pero a nivel interno las normativas para el acceso y manejo de los datos crudos (datos no alterados desde la fuente de captura o adquisición), datos procesados, datos históricos y la información resultante de los estudios y análisis no están difundidas, según la entrevista que se realizó a los jefes de área. Respecto a los respaldos de la información existe personal responsable de ejecución. Finalmente, en base al estado actual se puede decir que no se ha definido las políticas que estandaricen el manejo de esta información sensible y perpetua a nivel de las tres organizaciones contempladas en el presente estudio.

1.1.2. Aspectos comunes encontrados en el manejo de información en los Centros de Investigación

Para llevar el estudio de estos fenómenos naturales en el Ecuador y mantener informada a la población, autoridades y comunidades de científicas, los centros de investigación de desastres naturales sustentan su servicio apoyados en el desarrollo e implementación de modelos y herramientas tecnológicas para la interpretación de

datos. Como resultado, se obtiene una cadena de procesos que se indica en la Figura 1.4 que inicia con la captura de señales o muestreo provenientes del fenómeno natural a ser monitoreado, la siguiente etapa está caracterizada por la adquisición y almacenamiento de datos, para luego realizar su procesamiento aplicando diversos métodos necesarios para el análisis y monitoreo sistemático, a continuación se procede con la evaluación del fenómeno y sus cambios en el tiempo para ser presentados como información inmediata, así también, para fines de investigación científica; con la finalidad de contribuir a una efectiva reducción del riesgo y emisión de alertas tempranas.

Figura 1.4 Cadena de procesos de la información en los Centros de Investigación



Fuente: El Autor

Los Centros de Investigación desde sus inicios han ido incrementando su infraestructura de red en todo el territorio nacional para el monitoreo de estos fenómenos naturales, conformando diversos tipos de estaciones de monitoreo que capturan los cambios de comportamiento del fenómeno natural, estos datos son guardados temporalmente y enviados por diferentes medios de transmisión (Ver Figura 1.5) como son: microonda, fibra óptica, satélite, radio enlaces, internet, línea telefónica dedicada, hasta los centros de interpretación de cada institución para posteriormente efectuar la adquisición de datos, procesamiento de la información e interpretación del evento.

Figura 1.5 Medios de Transmisión de datos

Redes de Transmisión
Transporte de Datos

Institución	Medio de Transmisión	No. Nodos	Cant. Estaciones
IG-EPN	Microonda	21	74
INAMHI		-	-
INOCAR		-	-
IG-EPN	Fibra Optica	21	48
INAMHI		-	-
INOCAR		-	-
IG-EPN	Satelital	15	25
INAMHI		1	60
INOCAR		1	5
IG-EPN	Internet	16	16
INAMHI		-	-
INOCAR		1	6
IG-EPN	Linea Telefónica dedicada	-	-
INAMHI		-	-
INOCAR		5	10
IG-EPN	WiFi largo alcance	18	16
INAMHI		-	-
INOCAR		-	-
IG-EPN	Analógica Radio UHF, VHF	16	26
INAMHI		-	-
INOCAR		-	-
IG-EPN	Red de Voz	22	20
INAMHI			
INOCAR		10	270
IG-EPN	Spread Spectrum	35	120
INAMHI		-	-
INOCAR		-	-
IG-EPN	Red Telefonía Celular	-	-
INAMHI		4	116
INOCAR		1	18

Fuente: El Autor

Esta información es almacenada localmente y luego es clasificada para:

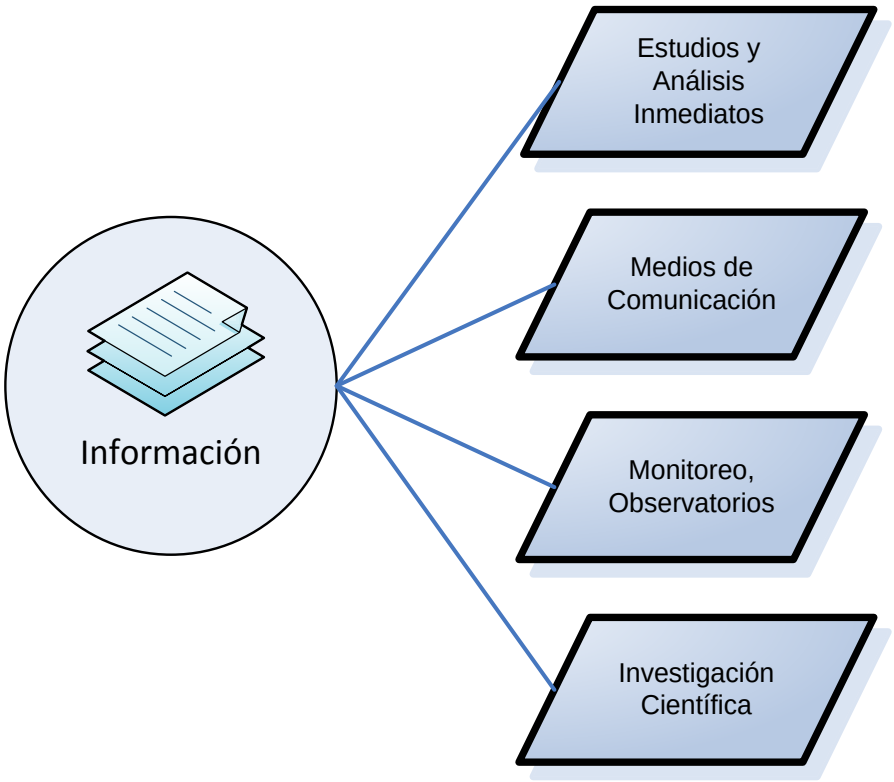
1) estudios inmediatos, análisis y correlaciones de eventos registrados,

2) interpretación de la información para ser entregada a las autoridades y dominio público a través de distintos medios de comunicación (boletines, informes, páginas web, prensa, redes sociales, prensa),

3) monitoreo en tiempo real en los centros de monitoreo y observatorios,

4) disponibilidad de la información para posteriores investigaciones en organizaciones nacionales e internacionales de interés científico en el ámbito del estudio de fenómenos naturales. (Ver Figura 1.6)

Figura 1.6 Usos de la información resultante en los centros de investigación



Fuente: El Autor

Es muy importante reconocer que los procesos para el tratamiento de la información que se manejan en estas instituciones son similares y deben ser gestionados bajo un mismo estándar de seguridad de la información, debido a la sensibilidad de los datos, a sus fines y a la información que se genera de forma continua. Sin embargo, en el área de TI de cada organismo ha visto la necesidad de establecer nuevas normas y procesos que regulen el manejo de la seguridad de la información en estos centros de investigación con el fin de reducir la probabilidad de incidentes de seguridad de alto impacto y pérdidas en su principal activo que es la información. Las medidas implementadas para seguridad de la información actualmente no han sido documentadas bajo alguna normativa y en ciertos casos se ha incurrido en medidas de carácter reactivo; es decir, los siniestros resueltos en el pasado son las referencias de prevención de ataques a futuro renunciando al factor preventivo para hacer frente al incremento de amenazas y vulnerabilidades internas, accidentales o externas. La seguridad de la información es un componente en el cual estas instituciones requieren incrementar sus métodos, controles, tecnología e involucrar la participación conjunta de los usuarios. Un estudio realizado en el Ecuador por la Secretaría Nacional de la Administración Pública (SNAP), propone realizar la implementación, control y seguimiento de la seguridad de la información en algunas organizaciones del sector público en el Ecuador. Sin embargo, en la documentación que se presenta de acuerdo a la página, (Secretaria Nacional de la Administración Pública, 2014, pág. 14) [35]:

> *"centralizar la generación de datos continuos, el acceso inmediato a estos, la presentación de estados de actividad del fenómeno y alertas tempranas son procesos fundamentales y propios de estos centros de investigación que deben estar soportados por una correcta gestión de la información."*.

En términos generales los centros de investigación de desastres naturales en el Ecuador manejan volúmenes importantes de información que son tratados de forma inmediata así como para futuras investigaciones, y no se ha establecido una normativa o método estandarizado para su manejo.

Como vemos en la cita señalada, la identificación de la problemática es vigente y el interés de organismos estatales, es el de centralizar la información con la finalidad de mejorar los procesos descritos.

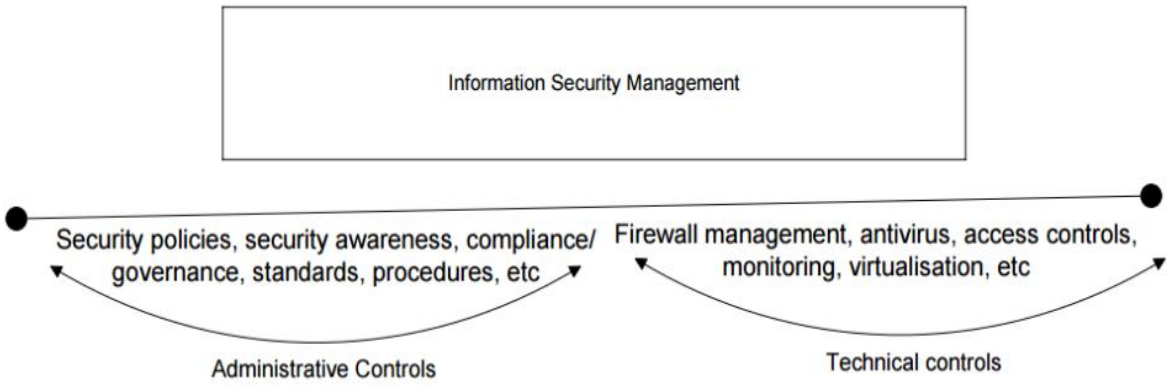
1.1.3. Antecedentes de la Gestión de SGSI en organismos internacionales relacionados a la investigación de desastres naturales.

Las comunidades sismológicas internacionales gestionan los sistemas de seguridad de TI mediante normas y procedimientos oficiales como es el caso del Servicio Geológico de EEUU, USGS Baker, 2007 [37]), y sus normas están bajo la regulación del Departamento U.S. Department of the Interior [37]. Estos procesos deben ser aplicados a los sistemas informáticos, personal involucrado en los sistemas de la información, áreas de desarrollo, técnicos, investigadores y en general para cada etapa del ciclo de vida de los datos [1] [35], [37].

Otra organización referente como es CTBTO lleva implementando en el área de TI el marco SGSI basado en la norma ISO 27001:2005, utilizando en sus procesos el modelo de mejora PHVA, ha desarrollado un Sistema de Gestión de la Seguridad de la Información [45]. En su enfoque para gestionar la seguridad de la información identificó como controles administrativos: a) políticas de seguridad, b) concienciación sobre seguridad, c) cumplimiento / gobierno, d) normas y procedimientos. Respecto a controles técnicos se identificó los siguientes: gestión firewalls, antivirus, controles de acceso, monitoreo, virtualización.

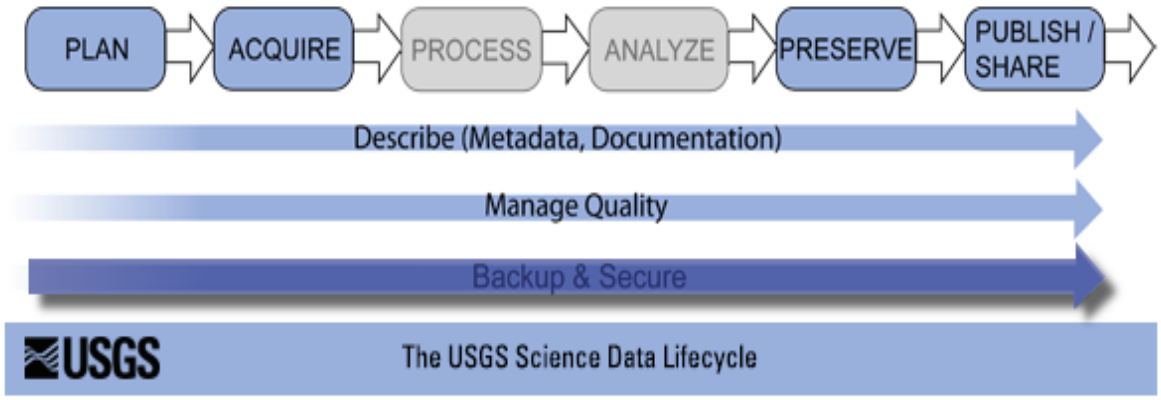
Estos centros de investigación han llevado una vigilancia permanente sobre los procesos de gestión de TI y con ello, se han implantado medidas necesarias para mantener un adecuado sistema de seguridad de la información.

Figura 1.7 Gestión de Seguridad de la Información - CTBTO



Fuente: CTBTO, [45].

Figura 1.8 Modelo de Gestión, ciclo de vida de datos - USGS



Fuente: USGS, [26].

La importancia de gestionar adecuadamente este tipo de información en distintos niveles y bajo los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, nos lleva a la necesidad de adoptar un conjunto de estándares y mejores prácticas para adoptar un modelo a nivel de estas instituciones locales que permita gestionar la seguridad de la información, analizar los incidentes y

el riesgo de las TI, así también, el modelo contribuirá con la adaptación de la información local a estándares aplicados por comunidades sismológicas internacionales como IRIS, USGS, CTBTO, y será un referente que facilite el control y regulación de los centros de investigación, diagnóstico y prevención de desastres naturales del país, de manera que estas instituciones IG, INOCAR, INAMHI formen parte de las redes sismológicas mundiales y de gestión de riesgos.

Los procedimientos en seguridad de la información han sido aplicados parcialmente en los procesos de cada organización; lo que genera problemas al momento de cruzar información entre estas instituciones, aumenta los tiempos de respuesta de entrega de información ante un desastre natural y pueden presentarse dificultades en los niveles directivos y coordinadores encargados de toma de decisiones.

De la misma manera, para el uso de esta información y datos crudos (datos no alterados desde la fuente de captura o adquisición) para futuras investigaciones, es necesario mantener un procedimiento estandarizado que pueda adaptarse a los requerimientos de centros de investigación de desastres naturales a nivel internacional.

La infraestructura de datos y la gestión de las TI que mantienen los centros de investigación locales debe ir apoyada en un sistema de seguridad de la información que agilite la aplicación de políticas, mecanismos y estándares durante el ciclo propuesto en la Figura 1.8, que parte en la adquisición de datos, almacenamiento, procesamiento, interpretación, análisis y difusión de la información.

1.2. Definición de Objetivos y Necesidades de Seguridad de Información en los Centros de Investigación de Desastres Naturales en el Ecuador.

El propósito de implementar procedimientos de seguridad de la información en los centros de investigación es garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados por la organización de forma documentada, sistemática,

estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno, los riesgos y las tecnologías.

1.2.1. Análisis del estado actual de los SGSI en los departamentos de TI en las instituciones locales.

Las prácticas de Seguridad de la Información realizadas en los Centros de Investigación de Desastres Naturales han sido reactivas según las entrevistas realizadas al personal responsable de las TI, es decir; no existe un nivel adecuado para el tratamiento de los riesgos, los test de seguridad de la información no han sido documentados en los últimos años; por lo que no existe un registro histórico de test de vulnerabilidad realizados para determinar la ocurrencia y la periodicidad de eventos de amenaza; esto permite deducir que estas instituciones son vulnerables a los riesgos de información e incidentes de seguridad relativamente graves, pues no se ha implantado una cultura de seguridad de la información transversalen dichas entidades.

Para alcanzar un nivel consensuado en el establecimiento de objetivos y necesidades de estos centros de investigación en el tema de seguridad de la información, es indispensable enfocarse en los objetivos organizacionales que cada institución tiene actualmente. Los mismos que son presentados a continuación:

Tabla 1.1 Resumen de objetivos propuestos por los centros de investigación

	Objetivos Generales	Objetivos Estratégicos
	Reducción del impacto de desastres sísmicos y volcánicos Difusión de los resultados de la vigilancia e investigación de la actividad sísmica y volcánica y comunicación de recomendaciones a entidades locales y público en general Proveer servicios de asesoría en vulcanología y sismología en el Ecuador Emitir pronósticos y alertas a las autoridades y población .- RESPONSABILIDADES: Realizar el monitoreo de la actividad sísmica y volcánica del país con el objeto de emitir alertas y evaluaciones oportunas y confiables. Realizar la investigación científica en el área de vulcanología y sismología para aportar a una efectiva reducción del riesgo; Fomentar el desarrollo de herramientas tecnológicas y su implementación, con el fin de asegurar la óptima adquisición y archivo de datos e información necesaria para el monitoreo sistemático y la evaluación de los fenómenos sísmicos y volcánicos; Promover la concienciación de la población y las autoridades sobre el potencial impacto de los fenómenos sísmicos y volcánicos, buscando incorporar el concepto y las acciones de prevención que conlleven al desarrollo sostenible y sustentable del país; Formar científicos y profesionales de alto nivel en las áreas de conocimiento del instituto. Las demás que señalen la ley, el Estatuto y los reglamentos.	Comprender el vulcanismo ecuatoriano para reducir el impacto de las erupciones Comprender la sismicidad tectónica y volcánica en el Ecuador para reducir el impacto de los terremotos y las erupciones Realizar la investigación científica fundamental para crear las bases necesarias para una efectiva reducción del riesgo Desarrollar y disponer de las herramientas tecnológicas para generar y mantener el flujo de información necesaria para el monitoreo e interpretación sísmica y volcánica Fortalecer la capacidad de gestión interna y consecución de fondos externos -. Proyecto Generación de capacidades para la difusión de alertas tempranas: Objetivo 1: Capturar, transmitir y almacenar de forma continua datos provenientes del monitoreo sísmico, geodésico y volcánico e integrar dichos datos a los algoritmos y procesos para su análisis. Objetivo 2: Proveer de información completa, confiable, actualizada y útil al Sistema Nacional de Gestión de Riesgos sobre la ocurrencia de terremotos de magnitud mayor a 5grados en el territorio nacional, su potencial para producir daños y su capacidad para generar tsunamis. Objetivo 3: Implementar observatorios volcánicos virtuales para poner a disposición del Sistema Nacional de Gestión de Riesgos y de la población amenazada, en tiempo real, información relativa al monitoreo e interpretación de la actividad de los volcanes del Ecuador, así como difundir alertas tempranas. Objetivo 4: Complementar el conocimiento científico sobre los volcanes Ninahuilca, Pululahua y Cuicocha y producir herramientas informáticas y comunicacionales sobre la peligrosidad de éstos y otros volcanes activos y potencialmente activos en el Ecuador.. Objetivo 5: Definir el potencial sismogénico del país y mapear la amenaza sísmica para proveer al Estado de información confiable para mitigar el riesgo sísmico

	Objetivos Generales	Objetivos Estratégicos
	Efectuar nuevas interpretaciones morfo-estructurales de fondo marino, en base a los elementos paleo-relieve, paleo-drenaje y otros medios de interpretación como datos batimétricos de alta densidad, datos de sísmica preexistente de referencia, reflectividad acústica, entre otros, para llegar a definir y conocer el fondo marino para construcción de obras civiles para el desarrollo de infraestructura hidrocarburífera y su adecuada protección. PRINCIPALES TAREAS Realizar, dirigir, coordinar y controlar todos los trabajos de exploración e investigación oceanográfica, geofísica y de las ciencias del medio ambiente marino. Realizar, dirigir, coordinar y controlar los levantamientos hidrográficos, fluviales, y oceanográficos para el desarrollo, compilación y elaboración de la Carta Náutica. Tener a su cargo la construcción, administración, control y mantenimiento de los faros, boyas y balizas en las costas del país. Propender al desenvolvimiento de las ciencias y artes necesarias para la seguridad a la navegación. Constituir el organismo oficial técnico y permanente al Estado, a quien representará en todo lo que se relacione a las investigaciones oceanográficas, hidrográficas, de navegación y de ayudas a la navegación. Controlar el funcionamiento de los repartos subordinados y Unidades adscritas al INOCAR.	Investigar la morfología submarina del lecho marino, a escala 1:50.000, para profundizar el conocimiento de todos los detalles geológicos, tectónico-sísmicos, en el área de interés. Impulsar la adquisición, procesamiento y análisis de datos geológicos y geofísicos que puedan tener aplicación en la industria petrolera (PETROECUADOR, INOCAR), ejecutadas por personal técnico especializado ecuatoriano. Analizar el comportamiento de estructuras y fallas geológicas integrando las áreas continentales con las submarinas adyacentes, para poder deducir el tipo de riesgo que existe y que puede afectar a una determinada instalación crítica existente y/o que a futuro se puede edificar en la zona de estudio. Sustentar y soportar el proyecto de investigación para su comprobación y sensibilización con información pre-existente de tipo geofísico (sísmica), en áreas donde exista la misma, a lo largo de las provincias del Guayas, Santa Elena, con la finalidad de reevaluar información antigua como datos técnicos importantes para la investigación propuesta. Obtener productos finales (Resultados), tales como mapas de fondo oceánico multitemáticos a escala detallada 1:50.000, y otros, en formato analógico y en digital, que permitan efectuar simulaciones matemáticas interactivas en 3D de modelos previamente definidos, a través de la migración de bases de datos procesados de otros sistemas.

	Objetivos Generales	Objetivos Estratégicos
AMHI	Contribuir al desarrollo sustentable del país a través del mejoramiento de la calidad y disponibilidad de la información hidrometeorológica, que sirva de base para la planificación territorial, la gestión de los recursos hídricos y la adopción de sistemas de alerta temprana frente a riesgos provocados por eventos naturales. PRINCIPALES TAREAS A través de la ciencia y la tecnología actual tiene la posibilidad de vigilar y predecir el comportamiento de la atmósfera y las aguas interiores. Produce información fundamental para emitir alertas tempranas que pueden salvar muchas vidas, reducir los daños materiales y proteger el medio ambiente. Contribuye al esfuerzo internacional mediante el intercambio de información con otros países, sobre el tiempo, el clima, los recursos hídricos, de acuerdo a las normas aplicadas a nivel internacional. Mantiene un sistema de cooperación y suministro de información oportuna y segura, con los medios de comunicación, prensa, radio, televisión; además de números telefónicos especiales, facsímil, correo electrónico, conversación directa con un meteorólogo, para la entrega del pronóstico diario del tiempo, predicciones y avisos de fenómenos meteorológicos e hidrológicos extremos, al público; Defensa Civil; Gobierno Central y otros organismos públicos y privados. Colabora en las actividades nacionales de planificación a corto y largo plazos para el desarrollo sostenible del país. Opera y mantiene la infraestructura nacional de estaciones meteorológicas e hidrológicas: recopila, estudia, procesa, publica, y difunde la información hidrometeorológica	Fortalecer el carácter científico y técnico en la estructura institucional e instituir procesos desconcentrados, con la coordinación, supervisión y fiscalización de la sede central del INAMHI en Quito. Optimizar y ampliar la cobertura espacial de las redes de observación hidrometeorológica por sistemas o cuencas hidrográficas, incorporando nuevas tecnologías de automatización, información y comunicaciones en su estructura y mejorando la calidad de las observaciones realizadas. Generar estudios e investigaciones relacionados con la meteorología, hidrología, Cambio Climático, Sistemas de alerta temprana hidrometeorológica, propendiendo al desarrollo de un sistema nacional de información que permita la consolidación de la información actual e histórica generada por las redes operadas por distintos actores públicos, privados y, que garantice el acceso a todos los usuarios. Reforzar y complementar los equipos técnicos y profesionales del INAMHI mediante la formación, capacitación y reclasificación del personal técnico que actualmente labora en la Institución y la incorporación de jóvenes profesionales.

Fuentes: 1) IG-EPN [39], 2) INAMHI [11], 3) INOCAR [5].

De la Tabla 1.1, se puede extraer que el factor fundamental y principal activo para dar cumplimiento a los objetivos planteados por las instituciones en mención es la ***"Información"*** que se genera para contribuir a la seguridad nacional frente a fenómenos naturales; es la información y los datos almacenados los que permiten realizar posteriores investigaciones de carácter científico que contribuyan a la reducción del riesgo.

Basándose en el Plan Estratégico propuesto por cada institución (Anexo A), no se contempla en forma explícita alguna acción relacionada a la implementación o mantenimiento de un Sistema de Seguridad de la Información, por lo cual se puede concluir que a nivel estratégico la gestión en seguridad de la información está implícita dentro de los procedimientos y actividades que se ejecutan en las áreas de TI. Este hecho conduce a que se debe dar un mayor compromiso a la inversión en las TI por parte de los directivos, ya que la información es su factor fundamental y crítico que está relacionado directamente al producto/servicio principal que estos centros de investigación generan de forma continua.

1.2.2. Definición de objetivos y necesidades de los Centros de Investigación

Como resultado de las entrevistas y opiniones recibidas por los directivos de las áreas de TI, a continuación se presentan los requerimientos de seguridad de la información que actualmente demandan los centros de investigación mencionados y que constituyen un factor crítico:

- Evaluar mediante normas estandarizadas y técnicas las vulnerabilidades a las cuales está expuesta la información de los Centros de Investigación de desastres naturales.

- Gestionar por niveles de acceso los activos de información e identificar las acciones para protegerlos estableciendo una escala de aceptación del riesgo controlable.

- Definir el modelo de gestión que adopte el control, prevención y reducción de incidentes de seguridad de la información identificados y su potencial impacto.

- Presentar un plan de acciones y herramientas necesarias para reestructurar en la gestión de comunicaciones y operaciones un sistema de gestión de seguridad de la información, considerando que los controles de acceso a los datos obtenidos e información generada son a distintos niveles en el medio interno y externo de cada institución.

- Establecer un plan de involucramiento a nivel directivo y participación activa de las gerencias y jefaturas para concientizar la vulnerabilidad del principal activo de estas instituciones que es la información, comprometiendo el estudio necesario para la asignación de recursos, factibilidad económica y técnica.

- Incrementar el compromiso del personal involucrado en las TI para dar cumplimiento a las políticas y buenas prácticas de seguridad acordes a los objetivos institucionales, alcances establecidos, valor de la seguridad de la información en cada organismo.

1.2.3. Determinación de los alcances del Estudio

Para definir el presente estudio se ha acordado con la alta dirección que deben actualizarse los lineamientos que permitirán una reforma trascendental en la gestión de seguridad de la información. Se ha reconocido la necesidad de llevar un análisis a los Sistemas de Información de estos Centros de investigación a nivel de topología de red y componentes tecnológicos tomando en consideración que la gestión de seguridad de la información debe comprender desde el origen de generación de los datos que son las estaciones de monitoreo (terminales) como puntos de partida, pasando por los medios de transporte de datos (redes privadas, nodos compartidos, redes públicas), una vez que arriban los datos a los centros de monitoreo, llevar el análisis en las fases de adquisición, procesamiento, análisis de datos, presentación de

resultados y elaboración de informes (servidores de acceso y gestión de la información, switchs, hubs, plataformas medios de comunicación), y como fase final el respaldo de datos crudos y procesados (servidores de respaldo) que son utilizados para investigaciones posteriores a nivel nacional e internacional.

Dentro de este ámbito se deberá considerar la identificación de activos, evaluaciones y recomendaciones de seguridad de la información en las áreas de administración de la red e infraestructura física, para las distintas áreas técnicas y administrativas, y finalmente, la gestión de seguridad que contemple las políticas y controles acceso físico y lógico a la información dentro de los centros de investigación a través de intranet e internet en los distintos niveles Directivo, Estratégico, Táctico y Operativo.

El entorno de este modelo se delimita a analizar y evaluar cualitativamente la seguridad de la información en estos Centros de Investigación para definir un estándar referente para acciones futuras de auditoría de la información y toma de decisiones a nivel de Jefaturas y Directivos.

El modelo a presentar no constituye un documento oficial de pruebas, implementación y aprobación en cada organismo; es un modelo que servirá para alinear la gestión de seguridad de información y requerirá de mayor afinamiento para llevarlo a procesos específicos y actividades que se desenvuelvan en las áreas de TI considerando sus demandas tecnológicas y reformas a futuro en su estructura organizacional.

Como resultados del estudio se procura favorecer a la Gestión de la Seguridad de la Información de los Centros de Investigación de desastres naturales identificando procesos y riesgos de información tomando como referencia las recomendaciones y modelos ISO 27000, Magerit, Octave, NIST SP 800-30 y Coras para acoplar y sintetizar un modelo específico aplicado a la infraestructura, equipos y prácticas del componente humano en estos Centros de Investigación.

1.3. Caracterización y Dimensionamiento del Caso de Estudio: Instituto Geofísico de la Escuela Politécnica Nacional.

En esta sección se presenta una descripción de las características tecnológicas del Instituto Geofísico para evidenciar las actividades más relevantes asociadas con el activo información.

1.3.1. Identificación del activo de información crítico

Esta institución ha llevado constantemente ampliaciones en su estructura tecnológica, debido al incremento de equipos físicos y software, indispensables para cubrir el monitoreo sísmico y volcánico en la mayor parte del territorio nacional.

Actualmente, la densidad de estaciones de monitoreo supera 300 terminales que registran diversos parámetros de medición en tiempo real como por ejemplo: estaciones de monitoreo sísmico, acelerográficas, inclinometría, gps, infrasonido, afm, geoquímica, imágenes en rango infrarrojo y rango visible. Estos equipos de monitoreo junto con los equipos para transmisión de datos principalmente tienen interfaces de comunicación con puertos Ethernet, inalámbrico y serial, los protocolos utilizados son RS232, TCP/IP, FTP, RTP, HTTP, IEEE 802.11a/b/g. La tasa de transmisión real utilizada en el transporte de los datos hacia el Centro de Monitoreo ubicado en la ciudad de Quito está en el rango que va desde 154Kbps hasta 4Mbps, dentro de las bandas de frecuencia no licenciadas de 900MHz, 2.4GHz, 5.7GHz y bandas licenciadas en 450-465MHz, 2.4GHz, 7.5GHz, Banda C, además de nodos de conexión a la Fibra Óptica de CELEC-TRANSELECTRIC con capacidad E1 y STM1. Actualmente esta red ha sido administrada de forma eficiente, no se han reportado incidentes de seguridad graves; sin embargo, se pudo evidenciar que no existe documentación, manuales y normativas para gestionar el control de acceso a las estaciones terminales y redes de transporte de datos, actualización de Firmware, métodos para encriptación y aplicaciones que registren la gestión de cambios, determinando así que existe un punto de vulnerabilidad muy sensible sobre los equipos

que adquieren las señales obtenidas del fenómeno natural en estudio y además en los medios que transportan los datos hasta el Centro de Monitoreo del IG-EPN [25].

Continuando con la cadena de procesos de la información identificada en estos Centros de Investigación y que se representa en la Figura 1.4, se tiene los datos que arriban al IG-EPN, los sistemas de almacenamiento y distribución están conformados por servidores donde el hardware y software que se utiliza para la adquisición y procesamiento de estos datos es heterogéneo, ya que los sistemas y redes de vigilancia actuales son equipos especializados y desarrollados por distintos fabricantes, diversas tecnologías y distintos formatos de adquisición y procesamiento; sin embargo, el IG-EPN ha tratado de consolidar dos sistemas de adquisición y procesamiento utilizados por los centros de investigación más representativos a nivel mundial [26], [37], [41], que son Seiscom3 y Earthworm para los datos sísmicos, acelerográficos e infrasonido. Los datos de geodesia son gestionados a través de un sistema adaptivo del modelo de la red GEOAZUR (Francia) para la gestión de datos. Respecto a los demás parámetros de medición del fenómeno natural, la adquisición y procesamiento se controla con sistemas independientes propios (matlab, c-shell) o de fabricante como son "Geotech, DOAS, Trimble", y software desarrollado en el IG-EPN "Sami". En esta fase la adquisición y procesamiento es soportada con servidores dedicados de alta disponibilidad para cada sistema Seiscom3, Earthworm, Geoazur y servidores descentralizados de menor capacidad para los demás parámetros de medición. El funcionamiento de estos sistemas es monitoreado por el personal de TI y el personal encargado del análisis y la interpretación de los datos obtenidos de los eventos sísmicos o volcánicos. Las acciones en el área de seguridad aplicadas en estos activos han permitido mantener a estos sistemas funcionales, existen aplicaciones de software libre, propietarias y desarrolladas en el IG para la gestión de la Data, además de manuales y guías sobre los procedimientos a seguirse en caso de fallos durante los procesos de adquisición y procesamiento, ya que el personal del IG-EPN mantiene el monitoreo, investigación y vigilancia desde el Instituto Geofísico y observatorios las 24 horas, los 365 días del año.

Los activos críticos en la etapa de adquisición y almacenamiento son los datos afectados por gaps o tiempos muertos en donde no se adquirieron o procesaron datos continuos de una estación, o datos de un grupo de estaciones que por factores internos presentan fallos provocados en las aplicaciones y sistemas de almacenamiento de datos crudos y datos procesados,. Otro factor se debe a retardos en la aplicación de soluciones por parte del personal que gestiona la Data en el Centro Nacional de Datos sísmicos y volcánicos CND y en el Centro de Monitoreo Terras; como factores externos se ha presentado interrupciones durante el transporte de los datos a tiempo real o cortes de energía eléctrica extendidos en el Centro de Monitoreo, esto provoca que las aplicaciones y software que están ejecutándose en los servidores y estaciones de trabajo generen errores en su base de datos o cierres inesperados en sus procesos, teniendo que recurrir a la reinicialización manual generando más procesos semiautomáticos, de recuperación de datos y una sobrecarga a los servicios que están corriendo a tiempo real en las estaciones terminales en el transporte de los datos y en el propio proceso de adquisición y almacenamiento. También se puede evidenciar que los servidores descentralizados, no están llevando un registro o control de actividad, ocasionando fallos relacionados a la capacidad de almacenamiento y saturación en los recursos de capacidad de almacenamiento, procesamiento y memoria necesaria para re-procesar datos en cola o ejecutar nuevos procesos que demandan los usuarios.

Existen otros recursos que se ven involucrados en estos fallos y de igual forma no se ha implantado un sistema estandarizado que permita consultar si se aplicaron políticas de seguridad de la información y gestión de cambios. Entre estos elementos se pueden mencionar switchs de acceso y distribución, routers, módems, discos externos, aplicaciones, accesos a la infraestructura física, salas de servidores, salas de monitoreo y equipos de radiocomunicaciones.

El sistema de respaldo de datos y de la información es el activo más crítico en la cadena de procesos de la Figura 1.4, debido a que el IG y los demás Centros de Investigación demandan el almacenamiento perpetuo de los datos crudos, datos

procesados, y de información resultante del análisis e interpretación; el objetivo es brindar una alta disponibilidad e integridad a la comunidad científica y público que así lo demande, para garantizar en el tiempo el acceso a datos históricos y facilitar la emisión de informes sobre alertas tempranas. Para el Caso de Estudio IG-EPN el volumen de datos generados en los últimos años ha superado los seis Terabytes anuales y se ha proyectado a mediano plazo bordearan los 10 Terabytes de información almacenadas en cada año, la cual debe tener alta disponibilidad, integridad para ser tratada y compartida con centros de investigación de desastres naturales a nivel mundial y bajo estándares internacionales. Los procedimientos para el manejo de los respaldos de datos e información han venido implementándose en función del crecimiento de las redes de monitoreo y avances tecnológicos de la institución [14].

El Centro de Datos del IG-EPN actualmente cuenta con un servidor Blade que maneja 5 nodos, 7 cuchillas, pero con capacidad de almacenamiento limitado, en este servidor se encuentran alojados respaldos del antiguo servidor de correo, el almacenamiento total de la red geodésica RENGEO, guardado de versiones de desarrollo y archivos fuentes, almacenamiento de video e imágenes de monitoreo y sistemas para aplicaciones relacionadas a la administración.

La adquisición más reciente es el Flex System Server, en donde se aloja la mayoría de procesos relacionados al tratamiento de los datos, entre ellos: la última versión del sistema de adquisición y procesamiento sísmico y tectónico Earthworm, los respaldos en crudo, datos procesados e información resultante que conforman la Base Nacional de Datos, el sistema de gestión SharePoint, el servidor para gestión de información geográfica GIS y el servidor para ambientes de desarrollo y pruebas. Este sistema cuenta con 152 núcleos, 500Gb en memoria RAM y 80 terabytes para almacenamiento de datos y un sistema de virtualización para garantizar la continuidad de operación del sistema de información.

Adicionalmente, se gestiona de forma independiente de los sistemas Blade y Flex, dos servidores físicos espejo para la gestión del sistema de adquisición y procesamiento

Seiscomp3 con el fin de mantener una réplica física y no lógica, este sistema abarca el mayor número de señales sísmicas que ingresan a tiempo real al IG-EPN.

Se ha identificado que durante las etapas de adquisición, almacenamiento y procesamiento de datos existe información que se respalda automáticamente en el servidor Flex, sin embargo existen pequeños volúmenes de información provenientes de otras redes (AFM, DOAS, estaciones sísmicas remotas) que no están debidamente respaldados, debido a que requieren de procesos manuales de extracción de datos, o son tramas de información que se interrumpen durante el transporte de datos y se encuentran alojado en estaciones de trabajo, laptops y discos externos de usuarios que procesan o respaldan los datos temporales. Existen además en las estaciones sísmicas, discos temporales de almacenamiento menores a 16GB en donde se colectan las señales adquiridas directamente y que de no recuperarse representarían brechas o vacíos no recuperables en los datos crudos.

Para contrarrestar estas pérdidas de datos en las estaciones terminales los usuarios internos realizan procesos de recuperación manuales o semi automatizados, pero no existe un registro físico y aplicaciones automatizadas que faciliten la gestión y control de la recuperación de datos crudos; en este aspecto se puede apreciar la necesidad de implantar un plan específico de gestión de respaldos total para aplicarlo durante toda la cadena de información.

Los procesos relacionados con Análisis, Interpretación y Evaluación se ejecutan mediante instancias al CE-DAS de los datos almacenados y datos que arriban en tiempo real de las redes de monitoreo; utilizando aplicaciones especializadas, software propietario y herramientas bajo Linux que facilitan la generación de Información inmediata preliminar que servirá para la determinación de alertas tempranas. Así también, estos resultados son complementados con otros procesos de análisis que agregan mayores fuentes de datos y son enviados a la Base Nacional de Datos como "Datos Procesados", en esta fase se evidencia la importancia de la alta disponibilidad de la Data para facilitar el análisis, interpretación y generación de alertas tempranas y cada uno de estos procesos y componentes de Software/Hardware deben estar

apoyados con la gestión de seguridad de las TI. Actualmente el IG-EPN lleva ejecutando los procesos mencionados parcialmente ya que no se han establecido normativas o políticas basadas en un estándar, los mecanismos que mantienen operativos estos procesos son el resultado del monitoreo continuo y soporte del personal de TI que labora en el IG-EPN.

En la cadena de procesos se identifica el proceso "Comunicación" en esta etapa se presentan los resultados obtenidos a través del principal medio de comunicación que es el portal Web del IG-EPN, de acuerdo a la cartera de productos y servicios del IG [25], aquí se da a conocer los estados de alerta sísmica y volcánica principalmente y otros servicios al público en general, comunidad científica, entidades gubernamentales y privadas. Por ello, en este proceso es fundamental implantar la gestión de seguridad de la información para garantizar la disponibilidad e integridad de los mensajes, informes, boletines, estados de alerta, imágenes, otros.

Los servicios de correo institucional, Internet, control antivirus e instructivos generales de Seguridad de la Información y uso adecuado de las TICs son regulados a través de la Dirección de Gestión de la Información y Procesos DGIP-EPN. Dentro de la estructura organizacional de la EPN, de acuerdo al Plan Estratégico Institucional de la EPN [39], nos señala que:

> *"las funciones a nivel de control y acceso a la red que el IG-EPN desempeña como Proceso Descentralizado e independiente son el servicio de internet alterno para la matriz y para los observatorios (sucursales), servidor de correo para el departamento de Geofísica, servidor cloud web autoescalable, servidor dedicado antivirus, gestión de canales por IP pública para una red de estaciones sísmicas dedicadas, gestión de la red de monitoreo sísmico a través de canales de servicio satelital y servicio de Fibra óptica que son gestionados en colaboración con proveedores externos a la EPN y son distribuidos dentro de la intranet del IG-EPN".*

En este aspecto se pueden identificar brechas de seguridad perimetral y debe realizarse una actualización en los procesos de gestión de Seguridad de la Información, ya que existen diversos canales externos para la transferencia de la información que no han sido gestionados a través de un estándar para el control de firewalls, ips, Cisco ASA, requerimientos hacia los proveedores externos estos servicios y gestión de soluciones para la intranet de la EPN.

Finalmente, durante las entrevistas realizadas al personal del IG-EPN se identificó otros requerimientos específicos dentro de cada una de las cinco áreas del IG, relacionadas a la gestión de seguridad de la información y que se mencionan a continuación:

- **Área de Sistemas:**
    - Automatizar la gestión de cambios en los activos de la red de información del IG.
    - Mejorar bajo una metodología estandarizada la gestión y control de activos de Información como son hardware: servidores, pc, portátiles, impresoras, infraestructura de red. Software: SO, software de aplicación y software especializado
    - Establecer procesos rutinarios de identificación y registro de amenazas y vulnerabilidades utilizando técnicas de Ethical Hacking, herramientas de seguridad, monitoreo de red, control de hardware y software, además de herramientas de control de virus y malware, evaluación y auditoría de seguridad de la información.
    - Centralizar en la Base de Datos del CND (Centro Nacional de Datos) motores de búsqueda que faciliten el uso de la información inmediata. Establecer protocolos y metodología de documentación y actualizarlos para los procesos de gestión de TI del IG-EPN

- Desarrollar el Plan de contingencia del CND actualizado con enfoque hacia el Centro de Datos alterno (espejo), realizando una clasificación y dimensionamiento de procesos, aplicaciones y recursos tecnológicos.

- **Área de Sismología:**
  - Realizar un estudio de factibilidad para potencializar al Centro Nacional de Datos símicos y volcánicos como Centro de Datos nivel 3 basado en el estándar ANSI/TIA-942.

- **Área de Vulcanología:**
  - Integrar una base de datos para consultas rápidas y estadísticas de calidad.
  - Incrementar la capacidad de almacenamiento y procesamiento para los servidores dedicados a la red de Geodesia.

- **Área Técnica:**
  - Implementar un sistema de gestión de cambios y registro de instalaciones, mantenimientos en estaciones terminales, en las redes de transporte de datos y arribo de datos al IG y Observatorios.

- **Área Administrativa:**
  - Implementar un sistema de control de equipos y control de cambios en las estaciones de monitoreo, en las oficinas del Instituto Geofísico, observatorios, estaciones temporales y repetidoras que son los componentes relacionados al tratamiento de los datos e información.

1.3.2. Dimensionamiento del sistema de información – caso de estudio

La implementación del modelo de gestión de seguridad de la información propuesto, pretende evaluar el estado actual de la seguridad de la información en los procesos centrales de Gestión de datos sísmicos-volcánicos y la Gestión de acceso a la

información relacionada al monitoreo sísmico y volcánico, con el objetivo de identificar las vulnerabilidades, impactos, riesgos a los que está expuesta la información y datos, así como proponer soluciones enmarcadas desde el enfoque de seguridad de la información.

El modelo de SGSI propuesto, será un referente para identificar por etapas los requerimientos, políticas, metodologías, procedimientos y acciones que deberán implementarse para fortalecer la seguridad de los activos de información en el Instituto Geofísico y fomentar a nivel directivo la necesidad de implantar un sistema de seguridad de la información que se acople a los requerimientos y demandas de este centro de investigación.

1.4. Discusión de Problemas y Posibles Soluciones

Los esfuerzos actuales para proteger los activos de información en los centros de investigación, diagnóstico y prevención de desastres naturales en el Ecuador, requieren ser enfocados hacia la integración de procesos estandarizados para el tratamiento de su principal activo y servicio que es la disponibilidad de los datos y el acceso a la información en el tiempo.

Los centros de investigación mundiales como USGS, IRIS, CTBTO, IRD han adoptado distintas metodologías y estándares de seguridad de la información, con el objetivo de proteger su información y gestionarla adecuadamente frente al desarrollo tecnológico e incremento de riesgos de seguridad de la información.

La propuesta de un modelo de seguridad de la información que contemple la estructura organizacional propia de los centros de investigación en el Ecuador, facilitará la identificación de soluciones específicas en el ámbito de seguridad de la información y optimización del recurso tecnológico, financiero y humano dedicado a la mitigación de riesgos de seguridad de la información.

CAPÍTULO 2. DESARROLLO DEL MODELO DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

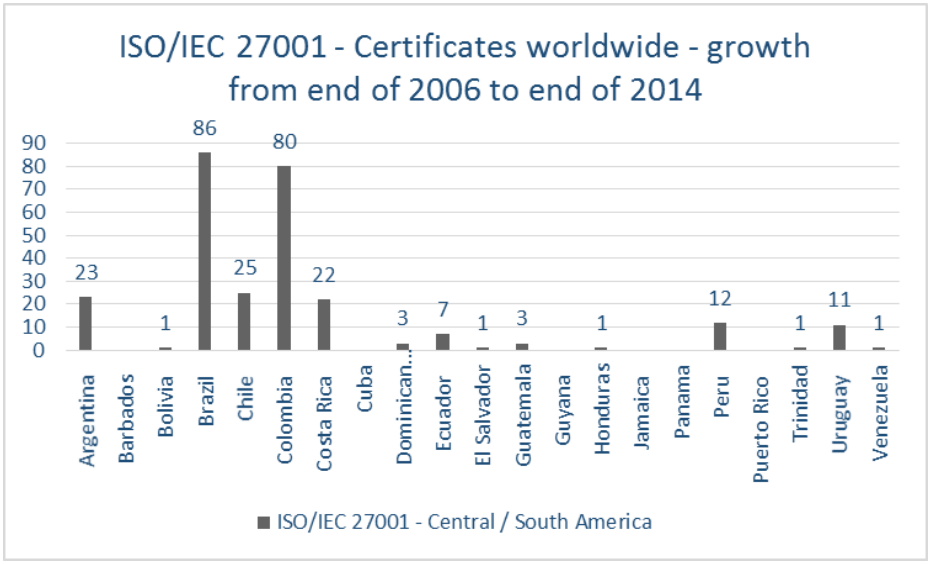
2.1. Selección de normas, marcos de trabajo y estándares internacionales

En la actualidad las organizaciones han adoptado distintas normas y prácticas relacionadas a seguridad de la información, en la mayoría de regiones han aplicado en su estructura organizacional las normas ISO 27001; un estudio presentado por la organización internacional ISO "World distribution of ISO/IEC 27001 certificates in 2014" muestra que la cantidad de certificados emitidos por organismos de certificación acreditados por la IAF(International Accreditation Forum) [12], en los países de Sudamérica es ascendente de la misma forma en el Ecuador como indica en la Figura 2.1 En EEUU, por ejemplo se ha aplicado la guía NIST SP-800 como estándar recomendado por el "U.S. Department of the Interior".

Figura 2.1 Certificaciones ISO/IEC 27001 emitidas a organizaciones en el Ecuador

Fuente: ISO SURVEY, [12].

Figura 2.2 Certificaciones ISO/IEC 27001 emitidas a nivel Centro y Sudamérica



Fuente: ISO SURVEY, [12].

En las Figuras 2.1 y 2.2 se evidencia que en Ecuador existe mayor interés en obtener la certificación ISO 27001 en los últimos años, con el objetivo de alcanzar mayor prestigio y seguridad en la información que manejan estas instituciones. Entre las empresas que han obtenido esta certificación se puede mencionar a Movistar, CNT y Telconet.

En el Ecuador, el Servicio Ecuatoriano de Normalización INEN además de otros organismos reguladores en el área de TI y seguridad de la información (Secretaria Nacional de Administración Pública SNAP, Ministerio de Telecomunicaciones y Sociedad de la Información MINTEL, Ley Orgánica de Transparencia y Acceso a la Información Pública LOTAIP) han propuesto aplicar como estándar la norma NTE INEN-ISO/IEC 27000 para la gestión de la seguridad de la información gubernamental.

En el estudio presentado por la Comisión para la Seguridad Informática y de las Tecnologías de la Información CSITIC en octubre del año 2011, indica que alrededor de 85 entidades públicas deben sujetarse a los controles establecidos por la SNAP, y que mediante acuerdos ministeriales No. 804 y No. 807 en el año 2011, acuerdo

No.309 de la SNAP fueron asignados como ente regulador en el tema de seguridad de la información en el Ecuador.

Los centros de investigación de desastres naturales INOCAR, Instituto Geofísico, INAMHI carecen de estas certificaciones, a nivel interno no se ha establecido como estrategia organizacional la aplicación de normas de seguridad de la información o metodologías de gestión de riesgo de seguridad de la información en todas las áreas/unidades de cada institución; esto conduce a tener una organización susceptible de pérdidas de datos (Anexo K) e información y potenciales amenazas que atentan contra la seguridad de los sistemas de información.

2.1.1. Normativas para la seguridad de la información en el Ecuador

La base legal vigente relacionada al área de gestión de seguridad de la información se indica en el Anexo B, comprende las leyes y normas que se indican a continuación:

- Constitución Política del Ecuador

  En referencia a los Artículos: 18, 23, 28, 81, 389.

- Normas de Control Interno de la Contraloría General del Estado.

  En referencia a los Artículos: 300-01, 300-02, 300-03, 300-04, 410-10,

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

  En referencia a los Artículos: Título 1 - Art.8 - Art. 9, Título 2 - Art.13 - Art. 14, Título 3 – Art. 50, Título 4 - Art.52, Título 5 - Art.57 - Art.60 - Art.61 - Art.62 - Art.63 - Art.262.

- Ley del Sistema Nacional de Registro de Datos Públicos.

  En referencia a los Artículos: 18, 26.

- Ley de Propiedad Intelectual (IEPI).

  En referencia a los Artículos: 3, 7, 8.

- NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27000:2012

  En referencia a la familia de normas SGSI NTE INEN-ISO/IEC: 27000, 27001, 27002, 27003, 27004, 27005, 27006, 27007, 27011.

- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)

  En referencia a los Artículos: 1, 4, 5, 6, 7, 10, 23.

- Acuerdos - Secretaría Nacional de la Administración Pública (SNAP).

  En referencia a los Acuerdos: 166, 309.

- Ley De La Cartografía Nacional (IGM).

  En referencia a los Artículos: 22, 25, 26, 27.

- Decreto No. 1246, Instituto Espacial Ecuatoriano (IEE)

  En referencia al Artículo 3 del Decreto No. 1246.

2.1.2. Políticas complementarias referentes de los centros de investigación internacionales

En las entrevistas realizadas al personal de TI y jefes de áreas de los centros de investigación locales, se puede constatar que las políticas seguridad de la información no están definidas y/o aprobadas por los directivos de cada institución. Se puede evidenciar que dichas políticas son asumidas de la legislación vigente en el Ecuador y que se describen en la sección 2.1.1 anterior. Los centros de investigación internacionales como es el caso de USGS presentan una serie de

manuales que contienen políticas dedicadas a varios procesos, entre estos el área de seguridad de la información, y que se presentan a continuación en la Tabla 2.1:

Tabla 2.1 Políticas de seguridad de información U.S. Geological Survey Manual

Department of the Interior	
U.S. Geological Survey Manual	
Administrative Series	
	Security
440.1	Identification Cards/Building Passes
440.2	Physical Security Program
440.3	National Security Information
440.4	National Security Information Automated
	Information Systems
440.6	Flags
440.7	National Security Position Program
440.8 Information	Nuclear Formerly Restricted Data (FRD) and Restricted Data (RD) Classification and Declassification
Program Series	
	USGS Program Policies
500.10	USGS Reporting Policy
500.15	Customer Service Policy
500.16	Classification and Inventory of USGS Web Services
500.20	Technology Transfer Authority
500.24	Policy for Release of Computer Databases and Computer Programs
500.25	Scientific Integrity

Fuente: USGS [37].

Tabla 2.2 Políticas de seguridad de información U.S.G.S

	Geographic Information Office Program Policies
600.3	Networking of Computing Resources
600.5	Information Technology Systems Security - General Requirements
601.1	USGS Web Standards
	Emergency Planning and Operations
1000.1	Emergency Planning and Operations - Purpose, Policy, Procedure
1000.2	USGS Workforce Accountability Plan

	Publishing
1100.1	Information Product Planning (replaces SM 500.17)
1100.2	Editorial Review of U.S. Geological Survey Publication Series
1100.3	USGS Publication Series (replaces part of SM 503.1)
1100.4	Use of Outside Publications, Including Abstracts (replaces part of SM 503.1)
1100.5	Authorship, Credits, and Acknowledgements in USGS Information Products (replaces SM 503.2)
1100.6	Use of Copyrighted Material in USGS Information Products (replaces 450.3)
1100.7	Audiovisual Media and Products (replaces SM 500.7)

Fuente: USGS [37].

El contenido de estos documentos (ver Anexo C), hace referencia a las obligaciones y responsabilidades que debe asumir el personal involucrado en las actividades que se desarrollan en el centro de investigación USGS. Uno de los objetivos de implementar un modelo SGSI es determinar si las políticas pueden ser adaptadas y si deben ser aplicables a los centros de investigación locales.

2.1.3. Análisis comparativo de las metodologías para la gestión de riesgos de seguridad de la información

El objetivo de estas metodologías es proponer una guía para la gestión de riesgos de seguridad de la información. A continuación se presenta un resumen de los aspectos que fueron considerados dentro de cada metodología.

Tabla 2.3 Cuadro comparativo de normas y metodologías para seguridad de la información

	ISO 27001	ISO 27005	MAGERIT	OCTAVE	NIST SP800-30	CORAS
TIPO	Norma	Norma	Metodología	Guía	Guía (Estándar en EEUU)	Metodología
Desc	Requisitos para el sistema de gestión de seguridad de la información	Directrices generales para la gestión de riesgos de seguridad de la información. De acceso restringido por pago	Análisis y Gestión de riesgos TI	Modelo para la creación de metodologías de análisis y gestión de riesgos	Modelo de gestión de riesgos	Metodología para construcción de plataformas para análisis de riesgos de sistemas críticos de seguridad
Ori	La última traducción en España bajo la versión UNE-ISO/IEC 27001:2014 de la AENOR España	Organización para la estandarización ISO	Ministerio de administración pública España 2006. Consejo Superior de Administración Electrónica	Instituto Nacional de Estándares y Tecnologías de EEUU, 2002	Universidad de Carnage Mellon, EEUU 2007	Grupo de investigación SINTEF Noruega, 2001
Alcan	En Anexo A presenta los objetivos de control y controles (iso27002). Pretende asegurar los principios de confidencialidad, integridad y disponibilidad de un sistema de información. Presenta una estructura de alto nivel que permite incorporarla con otros sistemas. Se basa en el ciclo PHVA de mejora continua	Permite realizar análisis cuantitativo y cualitativo, evaluación del riesgo, determinación de parámetros de identificación y valoración de activos, propone ejemplos de vulnerabilidades, valoración de activos y amenazas.	Recomendamiento de riesgos y planificación de medidas de control, facilita los procesos de evaluación, auditoría y acreditación. Análisis cualitativo y cuantitativo, estimación de ocurrencia de amenazas, estimación de riesgos. Catálogos de amenazas y medidas de control.	Identificar, relacionar amenazas y vulnerabilidades, divide los activos en Sistemas y Personas	Presenta un su estructura los elementos que intervienen como entradas y salidas para cada una de las actividades durante los procesos de análisis y gestión de riesgos. Identifica factores de riesgo específicos y niveles de aceptación del riesgo. Aseguramiento de sistema de información que almacenan, procesan y transmiten información	Análisis de riesgos en base a elaboración de modelos, entrevistas con expertos, lenguaje gráfico UML, representación XML, guías del proceso, editor gráfico basado en Microsoft Visio, biblioteca de gestión de casos.

Fases / Eta	ISO27001	ISO27005	MAGERIT	OCTAVE	NIST SP800-30	CORAS
	Presenta 114 categorías de control: (Anexo A-ISO27002-2013). Propone 7 cláusulas. Contempla 154 requerimientos, 14 Dominios de seguridad, 35 Objetivos de control.	Seis etapas: 1) Establecimiento del contexto 2) Valoración del riesgo 3) Tratamiento del riesgo 4) Aceptación del riesgo 5) Comunicación del riesgo 6) Monitoreo y revisión	Tres Libros: 1) Método, Metodología detallada, 2) Catálogo de elementos: inventarios de tipos de activos, criterios de valoración, amenazas y salvaguardas. 3) Guías Técnicas: análisis mediante tablas-algoritmo-coste/beneficio, árboles de ataque, diagramas de flujo de datos y otros. Enfoque de riesgos en tres fases: a) Análisis de riesgos, b) Caracterización de activos, c) Gestión de riesgos	Tres Fases: 1) Visión de organización, Activos, Amenazas, Prácticas actuales, Vulnerabilidades organizativas, Requerimientos de seguridad 2) Visión Tecnológica: Componentes clave, Vulnerabilidades técnicas 3) Planificación de las medidas y reducción de riesgos: Riesgos, Estrategia de protección, Planes de mitigación	Fase de análisis de riesgos: 1) Caracterización de sistemas, 2) Identificación de amenazas, 3) Identificación de vulnerabilidades, 4) Análisis de controles, 5) Determinación de probabilidades, 6) Análisis de impacto, 7) Determinación del riesgo, 8) Recomendación de controles, 9) Documentación de resultados Fase de gestión de riesgos: 1) Priorización de acciones, 2) Evaluación de opciones de controles recomendados, 3) Análisis coste-beneficio, 4) Selección de controles, 5) Asignación de responsabilidades, 6) Desarrollo del plan de implantación de salvaguardas, 7) Implantación de controles seleccionados.	Siete pasos: 1) Presentación Objetivos, Alcance, 2) Análisis de alto nivel: Entrevistas, identificación de amenazas, vulnerabilidades, escenarios e incidentes, 3) Aprobación. Detalle de objetivos, alcance y consideraciones, 4) Identificación de riesgos: detalle de amenazas, vulnerabilidades, escenarios e incidentes, 5) Estimación del riesgo: probabilidad e impacto de los incidentes identificados, 6) Evaluación del riesgo: informe de riesgos, 7) Tratamiento del riesgo: salvaguardas y análisis coste-beneficio

	ISO27001	ISO27005	MAGERIT	OCTAVE	NIST SP800-30	CORAS
Vent	La determinación de controles de seguridad existentes, facilita la creación de estrategias de protección, planes de mitigación e integración de sistemas de gestión. Estándar certificable	Estándar internacional, guía para monitorización y revisión de riesgos, contempla los procesos de análisis y gestión de riesgos. Establece parámetros de aceptación del riesgo	Contempla los procesos de análisis y gestión de riesgos. Contiene archivos de inventarios de recursos, información, activos, amenazas. Propone la herramienta PILAR para aplicar la metodología	Autoguiada, considera los procesos de análisis de riesgos y gestión de riesgos, participación de todo el personal, talleres en cada fase, involucra activos, recursos, vulnerabilidades, amenazas, salvaguardas	No requiere permisos de autorización	Facilita el desarrollo de nuevos sistemas de gestión de riesgos, especificación en lenguaje UML, presenta un repositorio de casos reusables, provee un registro de vulnerabilidades detectadas.
Desver	No existen las guías específicas para la definición del alcance, determinación de activos, amenazas, vulnerabilidades, impacto, riesgo. No presenta procesos definidos para la gestión de riesgo, se apoya en la ISO 31000 para la dirección de riesgos y oportunidades. Es una estructura de alto nivel no detallada	No es certificable, no contiene parámetros específicos de valoración de amenazas. Para la implementación no contiene guías técnicas de ayuda.	Los procesos, recursos y vulnerabilidades no están directamente relacionados en el modelo. Requiere complementar el inventario de Políticas de seguridad. Todas valoraciones son traducidas a factores monetarios	No define con exactitud el valor para los activos de información, sobrecarga de documentos anexos en los procesos de análisis de riesgos, profundiza aspectos técnicos, dentro de los objetivos de seguridad no considera el principio de no repudio.	No especifica una herramienta para el análisis y gestión de riesgos	No presenta guías específicas para el tratamiento del riesgo. Requiere de alta inversión con personal calificado durante todo el proceso.

Fuentes: ISO27001 [4], ISO27005 [17], Magerit [21], Octave [49], NISTSP800-30 [23], Coras [43].

Como se indicó en el Capítulo 1 y 2 literal 2.2 sobre la metodología utilizada por centros de investigación de desastres naturales tales como USGS, CTBTO, IRIS, IRD y las entidades de regulación en Ecuador, se determina que la metodología referente es la norma ISO 27001 para el presente estudio y se propone fortalecer esta normativa con otros estándares y metodologías como ISO 27005, Magerit, Octave, NISTSP 800-30, Coras, así como buenas prácticas que permiten puntualizar áreas y procesos específicos relacionados a la Gestión de seguridad de la información de los centros de investigación de desastres naturales en el Ecuador.

2.1.3.1. Presentación de los aspectos más relevantes de las normas, marcos de trabajo y estándares internacionales relacionados a los Centros de Investigación de Desastres Naturales en el Ecuador.

A continuación se presenta un análisis de las normas y metodologías que se abordan en el presente estudio, identificando los aspectos más relevantes que pueden ser adoptados en la determinación del modelo propuesto de Gestión de Seguridad de la Información. Se establece dos parámetros principales para la evaluación de aplicabilidad de las normas y metodologías que se describen en las Tablas 2.4, 2.5, 2.6, 2.7, 2.8 y 2.9. Estos parámetros son:

- **Prioridad.-** Los niveles de prioridad definen una escala (Baja, Moderada, Alta, Muy Alta) que representa la necesidad actual de aplicar ese componente específico de la norma/metodología en los sistemas de información de los centros de investigación.

- **Justificación.-** Representa en términos generales la razón por la que se requiere implementar dicho componente y su área o campo de aplicación en los centros de investigación.

2.1.3.2. Norma ISO 27001:2013:

En la normativa ISO 27001 / ISO 27002, publicada en español como UNE-ISO/IEC 27001:2014 se evidencia 14 componentes (cláusulas A.5 a A.18) relacionados a la conformación de un SGSI que incluyen categorías de seguridad, objetivos de control, controles de seguridad, evaluación/tratamiento del riesgo y guías de implementación, como se indica en la Tabla 2.3.

Tomando como eje de partida del presente estudio que es la Gestión de los datos sísmicos, volcánicos, oceanográficos, meteorológicos y gestión de acceso a los datos y a la información generada; a continuación se presenta los componentes más relevantes de esta normativa. Los resultados obtenidos corresponden a la estructura general del modelo propuesto y sobre el cual se complementará mediante otras normativas que se mencionan más adelante.

La norma ISO 27001:2013 [14] presenta una guía en forma general para la creación y gestión del SGSI, de igual manera para el mantenimiento y mejora del SGSI. El aspecto de mayor importancia en esta norma que se considera en el presente estudio se destaca en la descripción a detalle para el establecimiento de los dominios de seguridad, objetivos de control y controles (Tabla 2.4) que se deberán aplicar en los activos de información de los centros de investigación de desastres naturales.

El proceso total de gestión del SGSI se complementa con la norma ISO 27005:2012 (Tabla 2.5) y otras metodologías de gestión (Tablas: 2.6, 2.7, 2.8 y 2.9) para llegar al Diseño del Modelo de Gestión SGSI Versión 1-1.

Tabla 2.4 Norma ISO 27001: 2013 adaptada a centros de investigación

Componentes / Dominios de Seguridad - ISO/IEC 27001:2013	Prioridad	Justificación
A.5 Políticas de seguridad de la Información	Alta	Políticas a nivel Directivo en seguridad de información para adquisición, almacenamiento, procesamiento de ldatos y gestión de la información en base a la legislación gubernamental y requisitos institucionales
A.6 Organización de la seguridad de la información	Alta	Establecer roles de responsabilidad, coordinación y compromiso que permitan gestionar el SGSI

Componentes / Dominios de Seguridad - ISO/IEC 27001:2013	Prioridad	Justificación
A.7 Seguridad en los recursos humanos	Alta	El personal involucrado en el manejo y acceso de los datos debe conocer y comprender en sus funciones los compromisos para reducir los riesgos de pérdida de información o uso indebido de los datos y el cumplimiento de las políticas de acceso a los mismos.
A.8 Gestión de activos	Muy Alta	Creación de responsables del inventario de activos (datos SVMO) y controles que garanticen la protección adecuada de los activos.
A.9 Control de accesos	Muy Alta	Proporcionar niveles de acceso a la información y datos SVMO, gestionar la autorización o negación de acceso a usuarios a la red, sistemas operativos, aplicaciones, comunicaciones móviles y portátiles. Garantizar la confidencialidad, integridad, disponibilidad de los activos de información.
A.10 Criptografía	Moderada	Establecer políticas de control criptográfico y gestión de claves
A.11 Seguridad física y ambiental	Moderada	Determinar normas de seguridad física y ambiental y controles para prevenir daños en las instalaciones involucradas con los activos de la información, accesos no autorizados, interrupciones o situaciones que afecten los activos (datos SVMO)
A.12 Seguridad en las operaciones	Muy Alta	Implementar un registro para procedimientos de operación de los sistemas de información; gestión de cambios, segmentación de entornos de pruebas, desarrollo y operación, controles de código malicioso, apoyo en auditorías.
A.13 Seguridad en las comunicaciones	Muy Alta	Gestión de la información disponible en las redes, medios, intercambio de información y software.
A.14 Adquisición, desarrollo y mantenimiento de sistemas de información	Alta	Garantizar la seguridad de los procesos de desarrollo y soporte, archivos del sistema, protección de los datos utilizados en pruebas.
A.15 Relación con proveedores	Moderada	Asegurar la protección de activos relacionados con los proveedores de servicios.
A.16 Gestión de incidentes de seguridad de seguridad de la información	Muy Alta	Gestión de incidentes de seguridad, monitoreo, registros, auditorías, detección de vulnerabilidades.
A.17 Administración de la continuidad de negocio	Moderada	Inclusión del SGSI en los procesos de continuidad del negocio y análisis de riesgos, manteniendo actualizaciones del plan de continuidad
A.18 Cumplimiento	Moderada	Asegurar el cumplimiento de obligaciones legales, regulatorias, normas y políticas de seguridad de la organización.

Fuente: Norma ISO/IEC 27001:2013

Elaborado por: Autor

La Tabla 2.3 resume los dominios de la normativa ISO 27001:2013, y se define los niveles de prioridad de aplicación que se requiere analizar en los centros de investigación, con este enfoque general se establecerán los objetivos de control y controles que serán recomendados para el Caso de Estudio.

2.1.3.3. Norma ISO 27005:2012:

La norma NTE INEN-ISO/IEC 27005:2012 es una guía de gestión de riesgos en seguridad de la información [17] y da soporte a la norma ISO 27001 para su implementación. En el caso de estudio se ha considerado las siguientes etapas indicadas en la Tabla 2.5 y se ha definido su prioridad para conformar el modelo SGSI aplicado a centros de investigación de desastres naturales.

Tabla 2.5 Norma NTE INEN-ISO/IEC 27005:2012 adaptada a centros de investigación

Norma ISO 27005:2012	Prioridad	Justificación
1. Establecimiento del contexto	Muy Alta	Se determina los criterios de evaluación, impacto, aceptación del riesgo. Se define el alcance y límites en el centro de investigación, unidad o proceso.
2. Valoración del riesgo	Muy Alta	Esta etapa permite establecer el valor de los activos, realizar el análisis del riesgo, mediante la identificación de activos, amenazas, controles existentes, vulnerabilidades, consecuencias. Con estos resultados se realiza la estimación del riesgo cuantitativa o cualitativa.
3. Evaluación del riesgo	Alta	Se plantean los criterios para determinar si los riesgos son de importancia o tienen impacto sobre un activo. Con ello se presenta un resumen de los riesgos y su prioridad.
4. Tratamiento del riesgo	Alta	Selección de controles para reducir, retener, evitar o transferir los riesgos, para establecer el plan para tratamiento del riesgo.
5. Aceptación del riesgo	Alta	Determina si el riesgo residual está dentro de los parámetros de aceptación. Con ello se obtiene una lista de riesgos que asume el centro de investigación, unidad o proceso.
6. Comunicación del riesgo	Alta	Permite gestionar los riesgos, recolectar información, difundir el plan de tratamiento del riesgo, soporte a la toma de decisiones.
7. Monitorización y revisión del riesgo	Muy Alta	Facilita la identificación de cambios, nuevas amenazas, vulnerabilidades, para mantener actualización en planes y acciones de gestión del riesgo alineado a los criterios de aceptación del riesgo.

Fuente: Norma NTE INEN-ISO/IEC 27005:2012
Elaborado por: Autor

2.1.3.4. Metodología MAGERIT:

Magerit como metodología de análisis y gestión de riesgos de los sistemas de información ha sido considerada en el presente estudio ya que en su estructura detalla el catálogo de elementos y guías técnicas que permitirán fortalecer el modelo SGSI propuesto y adoptar la gramática tipo XML estandarizada para facilitar la actualización de activos. A continuación se presenta en la Tabla 2.6 los aspectos más relevantes que pueden aportar al análisis y gestión de riesgos en los centros de investigación de desastres naturales.

Tabla 2.6 Metodología Magerit adaptada a centros de investigación

Estructura Magerit-V3	Prioridad	Justificación
1. Método		
1.2 Método de análisis de riesgos	Muy Alta	Propuesta que identifica los activos, amenazas, determina el impacto y riesgo potencial, establecer salvaguardas, impacto y riesgo residual,
1.3 Proceso de gestión de riesgos	Muy Alta	Acciones que deben tomarse sobre los riesgos identificados, calificarlos y establecer una prioridad relativa.
1.4 Proyectos de análisis de riesgos	Alta	Establecer roles y funciones, propuesta del proyecto, análisis de riesgos, presentación de resultados e hitos de control.
1.5 Plan de seguridad	Alta	Identificar proyectos de seguridad, realizar la planificación, ejecución y controles de los planes de seguridad
1.6 Desarrollo de sistemas de información	Alta	Análisis de riesgos en el diseño y desarrollo de sistemas de información seguros con enfoque en los activos involucrados como son: datos que manejan, Sw/Hw de desarrollo, comunicaciones, instalaciones y usuarios.
2. Catálogo de Elementos	Muy Alta	Guías para identificar activos y su valoración, amenazas y salvaguardas, tratando de estandarizar (notación XML) los elementos que intervienen durante el análisis de riesgos.
2.1 Tipos de Activos	Alta	
2.1.1 Activos esenciales	Alta	a)Información: datos esenciales para la existencia de la organización, datos de carácter personal, datos clasificados b)Servicios que presta la organización
2.1.2 Arquitectura del sistema	Alta	Definen la arquitectura interna y externa: puntos de acceso, interconexión, proporcionados por externos
2.1.3 Datos/Información	Alta	Ficheros, copias de respaldo, datos de configuración, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad, código fuente, código ejecutable, datos de prueba

Estructura Magerit-V3	Prioridad	Justificación
2.1.4 Claves Criptográficas	Alta	Protección de la información, comunicaciones, soportes de información y certificados de clave pública. (DES, 3-DES, AES, RSA, Diffie-Hellman)
2.1.5 Servicios	Alta	Servicios entregados al público, usuarios internos y externos, anónimos, portal web, correo electrónico, accesos remotos, almacenamiento y transferencia de datos, gestión de identidades y privilegios, PKIs.
2.1.6 Software / Aplicaciones	Alta	Desarrollado por la organización, subcontratado, estándar, navegador web, servidores de: presentación, aplicaciones, correo electrónico, servidores de datos, gestión de bases de datos, ofimática, antivirus, sistemas operativos, gestión de respaldos, gestor de máquinas virtuales
2.1.7 Hardware / Equipo informático	Alta	Soportan los servicios, ejecución de aplicaciones, almacenamiento procesamiento, transmisión.
2.1.8 Redes de comunicaciones	Alta	Conforman los medios de transporte de datos
2.1.9 Soportes de información	Alta	Permiten el almacenamiento permanente de información
2.1.10 Equipo auxiliar	Alta	Equipos de soporte a los sistemas de información
2.1.11 Instalaciones	Alta	Espacios físicos donde se encuentran los sistemas de información y comunicaciones
2.1.12 Personal	Alta	Usuarios internos y externos, operadores, administradores, desarrolladores, programadores, proveedores.
2.2 Dimensiones de valoración	Alta	Propiedad de un activo de información desde las perspectivas de: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
2.3 Criterios de Valoración	Alta	Establecer escalas de valores estándar que pueden ser cualitativas o cuantitativas.
2.4 Amenazas	Alta	Catálogo de amenazas asociadas a tipos de activos que pueden ser afectados y sus dimensiones, descripción de la amenaza, su origen y efectos producidos. Ejm: Daños por incendio, agua, desastres industriales, contaminación mecánica – electromagnética.

Estructura Magerit-V3	Prioridad	Justificación
2.4 Amenazas	Alta	Ejm: Daños por incendio, agua, desastres industriales, contaminación mecánica – electromagnética, avería de origen físico/lógico, corte de suministro eléctrico, deficiencias de temperatura y humedad, fallos de servicios de comunicaciones, interrupción de otros servicios y suministros, degradación de soportes de almacenamiento de información, errores no intencionados de los usuarios internos / externos y deficiencias, difusión de software dañino, errores de enrutamiento / secuencia, alteración accidental de información, destrucción y fugas de la información, vulnerabilidades de los programas, errores de mantenimiento de Hw/Sw, caída del sistema, pérdida de equipos, indisponibilidad del personal, ataques intencionados, correlación de errores y ataques, nuevas amenazas.
2.5 Salvaguardas	Alta	Permite una clasificación y ordenamiento de las salvaguardas siguientes: protecciones generales, protecciones de datos, de claves criptográficas, de servicios, de Hw y Sw, de comunicaciones, interconexiones, soportes de información, elementos auxiliares, de las instalaciones, relacionadas al personal, de tipo organizativo, de continuidad de operaciones, externalización, adquisición y desarrollo.
3. Guías Técnicas	Moderada	Permiten el análisis de riesgos mediante técnicas generales y específicas
3.1 Tablas	Muy Alta	Métodos simples para identificar la importancia relativa de los activos expuestos a amenazas, magnitud de impacto y magnitud del riesgo
3.2 Técnicas algorítmicas	Moderada	Análisis deductivo
3.3 Árboles de ataque	Moderada	Técnicas que modelan cómo un sistema puede ser atacado de distintas formas e identificar las salvaguardas necesarias.
3.4 Análisis coste-beneficio	Moderada	Medición de costos de realización de un proyecto SGSI frente a beneficios esperados
3.5 Técnicas gráficas	Moderada	Diagramas de Gantt, puntos y líneas, tarta, barras, radar, Pareto
3.6 Valoración Delphi	Moderada	Identificar problemas y desarrollar estrategias de solución, identificar factores de resistencia al proceso de cambio, evaluación de tendencias.
3.7 Sesiones de Trabajo	Moderada	Entrevistas, reuniones, presentaciones, referencias que facilitan la participación e intercambio de información, resultados y optimización de esfuerzos.
3.8 Planificación de Proyectos	Moderada	Modelamiento, estimación de tiempos de realización, análisis de cambios.

Fuente: Magerit_V3, Libro 1 [21].

Elaborado por: Autor

2.1.3.5. Metodología OCTAVE-S:

Octave-S es una metodología de evaluación de riesgos en seguridad de la información, su estructura en tres fases contempla los aspectos organizacionales, tecnológicos y planes estratégicos de seguridad. En cada fase se establecen procesos, talleres, participantes, personal de evaluación coordinación y documentación. Para el presente estudio se ha considerado los elementos más relevantes en función de las necesidades de los centros de investigación.

Tabla 2.7 Metodología Octave- S adaptada a centros de investigación

Metodología Octave	Prioridad	Justificación
FASE DE PREPARACION	Muy Alta	Obtener el patrocinio de la alta dirección, selección de áreas operativas, participantes, conformar el equipo de análisis y coordinadores, definición del alcance de la evaluación
FASE 1: Visión organizativa	Alta	Construir perfiles de amenaza basada en activos
1.1 Identificar los conocimientos de la alta dirección	Moderada	Identificar los activos de mayor prioridad (5). Identificar las áreas de práctica por activo crítico de OCTAVE. Crear los requerimientos de seguridad: confidencialidad, integridad, disponibilidad, Determinar el impacto posible. Analizar las prácticas actuales de seguridad.
1.2 Identificar el conocimiento de la zona de gestión operacional	Moderada	
1.3 Identificar los conocimientos del personal	Alta	
1.4 Crear Perfiles de Amenaza	Alta	Consolidar los resultados obtenidos en los procesos 1.1 a 1.3 Identificación y categorización de amenazas Determinar la probabilidad de ocurrencia de una amenaza
FASE 2: Visión tecnológica	Muy Alta	Identificar vulnerabilidades en la infraestructura
2.1 Identificar componentes clave	Alta	Identificar en la infraestructura los componentes de red, acceso, almacenamiento de la información asociados a los activos críticos.
2.2 Evaluación de los componentes	Muy Alta	Evaluación de la vulnerabilidad, establecimiento del nivel de protección para cada activo crítico
FASE 3: Estrategia y desarrollo del plan	Muy Alta	Desarrollar estrategias y planes de seguridad
3.1 Identificar y analizar riesgos	Muy Alta	Evaluar el impacto de las amenazas. Establecer los criterios de evaluación de riesgos. Establecer criterios de evaluación de probabilidad de amenazas a los activos críticos
3.2 Desarrollar estrategias de protección y planes de mitigación	Muy Alta	Establecer estrategias de protección y mitigación para las áreas de práctica OCTAVE. Crear planes de mitigación

		Seleccionar enfoques de mitigación para cada riesgo. Proponer la estrategia de protección, planes de mitigación y una lista de acciones y ciclos de evaluación.

Fuente: Metodología OCTAVE
Elaborado por: Autor

2.1.3.6. Metodología NIST SP800-30:

Esta metodología es dirigida principalmente a la evaluación de riesgos, por lo que se ha considerado varios aspectos de su estructura para la identificación de amenazas y vulnerabilidades en los centros de investigación de desastres naturales. En la siguiente Tabla 2.8 se mencionan las etapas de NIST 800-30 y el grado de aplicabilidad en el presente estudio.

Tabla 2.8 Metodología NIST SP800-30 adaptada a centros de investigación

Etapas de Evaluación de Riesgos NIST 800-30	Prioridad	Justificación
1.- Valoración de Riesgos	Muy Alta	Permite identificar los riesgos que afecten a los activos de información en base a las amenazas.
1.1 Caracterización del sistema	Muy Alta	Determinar el alcance del sistema, funciones y límites del proceso.
1.2 Identificación de amenazas	Muy Alta	Define las fuentes potenciales de amenazas y vulnerabilidades, identifica los controles existentes.
1.3 Identificación de vulnerabilidades	Muy Alta	Lista de vulnerabilidades y amenazas reales que resultan de test de seguridad, búsquedas de posibles vulnerabilidades
1.4 Análisis de controles	Alta	Lista de controles actuales y generación de controles a implantarse que reducen las vulnerabilidades
1.5 Determinación de probabilidades	Alta	Clasificación de probabilidades de ocurrencia de amenazas potenciales y existentes
1.6 Análisis de Impacto	Alta	Clasificación que determina el nivel de impacto de una vulnerabilidad respecto a la pérdida de confidencialidad, integridad, disponibilidad.
1.7 Determinación del riesgo	Muy Alta	Niveles de riesgo en función de la probabilidad de amenaza, grado de impacto y efectividad de los controles

Etapas de Evaluación de Riesgos NIST 800-30	Prioridad	Justificación
1.8 Recomendación de controles	Alta	Recomendaciones en base a la efectividad del control, impacto en los procesos operacionales, cumplimientos regulatorios y políticas.
1.9 Documentación de resultados	Alta	Informe de valoración de riesgos
2.- Mitigación de Riesgos	Alta	Procesos para mitigar los riesgos, establecimiento de controles, costos asociados a su implementación y seguimiento de riesgos residuales.
2.1 Alternativas para la mitigación de riesgos	Moderada	Posibles acciones para la mitigación del riesgo que pueden ser: Admisión, prevención, limitación, planeación, reconocimiento e investigación, transferencia del riesgo.
2.2 Estrategia de mitigación de riesgos	Moderada	Define las acciones que deben tomarse para cada caso donde se ha identificado una amenaza y vulnerabilidad
2.3 Enfoque para implementación de controles	Alta	Contempla 7 etapas: Priorización de acciones, Evaluación de opciones de controles recomendados, Análisis coste-beneficio, Selección de controles, Asignación de responsabilidades, Desarrollo de un plan de implantación de salvaguardas, Implantación de controles seleccionados.
2.4 Categorización de controles	Moderada	Clasificación de controles en función de las áreas o ambientes que pueden ser: operativos, administrativos, técnicos, desarrollo e investigación.
2.5 Análisis costo – beneficio	Moderada	Contempla el impacto de la aplicación de controles y los costos de implementación frente a la criticidad del sistema y los datos
2.6 Riesgos residuales	Alta	Seguimiento a los resultados obtenidos de controles implementados que han minimizado el impacto de los riesgos

Fuente: Metodología NIST 800-30
Elaborado por: Autor

2.1.3.7. Metodología de CORAS:

La metodología de análisis de riesgos de seguridad utiliza el lenguaje gráfico UML y representación XML, un editor gráfico en base a Microsoft Visio, activa participación de expertos durante todo el proceso que consta de ocho etapas, presenta una biblioteca de casos, herramientas de gestión y formatos de comunicación durante el análisis de riesgos. En el presente estudio se ha considerado varios aspectos del lenguaje que se utiliza en esta metodología con el

objetivo de adoptar una nomenclatura estándar, mantener registros de casos reutilizables de modo que facilite el uso de futuras aplicaciones que automaticen los procesos de gestión de seguridad de la información en estos centros de investigación.

Tabla 2.9 Metodología Coras adaptada a centros de investigación

Etapas del Método CORAS	Prioridad	Justificación
1. Preparación del análisis de riesgos	Muy Alta	Definir los objetivos y alcance del análisis, establecer requerimientos indispensables para el análisis real
2. Presentación	Muy Alta	Presentar objetivos, alcance, método a utilizar en el análisis, metas, sistema a analizar. Planificación de reuniones y talleres de trabajo
3. Preparación para el Análisis	Alta	Presentar los avances y comprensión del estudio por parte del equipo de análisis. Identificar los activos de mayor prioridad frente a escenarios de amenazas, vulnerabilidades y riesgos.
4. Establecimiento del contexto	Alta	Revisión de objetivos, enfoque y metodología para su aprobación. Definir los criterios de evaluación de riesgo para cada activo y escalas de ocurrencia y efectos
5. Identificación de riesgos	Muy Alta	Utilización del método Brainstorming en talleres guiados por el equipo de análisis para identificar los riesgos desde varias perspectivas que implica amenazas, incidentes, vulnerabilidades, utilizando el lenguaje y diagramas de amenaza de CORAS
6. Estimación de riesgo	Muy Alta	Identificar los niveles de riesgo en incidentes no deseados, documentarlos mediante el diagrama de amenazas, estimar la probabilidad de ocurrencia de cada incidente no deseado y el impacto en los activos involucrados
7. Evaluación del riesgo	Muy Alta	Evaluar los riesgos identificados si son aceptables, estimar los riesgos en activos indirectos
8. Tratamiento del riesgo	Muy Alta	Identificar y analizar los procedimientos a realizarse para reducir la probabilidad de ocurrencia de incidentes no deseados y estimar el costo-beneficio para cada tratamiento.

Fuente: Metodología CORAS
Elaborado por: Autor

2.1.4. Identificación de procesos y servicios críticos de los centros de investigación

Para el presente estudio, se han considerado los productos y servicios más relevantes de los centros de investigación; en el Anexo D (Productos y servicios de los centros de investigación) se debe establecer su nivel de criticidad o relevancia, de donde se ha obtenido que las tareas más notables están relacionadas a la Gestión de los Datos sísmicos, volcánicos, meteorológicos, oceanográficos, así también la Gestión de Acceso a la Información generada como resultado de la interpretación de estos datos. La siguiente Tabla 2.10, presenta un resumen de los productos y servicios de mayor relevancia, de acuerdo a los criterios y opiniones recibidas por el personal de TI de los centros de investigación:

Tabla 2.10 Productos y Servicios de los Centros de investigación más relevantes

Área / Departamento	Componente	Productos y Servicios	Relevancia de Activos
INSTITUTO GEOFISICO - IG			
Sistemas	Redes y Comunicaciones	Gestión de la infraestructura de Red y Arquitectura	Muy Alta
		Administración de la red	Muy Alta
		Gestión de Tecnologías Web (correo electrónico, páginas web, intranet, motores de búsqueda)	Muy Alta
	Bases de Datos	Adquisición de Datos y Procesamiento	Muy Alta
	Coordinación	Gestión de Información Documental	Muy Alta
		Gestión de Datos y Documentos del Centro de Datos	Muy Alta
		Gestión de Seguridad de la Información	Muy Alta
Instrumentación	Instalación y Mantenimiento	Operación de Redes de Telecomunicaciones - REPET	Muy Alta
		Operación de Redes de monitoreo sísmico y volcánico	Muy Alta
		Gestión de Redes de Comunicaciones	Muy Alta
		Gestión de Adquisición de Datos	Muy Alta
Sismología	Vigilancia	Operación del Centro de Procesamiento, Información y Alerta Volcánica y Sísmica - TERRAS	Muy Alta
		Tratamiento de señales	Muy Alta
		Vigilancia con cámaras de la Red virtual de observatorios volcanológicos	Muy Alta
		Provisión de información en tiempo real de la actividad sísmica y volcánica actual	Muy Alta
	Coordinación	Coordinación de actividades del Centro TERRAS	Muy Alta
		Gestión de datos para adquisición y procesamiento	Muy Alta
		Gestión de la información sísmica y volcánica	Muy Alta

Área / Departamento	Componente	Productos y Servicios	Relevancia de Activos
		Generación de sistemas de alerta temprana frente a fenómenos naturales	Muy Alta
Vulcanología	Monitoreo	Operación del Observatorios volcanológicos - ROVIG	Muy Alta
		Monitoreo de datos de la Red Geodésica RENGEO	Muy Alta
		Monitoreo de datos de la red de monitoreo geoquímico	Muy Alta
	Coordinación	Gestión de la información para procesamiento e interpretación de datos geoquímicos	Muy Alta
		Generación de sistemas de alerta temprana frente a fenómenos naturales.	Muy Alta
INSTITUTO NACIONAL DE METEOROLOGÍA E HIDROLOGÍA - INAMHI			
Información Hidrometeorológica	Recopilación de Información	Recopilación e interpretación de datos de Estaciones Meteorológicas	Muy Alta
		Recopilación e interpretación de datos de Estaciones Hidrológicas	Muy Alta
		Elaboración de Informes	Muy Alta
	Coordinación	Informes diarios y mensuales meteorológicos	Muy Alta
		Datos para informes diarios de hidrología	Muy Alta
	Difusión de la información	En herramientas web	Muy Alta
		Información en tiempo real automáticas y convencionales	Muy Alta
Pronóstico Y Alertas Hidrometeorológicas	Vigilancia	Operación del Centro de Procesamiento, Información y alertas hidrometeorológicas	Muy Alta
		Tratamiento de señales	Muy Alta
		Provisión de información en tiempo real de la actividad diaria meteorológica e hídrica	Muy Alta
		Generación oportuna de alertas en coordinación con la SGR	Muy Alta
	Pronóstico	Elaboración de pronósticos diarios y mensuales de meteorología	Muy Alta
		Elaboración de pronósticos diarios y mensuales de hidrología	Muy Alta
		Evaluación de la vulnerabilidad ante eventos hidrometereológicas importantes	Muy Alta
	Coordinación	Generación de avisos en forma temprana frente a fenómenos naturales	Muy Alta
	Estadísticas	Generación de estadísticas diarias meteorológicas	Muy Alta
	Avisos, boletines y alertas	Boletines Meteorológicos, Climáticos, Agroclimáticos e Hidrológicos	Muy Alta
		Avisos Meteorológicos, Climáticos, Agroclimáticos e Hidrológicos	Muy Alta
		Alertas Meteorológicos, Climáticos, Agroclimáticos e Hidrológicos	Muy Alta
INSTITUTO NACIONAL DE OCEANOGRAFÍA DE LA ARMADA - INOCAR			
Hidrografía	División y Levantamientos	Levantamientos geodésicos y de perfiles de playa	Muy Alta
		Levantamientos hidrográficos	Muy Alta
		Levantamientos topográficos	Muy Alta
		Levantamientos barimétricos	Muy Alta
	División Cartográfica	Procesamiento digital y georeferencial de Imágenes	Muy Alta
		Estructuración de información cartográfica y depuración	Muy Alta
Ayudas a la Navegación	Coordinación	Gestión de datos para adquisición y procesamiento	Muy Alta

Área / Departamento	Componente	Productos y Servicios	Relevancia de Activos
		Generación de sistemas de alerta	Muy Alta
Ciencias Del Mar	División Meteorología	Adquisición de datos y parámetros meteorológicos	Muy Alta
		Procesamiento de datos históricos y actuales de parámetros meteorológicos	Muy Alta
		Estudios climatológicos y pronósticos costeros	Muy Alta
	División de Tsunamis	Protocolo de comunicación interno del Centro Nacional de Alerta de Tsunamis	Muy Alta
		Colaboración JICA	Muy Alta
	Centros de Investigaciones Marinas	Centro de Investigación Galápagos	Muy Alta
		Centro de Investigación La Libertad	Muy Alta
		Centro de Investigación Esmeraldas	Muy Alta

Fuente: Anexo D
Elaborado por: Autor

Para el caso de los procesos y áreas no contempladas en el estudio, se considera en términos generales el método y políticas que deben aplicarse, ya que son procesos complementarios para el presente estudio.

2.2. Definición del Alcance y Límites del Modelo de Gestión

El análisis comparativo ha permitido identificar los requerimientos en seguridad de la información de los centros de investigación frente a los controles y objetivos de control de seguridad de la normativa ISO 27001, ISO 27005 y metodologías de gestión de riesgos MAGERIT, OCTAVE, NISTSP800-30, CORAS.

Los centros de investigación son instituciones que pueden variar en su volumen de activos físicos y lógicos, volumen de información, usuarios internos y externos; sin embargo, en su estructura interna (Figura 1.4) puede tomar áreas o campos de acción similares, las vulnerabilidades en los activos críticos pueden afectar directamente la entrega de la información que es su principal producto/servicio.

En segunda instancia, si la decisión de los Directivos en conjunto con el Comité de Seguridad de la Información es atender a las necesidades de seguridad de la información de otras áreas de cada institución, se definirá de manera progresiva el alcance, límites y se aplicarán las etapas del modelo propuesto hasta lograr el

acoplamiento del modelo como tal, y conseguir implementarlo en toda la organización.

2.2.1. Alcance del Modelo de SGSI propuesto:

El modelo de SGSI propuesto se enfocará en establecer lineamientos de gestión de seguridad de la información mediante un análisis a los Sistemas de Información de estos centros de investigación a nivel de topología de red y componentes tecnológicos; tomando en consideración que el estudio debe comprender desde el origen de generación de datos, medios de transporte de datos, adquisición, procesamiento, análisis de datos, presentación de resultados e informes y respaldos, obteniendo como beneficio la identificación de activos, evaluaciones y recomendaciones de seguridad, políticas, controles de acceso físico y lógico en las áreas de: administración de la red e infraestructura física, áreas técnicas y administrativas, dentro de un marco de gestión de seguridad de la información basado en normas internacionales y metodologías de gestión de riesgos que permita articular y sintetizar un modelo específico aplicado a la infraestructura y prácticas del componente humano.

2.2.2. Límites del Modelo SGSI propuesto:

El entorno del modelo SGSI se limita a analizar y evaluar cualitativamente la seguridad de la información en estos centros de investigación; su aplicación en un caso práctico está sujeta al avance y cumplimiento de las etapas del modelo, el mismo que debe ser gestionado a través del comité de seguridad de la información y los directivos quienes revisan y autorizan la ejecución de cada etapa.

El modelo servirá para alinear la gestión de seguridad de información y requerirá de mayor afinamiento para llevarlo a procesos específicos y actividades que se desenvuelvan en las áreas de TI, considerando las demandas tecnológicas y reformas en la estructura organizacional.

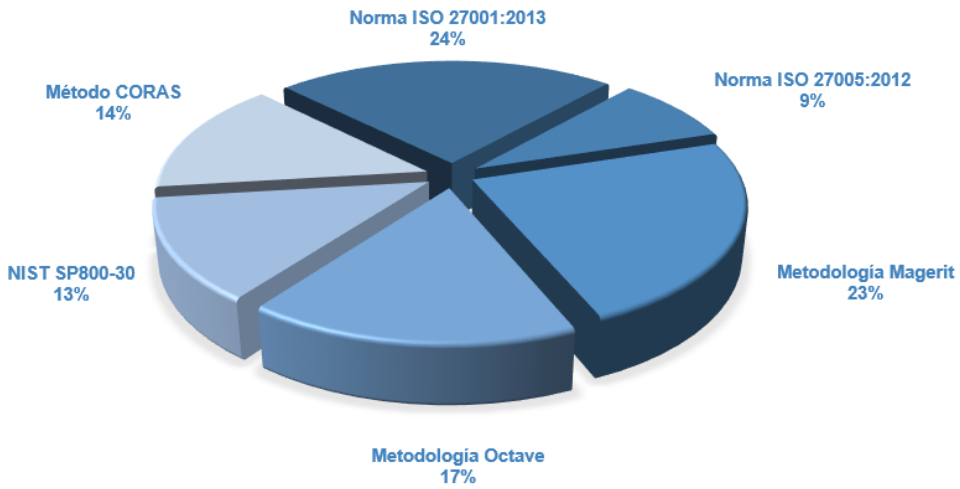
2.3. Diseño del Modelo de Gestión

EL modelo propuesto está desarrollado para cubrir los requerimientos de los centros de investigación basándose en el estándar ISO 27001 y otras metodologías de gestión de riesgos de seguridad de la información. Una vez ejecutado el modelo puede ser auditado y facilitará los procesos de certificación de la norma ISO 27001 si es de interés en la institución.

Para establecer el modelo de gestión de seguridad SGSI_Versión 1-1, se ha tomado como referencia el proceso de implementación de la norma ISO 27001:2013 [14], ISO 27005:2012 [17], así también varias propuestas para gestión de seguridad de la información [15], [33], [34]. De donde se ha tomado los aspectos más representativos y que pueden adoptarse en los centros de investigación de desastres naturales.

La Figura 2.3 representa las normas y metodologías utilizadas para conformar el Modelo de Gestión SGSI propuesto, donde se enfatiza como principal referencia a la norma ISO 27001 de acuerdo al Literal 2.2 sobre la selección de normas, marcos de trabajo y estándares internacionales.

Figura 2.3 Normas y Metodologías utilizadas en el Modelo SGSI propuesto



Fuente: El Autor. Representación gráfica - Anexo F

2.3.1. Etapa 1.- Fase de Preparación

Esta etapa ha sido construida en base a los fundamentos encontrados en las metodologías OCTAVE (Fase de Preparación, Visión Tecnológica – Componentes Clave), norma ISO 27001:2013 (Contexto de la organización, Liderazgo, Planificación) y MAGERIT (Método - Proyecto de análisis de riesgos). Como resultados se han definido los siguientes componentes:

2.3.1.1. Sistematización del problema:

Este componente ha sido desarrollado en el Capítulo I, literales 1.1 y 1.2; corresponde al análisis de la situación actual en seguridad de la información del centro de investigación; se ha establecido los objetivos y necesidades de la institución o unidad / área; se identifican los servicios comunes que presta en relación al sistema de seguridad de la información sobre el cual se aplicará el modelo de gestión SGSI; con ello, se identifican los procesos fundamentales y críticos que deberán ser gestionados en el ámbito de seguridad de la información y se estructura la propuesta de implementación del Modelo SGSI que se desarrollará en las siguientes etapas.

2.3.1.2. Obtener el apoyo de la Dirección:

En esta fase se plantean los aspectos fundamentales para la implementación del modelo SGSI. Los Directivos en cada Centro de Investigación deberán conocer formalmente la propuesta de implementación del modelo de SGSI, mediante un resumen ejecutivo que contemple la situación actual de la organización frente a los beneficios de la aplicación del modelo, así como los requerimientos tecnológicos y administrativos, costos, tiempos de implementación, ejecución y ciclos de mejora continua. El compromiso por parte de la Dirección en aprobar formalmente y respaldar la ejecución del modelo será de vital importancia para conseguir los objetivos planteados.

2.3.1.3. Compromiso y liderazgo en la organización:

Dentro de la estructura de estos centros de investigación se debe identificar las responsabilidades y funciones que deben asumirse a nivel directivo, estratégico, táctico y operacional; se debe asignar personal con funciones exclusivas que integre el equipo de seguridad de la información. La identificación de los roles, ejecución y su seguimiento, permitirá implementar el modelo SGSI y aplicar las acciones de mejoramiento continuo acorde a la demanda de seguridad. Es importante señalar que todo el personal participará de forma directa o indirecta para conseguir los objetivos de seguridad de la información.

La Figura 2.4, presenta la estructura organizacional y los niveles de responsabilidad desde el enfoque de seguridad de la información.

Figura 2.4 Estructura organizativa en forma piramidal

Fuente: Sistema de gestión de la seguridad de la información. UOC [16]

2.3.1.4. Definición de roles, responsabilidades y autoridades:

A continuación se define las funciones que deberá asumir el personal que forma parte del equipo de Seguridad de la Información, tomando como referencia la norma ISO 27001:2013 (Liderazgo, Objetivos de Control A.6 y A.7) y la metodología OCTAVE (Fase de Preparación):

- **Comité de Seguridad de la información:** Está conformado por representantes de las áreas de TI, área administrativa, y el oficial de seguridad de la información. Representan el principal medio de comunicación con la Alta Dirección y presentan las propuestas, avances y requerimientos del sistema de gestión de seguridad de la información del Centro de Investigación.
- **Promotor:** Un "promotor" no participa activamente en el mismo, interviene si el proyecto está paralizado. El gerente del proyecto debe informar regularmente al promotor del proyecto acerca del estado del mismo;
- **Coordinador:** La función es coordinar, garantizar la implementación ininterrumpida del SGSI dentro de los plazos establecidos y los recursos necesarios para la implementación, informar al promotor y altos directivos sobre el progreso del SGSI, realizar trabajos administrativos relacionados con el mismo.
- **Equipo de análisis**: Impulsar las acciones asociadas a la gestión de la seguridad de la información, se encarga de asignar personal para la conformación de equipos de trabajo multidisciplinarios, personal de documentación y formación. Establece el cronograma de trabajo del modelo SGSI. Análisis del riesgo, priorización, aceptación y tratamiento.
- **Equipo de seguridad de la información:** La función es ayudar en la implementación del SGSI, ejecutar tareas preestablecidas y aportar en la toma decisiones que requieren un enfoque multidisciplinario.
- **Administrador:** Es el responsable del activo/información y procesos relacionados, así como gestionar los avances, evaluaciones, reportes y cambios. Se encarga de determinar el nivel de seguridad de la información del activo.
- **Analista de seguridad del sistema:** La función es monitorizar las acciones de seguridad en el sistema de información, gestión y configuración de hardware y software, evaluación de medidas de seguridad del sistema y propuesta de cambios.
- **Personal técnico**: La función es el manejo de la información, administración de activos de información e implementación de soluciones de TI.

Utilizando el esquema de la matriz RACI (Responsible, Accountable, Consulted, Informed), se propone en la Tabla 2.11 la asignación de funciones del personal y responsabilidades para los activos de la organización.

Tabla 2.11 Asignación de funciones del personal y responsabilidades para los activos de la organización, utilizando matriz RACI

ACTIVO	FUNCIONES	RESPONSIBLE (Autoridad)	ACCOUNTABLE (Responsable)	CONSULTED (Consultor)	INFORMED (Participante)
		Administrador	Coordinador	Promotor	Son las partes interesadas en el avance

Fuente: Magerit [21]

2.3.1.5. Planteamiento de recursos y competencias:

Se refiere a los recursos necesarios para la implementación del SGSI sean económicos, recursos humanos, tecnológicos. De esta manera se puede identificar los siguientes:

- *Recurso Humano*: Personal que conforma el equipo de seguridad de la información, que puede ser contratado o asignado por la organización propiamente, con el fin de garantizar el cumplimiento de SGSI

- *Tecnológico:* Comprende el Hardware y Software necesarios para el desarrollo del SGSI, auditoría, test de vulnerabilidades e incidentes.

- *Económico:* Contempla los costos de implantación del SGSI, costos asociados a la capacitación y concientización del personal en el área de seguridad de la información, costos asociados a la contratación de personal para el tratamiento y gestión de la información, o contratación del servicio externo. También se contempla los costos adicionales de certificación de la normativa ISO_27001.

Se debe considerar que cuando se especifica el planteamiento de recursos y competencias, están relacionados al alcance del SGSI

2.3.1.6. Identificar los requerimientos:

A continuación se presentan los requerimientos que demandan los centros de investigación:

- *Requerimientos legales, normativos y contractuales:* Los centros de investigación deberán establecer sus requerimientos mediante acuerdos de aplicación de las leyes vigentes asociadas a la seguridad de la información en el Ecuador como se indicó en los literales 2.1 a 2.3. Se analizarán las políticas aplicadas por centros de investigación internacionales como referentes para fortalecer las normas locales. Así también cada centro de investigación podrá adoptar el modelo SGSI propuesto, establecer auditorias con el fin de dar cumplimiento a los objetivos propuestos

- *Programas de capacitación y conocimiento del SGSI:*

    - Programar sesiones para capacitación a todos los empleados en el nivel de las habilidades necesarias y participación que tengan dentro del SGSI. (Objetivo de Control A.8.2.2, norma ISO 27001)

    - Conformar eventos de concientización a terceros involucrados con los servicios de los centros de investigación y la importancia de mantener el SGSI

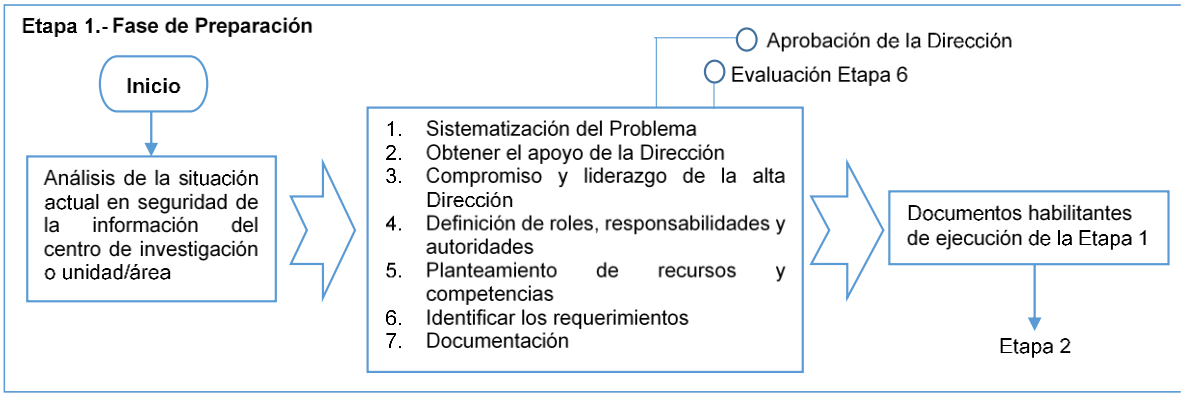
2.3.1.7. Documentación – Etapa 1: Entregables

A continuación se propone a manera de resumen los documentos habilitantes que servirán de respaldo a los resultados obtenidos en esta primera fase , los cuales deberán formalizarse por el Comité de Seguridad de la Información y serán sujetos a las actualizaciones que demande el proceso de mejoramiento continuo. Estos documentos se obtienen del desarrollo de la Etapa 1 y en referencia al control de documentos que presenta la norma ISO 27001 y documentación Magerit – Método.

- Propuesta de implementación – Resumen Ejecutivo.
- Acta de compromiso de la alta Dirección.
- Conformación del equipo de seguridad de la información.
- Asignación de responsabilidades a nivel directivo, estratégico, táctico y operacional.
- Sustento legal, normativas y políticas gobernantes actuales.
- Programa de capacitación y conocimiento del SGSI.

En la siguiente Figura 2.5 se representa los componentes de la Etapa 1:

Figura 2.5 Esquema de la Etapa 1



Fuente: El Autor

2.3.2. Etapa 2.- Establecimiento del Modelo de Gestión de Seguridad de la Información

Esta etapa ha sido construida en base a los fundamentos encontrados en la norma ISO 27001:2013 (Contexto de la organización, Planificación, Operación, Anexo A: Políticas de Seguridad de la Información), norma ISO 27005:2012 (Establecimiento del Contexto), NIST SP800-30 (Caracterización del sistema) y método CORAS (Preparación del análisis de riesgos, Presentación, Establecimiento del contexto).

Como resultados se han definido los siguientes componentes:

2.3.2.1. Definición del Alcance y Límites:

A continuación se presenta los lineamientos requeridos para definir el alcance general y las limitaciones del modelo de Gestión de Seguridad de la Información para Centros de Investigación, Diagnóstico y Prevención de Desastres Naturales.

- **Guía para establecer el Alcance del SGSI:** El Alcance (definido en el literal 2.5.1) pretende identificar la extensión o campo de acción del SGSI propuesto, activos y actores que deben intervenir en el proceso, en función de la situación actual de los centros de investigación, los recursos que disponen y los requerimientos en el área de seguridad de la información.

- **Guía para establecer los Límites del SGSI:** Los límites del SGSI (indicados en el literal 2.5.2) se refieren al tipo de análisis y evaluación que se desarrollará en los activos de información, así como el nivel de detalle en los campos tecnológico y organizativo del SGSI propuesto. En este componente se determina si el SGSI se aplicará en toda la organización o en alguna unidad, área, proceso o proyecto.

2.3.2.2. Desarrollo de la política de seguridad de la información:

La Política de seguridad de la información es el documento que permite a la Dirección controlar la gestión de la seguridad de la información sujetándose a los requerimientos legales, regulatorios y contractuales; contiene la normativa interna de la institución para el uso de los activos, acciones en caso de presentarse incidentes de seguridad, compromisos por parte de los directivos (ISO 27001), acciones para la gestión de los sistemas de información; así también contiene el marco regulatorio vigente en el Ecuador mencionado en el literal 2.1.1, y otras políticas complementarias referentes de los centros de investigación internacionales mencionadas en el literal 2.2.2

Las políticas definidas deben ser de conocimiento y aplicación de todo el personal en cada centro de investigación. Se ha clasificado en: políticas generales, políticas

para el personal, políticas de seguridad de red e infraestructura, políticas de seguridad de hardware y software.

- **Políticas generales**: Comprenden el marco legal vigente en el Ecuador, y las políticas complementarias que mantienen los centros de investigación internacionales.
- **Políticas para el personal:** Se especifican las responsabilidades del personal que conforma el equipo de seguridad de la información descrito en el literal anterior (Definición de roles, responsabilidades y autoridades) y los efectos que conllevaría si existe incumplimiento de los roles asignados.
- **Políticas de seguridad de red e infraestructura:** Se refieren a las acciones que deben implementarse para reducir el acceso no autorizado a los sistemas de información e infraestructura.
    - *Seguridad de la Infraestructura*: Establecer procedimientos, mecanismos de control y personal de seguridad para restringir el acceso a áreas específicas como son: Centro de Datos, Centro de Monitoreo, Área de infraestructura de las telecomunicaciones, Laboratorios de pruebas y desarrollo, Bodegas, Otras áreas. El personal autorizado tendrá acceso a las áreas mencionadas y debe implementarse un registro (cámaras de vigilancia, tarjeta magnética) que facilite el seguimiento de ingreso/salida, actividades realizadas y tiempo de permanencia.
    - *Seguridad de red*: Mejorar las operaciones de monitorización de seguridad de la red, mediante procedimientos y herramientas complementarias que faciliten la gestión de la red, solución de problemas de la red de comunicaciones, auditoría de seguridad, disponibilidad de servidores y servicios, desarrollo de protocolos y autenticación de archivos.
- **Políticas de seguridad de hardware:** Mantener los registros actualizados del hardware que se utiliza en los centros de investigación, determinar su estado de funcionamiento y los cambios realizados. Generar informes de anomalías detectadas y reportarlas al personal encargado de análisis de seguridad del sistema.

- **Políticas de seguridad de software:** Consiste en controlar el software utilizado en los centros de investigación, verificar que no se utilice software y aplicaciones que atente a la seguridad de la información, definir políticas y gestionar permisos de usuario. Generar informes de uso de software, aplicaciones y reportes al personal de seguridad de la información.

2.3.2.3. Definición de la metodología de gestión del riesgo:

Para el estudio propuesto la metodología de gestión de riesgos está desarrollada en dos fases: 1) Identificación de los riesgos y 2) Gestión de los riesgos, tomando como referencia las metodologías Magerit, Octave, NISTSP 800-30, Coras y la norma ISO 27005. Como resultado del estudio comparativo de estas metodologías presentado en el literal 2.3.1 y en el Anexo F, se ha determinado la estructura de la metodología de gestión de riesgos para los centros de investigación y que se indica a continuación:

Tabla 2.12 Metodología de gestión de riesgos aplicable a los centros de investigación de desastres naturales

Metodología de Gestión de Riesgos		
	Identificación y valoración de activos	
	Identificación y valoración de amenazas	
	Identificación de vulnerabilidades	
	Identificación de Controles existentes	
	Valoración de impactos	
	Valoración de riesgos	
	Tratamiento de riesgos	
	Selección de objetivos de control y controles	
	Implementación de controles	
	Aceptación del riesgo y riesgo residual	
	Estrategia de protección y Plan de mitigación	
	Declaración de aplicabilidad	
	Comunicación del riesgo	
	Monitorización y Revisión del riesgo	

Fuente: Norma ISO 27005:2012, NIST SP800-30 [23], Magerit [20] [21], Anexo F.

2.3.2.4. Definición de los componentes de gestión de seguridad de la información:

Dentro de la estructura del modelo SGSI propuesto, para lograr gestionar la seguridad de la información de manera sistemática se requiere de los objetivos de control y controles establecidos por la norma ISO 27001:2013, para consolidar el ciclo de mejora continua y realimentar los procesos de gestión de seguridad de la información para los centros de investigación. Esta fase permitirá ampliar los requerimientos de seguridad que demande las distintas áreas/unidades, consiguiendo la aplicación del modelo en los procesos estratégicos, gobernantes y de apoyo en cada institución. En la Tabla 2.13, se presenta los componentes de gestión de seguridad de la información aplicables en los centros de investigación.

Tabla 2.13 Componentes de gestión de seguridad de la información para los centros de investigación

	Políticas de seguridad de la Información	
	Organización de la seguridad de la información	
	Seguridad en los recursos humanos	
	Gestión de activos	
	Control de accesos	
	Criptografía	
	Seguridad física y ambiental	
	Seguridad en las operaciones	
	Seguridad en las comunicaciones	
	Adquisición, desarrollo y mantenimiento de sistemas de información	
	Relación con proveedores	
	Gestión de incidentes de seguridad de seguridad de la información	
	Administración de la continuidad de negocio	
	Cumplimiento	

Fuente: Norma ISO 27001:2013, [14]

2.3.2.5. Planteamiento de operación del SGSI:

En esta etapa se presentan las acciones adicionales que completarán la puesta en marcha del SGSI, se presenta un compendio con la terminología y definiciones, procedimientos y documentación necesarios para: monitorización global del SGSI, evaluación del modelo propuesto, revisiones, correcciones y planificación de auditorías.

Tabla 2.14 Operación del SGSI para los centros de investigación

SGSI	Operación del SGSI	
	Términos y definiciones	
	Evaluación de la funcionalidad de las etapas modelo y medidas correctivas	
	Establecimiento de programas de auditoría interna y externa	
	Revisiones y aprobaciones por parte de la Dirección	
	Documento de Seguridad	
	Certificación del SGSI	

Fuente: Norma ISO 27001:2013 [4], [14].

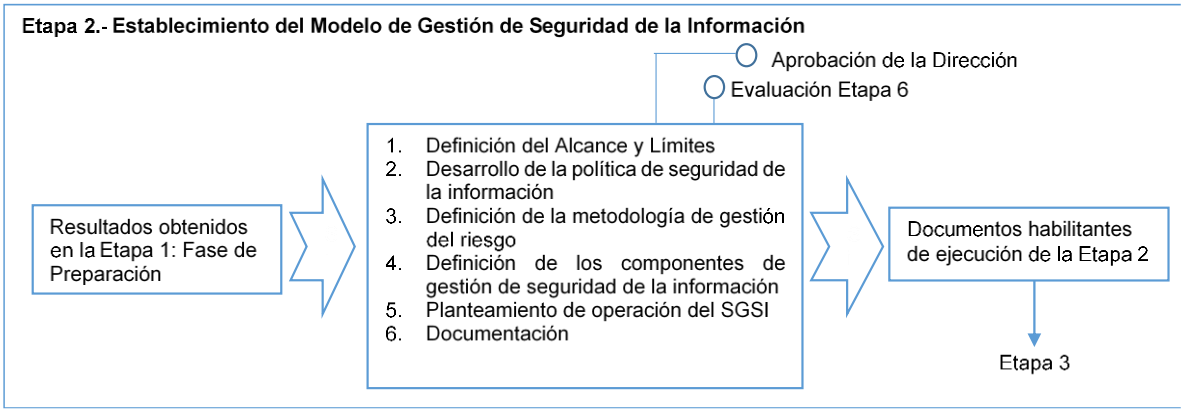
2.3.2.6. Documentación - Etapa 2: Entregables

Los resultados obtenidos en la segunda etapa, facilitarán la conformación de los siguientes documentos, que deben ser revisados y aprobados por el Comité de Seguridad de la Información, Directivos y serán sujetos a las actualizaciones que demande el proceso de mejoramiento continuo. Estos documentos se obtienen de referencias que presenta la norma ISO27001, ISO27005, NIST SP800-30 y CORAS:

- *Documento Alcance del SGSI*
- *Política de seguridad de la información*
- *Estructura general del proceso de gestión del riesgo*
- *Componentes de gestión de seguridad de la información*
- *Planteamiento de operación del SGSI*

En la Figura 2.6 se representa los componentes de la Etapa 2:

Figura 2.6 Esquema de la Etapa 2



Fuente: El Autor

2.3.3. Etapa 3.- Identificación de los riesgos

Esta etapa ha sido construida en base a las metodologías CORAS (Etapas de identificación, estimación, evaluación y tratamiento del riesgo), NIST SP800-30 (Valoración de riesgos) y OCTAVE (Fase 1: Visión organizativa y Fase 2: Visión Tecnológica). Como resultados se han definido los siguientes componentes:

2.3.3.1. Identificación y valoración de activos:

Para la determinación de activos, se ha dispuesto inicialmente una clasificación de los activos de información en los centros de investigación, y se han categorizado en función de la información que manejan y los servicios que prestan tomando la estructura de "Dependencias" [18] de Magerit, en donde se menciona que se puede organizar a los activos en capas. Así también, se ha aplicado la escala de valoración de activos de la metodología Magerit [19] en referencia a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información como se indica a continuación:

Tabla 2.15 Identificación del activo de la información y valoración, aplicada a los centros de investigación

TIPO DE ACTIVOS	Descripción / Categoría	Clase (Confidencial, Compartido, Público)	Valoración de Activos					Responsable del Activo
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Servicios:	Son los procesos internos y externos de la organización que estructuran el sistema de información							
	Gestión Administrativa							
	Gestión Académica							
	Correo Electrónico							
	Soporte y mantenimiento							
	Gestión de la infraestructura de red y arquitectura							
	Comunicaciones con el medio externo							
	Portal de servicios web							
	Gestión de Información Documental							
	Gestión de Datos y Documentos del Centro de Datos							
	Gestión de Seguridad de la Información							
	Gestión de Bases de Datos							
Datos/ Información:	Son el engrane del sistema, Datos o Información almacenada, o procesada física o electrónicamente							
	Datos adquiridos							
	Datos procesados							
	Datos almacenados							
	Datos analizados e interpretados							
	Bases de datos							
	Directorio Activo							

TIPO DE ACTIVOS	Descripción / Categoría	Clase (Confidencial, Compartido, Público)	Valoración de Activos					Responsable del Activo
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
	Desarrollo de soluciones de TI							
	Diseño, Creación, Investigación							
	Programación							
	Documentación de información del sistema							
Software	Las aplicaciones informáticas de la organización							
	Herramientas de Ofimática							
	Herramientas de Desarrollo							
	Bases de Datos							
	Licencias, soporte, mantenimiento							
	Software del Sistema							
	Software de Aplicación							
	Software Especializado							
	Software administrativo							
	Software Desarrollado localmente							
Tecnología								
Hardware	Equipos de Computación fijos							
	Servidores de aplicaciones							
	Servidores del Centro de Datos							
	Servidores Web							
	Equipos de Computación portátil							

TIPO DE ACTIVOS	Descripción / Categoría	Clase (Confidencial, Compartido, Público)	Valoración de Activos					Responsable del Activo
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
	Instrumentación especializada para monitoreo sísmico-volcánico, geodesia, geografía y meteorología.							
	Instrumentación para evaluación de componentes de telecomunicaciones, electrónica y redes							
	Equipos para desarrollo de hardware especializado							
	Equipos de Comunicación							
	Unidades de escaneo, e impresión							
	Unidades de pantalla, interactiva y proyección							
Comunicaciones:	Son las redes que dan soporte a la organización para el movimiento de la información.							
	Redes de monitoreo sísmico, volcánico, geodesia, meteorología.							
	Redes de comunicación por voz y telefonía.							
	Intranet e Internet.							
	Redes de transporte de datos, de monitoreo sísmico, volcánico, geodesia, meteorología.							
Soportes de información:	Son los soportes físicos que permiten el almacenamiento de la información.							
	Discos de almacenamiento							
	Cinta magnética.							
	Unidades de respaldo de datos							

TIPO DE ACTIVOS	Descripción / Categoría	Clase (Confidencial, Compartido, Público)	Valoración de Activos					Responsable del Activo
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Personal:	Por su conocimiento, habilidades, experiencia							
	Directivos							
	Administradores							
	Operadores							
	Clientes							
Equipamiento auxiliar:	Activos que soportan el funcionamiento del entorno							
	Central telefónica							
	Suministro de energía y sistemas de respaldo							
	Cableado Estructurado							
	Controles de acceso físico							
Instalaciones:	espacio físico en donde se alojan los sistemas de información							
	Oficinas, edificios…							
	Gestión de la infraestructura física							
	sucursales							
Intangibles:	Imagen y reputación de la organización							
	Credibilidad de la organización							
	Competencia en investigación							
	Generación de conocimiento							
	Capacidad de respuesta y operación							

Fuente: El Autor.

En la Tabla 2.16, para el campo de valoración de los activos se propone la estimación a los cinco requerimientos de análisis de riesgos (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad), de acuerdo a la siguiente escala de valoración de activos, tomando como referencia los criterios y dimensiones de valoración de la metodología MAGERIT [20].

Tabla 2.16 Valoración del activo y dimensiones del análisis de riesgos

Valoración del Activo		Dimensiones de análisis de riesgos				
Nivel	Escala	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Muy Bajo	1	Información del activo es pública	Información alterada no afecta al activo	El activo no es vital en los procesos críticos del sistema de información	El activo suplantado no tiene importancia en el sistema de información	Registro de acciones realizadas al activo no es indispensable
Bajo	2	Información del activo es compartida	Información alterada afecta al activo al mínimo	El activo es de apoyo en los procesos críticos del sistema de información	El activo suplantado tiene importancia leve en el sistema de información	Registro de acciones realizadas al activo es opcional
Moderado	3	Información del activo es restringida	Información alterada afecta parcialmente al activo	El activo es complementario en los procesos críticos del sistema de información	El activo suplantado tiene importancia relevante en el sistema de información	Registro de acciones realizadas al activo es complementario
Alto	4	Información del activo es confidencial	Información alterada causa afectación grave al activo	El activo afecta directamente en los procesos críticos del sistema de información	El activo suplantado tiene importancia alta en el sistema de información	Registro de acciones realizadas al activo es requerido
Muy Alto	5	Información del activo es secreta	Información alterada afecta al activo en su totalidad	El activo es vital en los procesos críticos del sistema de información	El activo suplantado tiene total impacto en el sistema de información	Registro de acciones realizadas al activo es indispensable

Fuente: El Autor, [20].

Durante la identificación de los activos en un caso práctico, se debe agregar otros parámetros adicionales que caractericen al activo, como son: código, descripción, ubicación del activo, cantidad. Esto facilitará la gestión de los activos de información y contribuye en los procesos de gestión de riesgos y del SGSI.

2.3.3.2. Identificación y valoración de amenazas:

Una amenaza, es un suceso que puede ocasionar un incidente no deseado a los activos causando un perjuicio a la organización. El objetivo es determinar a qué amenazas están expuestos los activos. Las amenazas pueden ser internas o externas, la norma ISO 27005 ha clasificado a las amenazas por su origen en: Deliberadas, Accidentales, Ambientales o naturales. También en la metodología Magerit, las amenazas pueden ser identificadas de la siguiente manera, y para el estudio se tomará esta categorización:

Tabla 2.17 Identificación de las amenazas

Amenaza	Descripción
De origen natural	Accidentes naturales (terremotos, inundaciones, tormenta eléctrica).
Del entorno (de origen industrial)	Desastres industriales (contaminación, fallos eléctricos, incendios)
Defectos de las aplicaciones	Problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente vulnerabilidades.
Causadas por las personas de forma accidental	Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión (fallos en los servicios de red, hardware, software, aplicaciones, control de recursos, medidas de contingencia)
Causadas por las personas de forma deliberada	Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; beneficiarse indebidamente, causar daños y perjuicios a los propietarios de los activos de información (Hacking, filtrado de información, vandalismo, robo)

Fuentes: [21] y [22].

Estos defectos se clasifican habitualmente bajo la taxonomía conocida como CVE (Common Vulnerability Enumeration), una norma internacional de facto. La mayor parte de estos defectos suelen afectar a aplicaciones software.

Para la valoración de las amenazas en el caso de que ocurrieran sobre los activos de información, se considera la probabilidad de ocurrencia con enfoque cualitativo y de esta manera interpretar si es posible o no que se materialice la amenaza.

Tabla 2.18 Probabilidad de ocurrencia de una amenaza.

Magnitud	Escala	Probabilidad		Descripción
10	Muy alta	muy frecuente	a diario	La amenaza se encuentra altamente producida, los controles para prevenir que explote la vulnerabilidad son ineficientes
7.5	Alta	frecuente	mensualmente	
5.0	Media	normal	una vez al año	La amenaza se encuentra producida, los controles implantados pueden prevenir que explote la vulnerabilidad
2.5	Baja	poco frecuente	cada varios años	La amenaza no se produce, o los controles implantados impiden que explote la vulnerabilidad
1	Muy baja	muy poco frecuente	siglos	

Fuentes: [21] y [23]

Aplicando lo indicado anterior, se presenta el catálogo de amenazas para los centros de investigación:

Tabla 2.19 Catálogo de amenazas para los centros de investigación

ACTIVO				AMENAZAS			
Activo	Tipo	Categoría	Valoración	Origen	Descripción	Consecuencias	Probabilidad de Ocurrencia
. Activos de información a ser evaluado	Servicios	Sección o proceso al que pertenece el activo	Confidencialidad	De origen natural	Descripción del daño o error en el activo	Revelación	muy frecuente
	Datos/ Información		Integridad	De entorno (origen industrial)		Modificación	frecuente
	Software		Disponibilidad	De fallos de las aplicaciones		Pérdida	normal
	Soportes de información		Autenticidad	Causadas por las personas de forma accidental		Destrucción	poco frecuente
	Personal		Trazabilidad			Interrupción	muy poco frecuente
	Equipamiento auxiliar			Causadas por las personas de forma deliberada			
	Instalaciones						
	Intangibles						
Ejm: Localización automática de eventos sísmicos	Datos/ Información	Ejm: Adquisición de datos, procesamiento, análisis e interpretación	Disponibilidad, Integridad	Causadas por las personas de forma accidental	Ejm: Mal funcionamiento de las aplicaciones internas	Interrupción, Pérdida	poco frecuente

Fuente: El Autor

2.3.3.3. Identificación de vulnerabilidades:

Entendiendo la definición de Vulnerabilidad como "Toda debilidad que puede ser aprovechada por una amenaza, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para proteger el valor propio o acumulado sobre un activo" [21]. Las vulnerabilidades se relacionan directamente con las debilidades de los activos y con los controles (Objetivos de control y controles: Etapa 4: Gestión de riesgos) que se implementan para proteger los activos de información.

Tabla 2.20 Formato para identificación de vulnerabilidades en los centros de investigación.

Activo	Vulnerabilidad	Origen de la Amenaza	Descripción de la Amenaza	Recomendaciones
Ejm.: Suministro de energía y sistemas de respaldo	Falta de mantenimiento y control de operación	Causada por las personas de forma deliberada	Cortes del servicio de energía eléctrica e interrupción en las operaciones del centro de investigación	

Fuente: Autor

La identificación de las vulnerabilidades para cada activo debe ser analizada con el equipo de seguridad de la información conformado dentro de cada centro de investigación. Las actividades principales son identificar las vulnerabilidades en cada categoría mediante herramientas de evaluación de la vulnerabilidad, establecer un reporte y el catálogo de vulnerabilidades asociado a los activos, controles y amenazas

2.3.3.4. Identificación de Controles existentes:

En esta sección se identifican los controles que mantienen los centros de investigación, también deben constar los planes de acción desarrollados que apoyen a la implementación de controles, a continuación se presenta un formato para registrar los controles existentes. Para el caso de nuevos controles y actualización de los existentes se aborda en la Etapa 4 del modelo SGSI la selección de objetivos de control e Implementación de controles.

Tabla 2.21 Catálogo de Controles existentes.

Activos		Controles Existentes		
Tipo	Activo	Control	Responsable	Estado de Operación

Fuente: El Autor

2.3.3.5. Valoración de impactos:

Para valorar el impacto se debe asignar un valor o grado de afectación del daño causado al activo obtenido de la materialización de la amenaza. Cuando se determina el grado de afectación, se debe tomar en cuenta si la amenaza influye a un solo activo, a un grupo de activos de la información o si influye en todo el sistema. Este resultado representa la magnitud de pérdida probable (lo peor que puede ocurrir).

Tomando como referencia la Guía NIST SP 800-30, ISO 27005 y Magerit se ha definido el grado de afectación de un activo (Nivel) y la valoración del impacto (Escala); para los centros de investigación se consideran los cinco criterios de seguridad de la información.

Tabla 2.22 Criterios de valoración del impacto para los centros de investigación, basado en la norma ISO 27005, Magerit y NIST-SP800-30

Nivel	Escala	Descripción	Magnitud
5	Muy Alto	Crítico, impacto total sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad	76 a 100%
4	Alto	Mayor, impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad	51 a 75 %
3	Moderado	Moderado, impacto medio sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad	26 a 50 %
2	Bajo	Menor, impacto leve sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad	1 a 25 %
1	Muy Bajo	Insignificante, impacto no tiene trascendencia sobre el valor del activo, no existe afectación en la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad	Menor a 1%

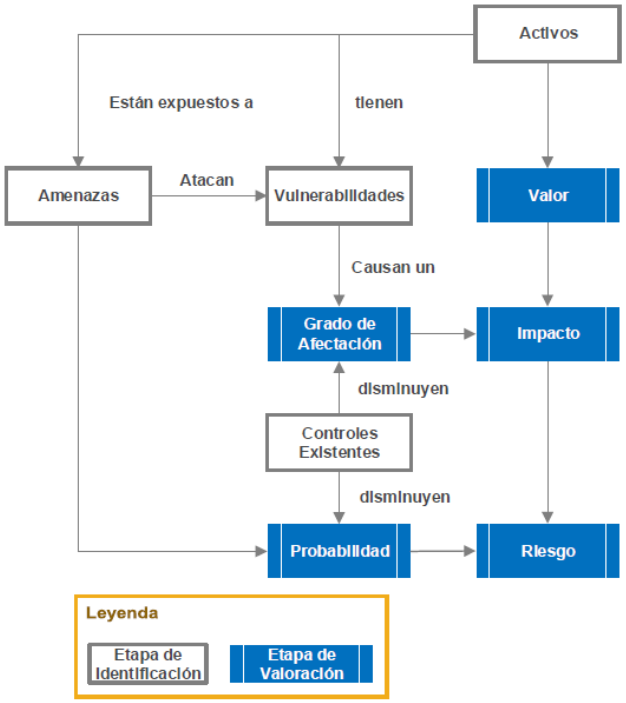
Fuente: El Autor

2.3.3.6. Valoración de riesgos:

Para realizar una valoración adecuada del riesgo debemos seguir los pasos que se detallan a continuación:

- *Análisis del riesgo:* Para el análisis del riesgo se debe relacionar activos, amenazas, vulnerabilidades y controles, obteniendo como resultados la magnitud del riesgo al que está expuesto el activo de información y las acciones que deben implementarse (etapa 4: tratamiento del riesgo) para prever los posibles riesgos. Del análisis del riesgo depende la toma de decisiones correcta para gestionar los riesgos apropiadamente. En la Figura 2.7 se presenta un esquema de los elementos del análisis de riesgo.

Figura 2.7 Elementos del análisis de riesgos potenciales Magerit.



Fuente: Magerit [21]

El resultado del análisis de riesgos es sólo un estudio a partir del que disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados), de lo que nos queremos proteger (amenazas

valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

- *Identificación del Riesgo:* Representa los posibles puntos de peligro a los que enfrentan los activos de información; es el proceso de identificar, registrar y caracterizar a los elementos del riesgo alineándose al alcance propuesto y su relación con otros procesos de la organización. En el presente estudio, se ha identificado los riesgos mediante la identificación y valoración de: activos, amenazas, vulnerabilidades, controles existentes e impacto, que se desarrolló en las secciones anteriores. Los riesgos registrados son tratados en las siguientes etapas y los que no se hayan detectado son considerados riesgo oculto.

- *Estimación del Riesgo:* Representa la relación entre el impacto ponderado (magnitud del impacto) frente a la probabilidad de ocurrencia (o expectativa de materialización) de la amenaza. Para el modelo propuesto se aplica la estimación cualitativa, ya que facilitará la aproximación inicial de identificación de los riesgos críticos. El riesgo refleja el daño probable (lo que probablemente ocurra).

Tomando como referencia las propuestas de Probabilidad de ocurrencia de una amenaza (Tabla 2.23) y Valoración del Impacto (Tabla 2.24), se presenta la Matriz de Estimación del riesgo:

Tabla 2.23 Probabilidad de ocurrencia de una amenaza

Magnitud	Escala	Probabilidad	
10	Muy alta	muy frecuente	a diario
7.5	Alta	frecuente	mensualmente
5.0	Media	normal	una vez al año
2.5	Baja	poco frecuente	cada varios años
1	Muy baja	muy poco frecuente	siglos

Fuente: Valoración de las Amenazas, Magerit [21]

Tabla 2.24 Valoración de impacto

Nivel	Escala	Magnitud
5	Muy Alto	76 a 100%
4	Alto	51 a 75 %
3	Moderado	26 a 50 %
2	Bajo	1 a 25 %
1	Muy Bajo	Menor a 1%

Fuente: El Autor, Determinación del impacto potencial Magerit [21]

Tabla 2.25 Estimación del riesgo

Riesgo		Probabilidad				
		Muy baja	Baja	Media	Alta	Muy alta
Impacto	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo
	Bajo	Muy Bajo	Bajo	Bajo	Medio	Medio
	Moderado	Bajo	Medio	Medio	Alto	Alto
	Alto	Medio	Alto	Alto	Muy Alto	Muy Alto
	Muy Alto	Alto	Muy Alto	Muy Alto	Muy Alto	Muy Alto

Fuente: El Autor

- *Evaluación de riesgo:* La evaluación de riesgos permite comparar el criterio de evaluación del riesgo y los criterios de aceptación, diferenciando de los activos, los que sean de mayor relevancia para priorizarlos en el tratamiento del riesgo.

  Para conseguir consolidar los criterios de aceptación del riesgo, se recomienda realizar una auditoría interna y/o utilizar herramientas de evaluación de riesgos como MSAT, y los resultados obtenidos de las técnicas de hackeo ético; con ello, se conseguirá establecer en la escala de estimación del riesgo, el valor de umbrales (criterios de aceptación) sobre los que se considere necesario realizar el tratamiento de los riesgos.

El modelo propuesto tiene la escala de valoración del riesgo de 0.01 a 10; se sugiere establecer el valor referencial para el tratamiento de riesgos conforme al análisis que realicen el equipo de seguridad de la información y los directivos.

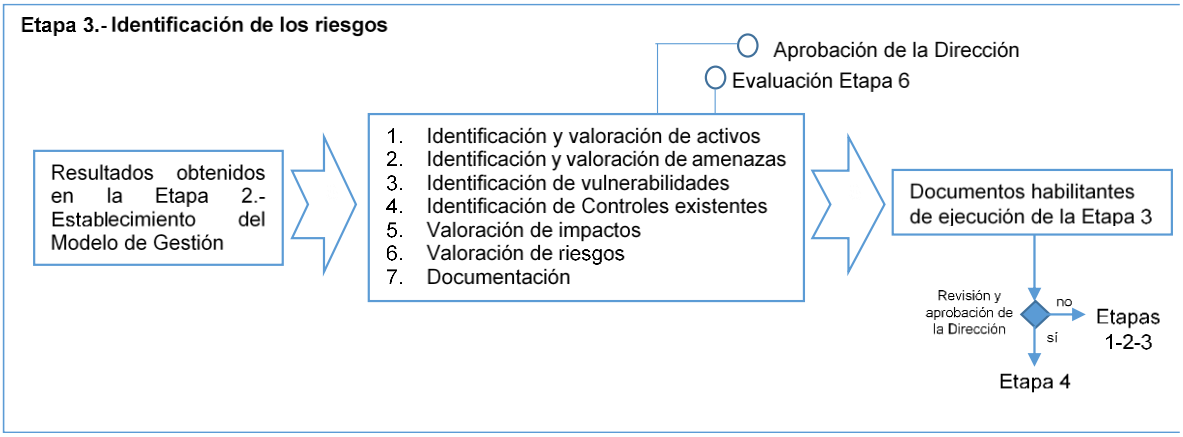
2.3.3.7. Documentación – Etapa 3: Entregables

Los documentos generados durante la Etapa 3 representan los resultados de la identificación de riesgos, en referencia al control de documentos que presenta el Método CORAS, NIST SP800-30 y OCTAVE, los mismos que deberán ser revisados y aprobados por el Comité de Seguridad de la Información y los Directivos.

- Matriz de activos (identificación y valoración de activos)
- Catálogo de amenazas
- Catálogo de vulnerabilidades
- Catálogo de controles existentes
- Valoración de impactos
- Matriz de riesgo (niveles del riesgo)
- Informe de evaluación de riesgos

En la siguiente Figura 2.8 se representa los componentes de la Etapa 3:

Figura 2.8 Esquema de la Etapa 3



Fuente: El Autor

2.3.4. Etapa 4.- Gestión de riesgos

Esta etapa ha sido construida en base a los fundamentos encontrados en la norma ISO 27005:2012 (Valoración y Tratamiento de riesgos, Aceptación del riesgo, Comunicación, Monitoreo y Revisión del riesgo), metodología OCTAVE (Fase 3: Desarrollar estrategias de protección y planes de mitigación), metodología MAGERIT (Proceso de Gestión de riesgos, Salvaguardas), NIST SP800-30 (Análisis de controles, Mitigación de riesgos) y método CORAS (Tratamiento del riesgo). Como resultados se han definido los siguientes componentes:

2.3.4.1. Tratamiento de riesgos:

El Tratamiento de riesgos es el proceso destinado a modificar el riesgo aplicando controles apropiados para cumplir con los requerimientos de seguridad, estimar el costo/beneficio de cada tratamiento y finalmente consolidar el Plan de tratamiento de riesgos. En el caso de los centros de investigación el tratamiento de riesgos está basado en las metodologías ISO27005, MAGERIT, OCTAVE, NIST SP800-30, CORAS y parte de dos aspectos fundamentales que son:

- La evaluación de riesgos, obtenida del análisis de riesgos y donde se obtiene los riesgos con mayor prioridad (Matriz de Riesgos Inicial)
- Los criterios de la evaluación de riesgo, que son analizados entre la comisión de seguridad de la información y la dirección.

Con estos antecedentes se procede con las acciones para el tratamiento de riesgos que deben ser acordes al alcance del SGSI, normativa legal vigente en el Ecuador indicada en el literal 2.1, y políticas de los centros de investigación en el literal 2.2 del modelo SGSI propuesto. Las acciones propuestas por la ISO 27005 [17] para el tratamiento de riesgos son:

- **Reducir el riesgo,** reducir el impacto y la probabilidad de ocurrencia mediante la aplicación de controles adecuados y aprobados que cumplan con los requerimientos de tratamiento del riesgo.
- **Retener el riesgo,** el nivel de riesgo es aceptado, se debe mantener los procedimientos de controles actuales o no implementar ningún control de seguridad si el nivel de riesgo es menor.
- **Evitar el riesgo,** cuando el nivel de riesgo es alto, se debe evitar o eliminar acciones y procedimientos que puedan generar el riesgo
- **Transferir el riesgo,** trasladar el riesgo a terceros que puedan asumir el riesgo y gestionarlo con mayor moderación.

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo [21], determinándose si:

- Es **crítico** en el sentido de que requiere atención urgente
- Es **grave** en el sentido de que requiere atención
- Es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento
- Es **asumible** en el sentido de que no se van a tomar acciones para atajarlo

2.3.4.2. Selección de objetivos de control y controles:

Como se indicó en la Tabla 2.15 sobre la Identificación de activos de la información de los centros de investigación, se presenta en el Anexo I el Catálogo de Controles seleccionados para cada tipo de activo, utilizando la guía de controles del estándar ISO 27001:20013. A continuación en la Tabla 2.26 se indican a manera de ejemplo algunos de los controles seleccionados para activos relacionados a Servicios, Datos / Información, Software, Hardware, Personal, Equipamiento auxiliar, Instalaciones e Intangibles.

Tabla 2.26 Controles seleccionados para los centros de investigación, basados en la norma ISO/IEC 27001:2013

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
Servicios: (Son los procesos internos y externos de la organización que estructuran el sistema de información)	Gestión Administrativa	6.1 Organización interna. 17.1 Continuidad de la seguridad de la información. 18.1 Cumplimiento de los requisitos legales y contractuales. 18.2 Revisiones de la seguridad de la información.	6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 18.1.1 Identificación de la legislación aplicable. 18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal. 18.2.2 Cumplimiento de las políticas y normas de seguridad.
	Gestión Académica	6.1 Organización interna. 18.1 Cumplimiento de los requisitos legales y contractuales. 18.2 Revisiones de la seguridad de la información.	6.1.4 Contacto con grupos de interés especial. 18.1.2 Derechos de propiedad intelectual (DPI). 18.2.1 Revisión independiente de la seguridad de la información.
Datos / Información: (Son el núcleo del sistema, Datos o Información almacenada o procesada física o electrónicamente)	Datos adquiridos	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 9.4 Control de acceso a sistemas y aplicaciones. 12.1 Responsabilidades y procedimientos de operación. 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.3 Datos de prueba.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.2.1 Directrices de clasificación. 8.2.3 Manipulación de activos. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas. 12.1.1 Documentación de procedimientos de operación. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6.1 Gestión de las vulnerabilidades técnicas. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.3.1 Protección de los datos utilizados en pruebas.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
Software (Las aplicaciones informáticas de la organización)	Software del Sistema. Software de Aplicación. Software Especializado. Software administrativo	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 9.1 Requisitos de negocio para el control de accesos. 9.2 Gestión de acceso de usuario. 9.3 Responsabilidades del usuario. 9.4 Control de acceso a sistemas y aplicaciones. 10.1 Controles criptográficos. 12.1 Responsabilidades y procedimientos de operación. 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.4 Registro de actividad y supervisión. 12.5 Control del software en explotación. 12.6 Gestión de la vulnerabilidad técnica. 12.7 Consideraciones de las auditorías de los sistemas de información. 14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso. 9.3.1 Uso de información confidencial para la autenticación. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso a código fuente de los programas. 10.1.2 Gestión de claves. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5.1 Instalación del software en sistemas en producción. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7.1 Controles de auditoría de los sistemas de información. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
Hardware:	Instrumentación especializada para monitoreo sísmico-volcánico, oceanografía y meteorología	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 11.1 Áreas seguras. 11.2 Seguridad de los equipos. 12.1 Responsabilidades y procedimientos de operación. 12.6 Gestión de la vulnerabilidad técnica.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software.
Personal: (Por su conocimiento, habilidades, experiencia)	Directivos	6.1 Organización interna. 7.1 Antes de la contratación. 7.2 Durante la contratación. 7.3 Cese o cambio de puesto de trabajo. 9.2 Gestión de acceso de usuario. 12.1 Responsabilidades y procedimientos de operación.	6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la información. 7.2.3 Proceso disciplinario. 7.3.1 Cese o cambio de puesto de trabajo. 9.2.5 Revisión de los derechos de acceso de los usuarios. 12.1.1 Documentación de procedimientos de operación. 12.1.3 Gestión de capacidades.

Tipo de Activos	Descripción/ Categoría	Objetivos de Control	Controles Seleccionados
Equipamiento auxiliar: (Activos que soportan el funcionamiento del entorno)	Suministro de energía y sistemas de respaldo	8.1 Responsabilidad sobre los activos. 11.1 Áreas seguras. 11.2 Seguridad de los equipos. 12.1 Responsabilidades y procedimientos de operación. 12.6 Gestión de la vulnerabilidad técnica.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. 12.1.1 Documentación de procedimientos de operación. 12.6.1 Gestión de las vulnerabilidades técnicas.
Instalaciones: (espacio físico en donde se alojan los sistemas de información)	Gestión de la infraestructura física		
Imagen: (Imagen y reputación de la organización)	Capacidad de respuesta y operación	7.2 Durante la contratación	7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario.

Fuente: El Autor, (Anexo I)

Una vez identificados los controles, el equipo de seguridad de la información deberá iniciar la aplicación de los controles seleccionados en los activos de información "críticos = nivel de riesgo muy alto" y "graves = nivel de riesgo alto", en corto plazo. Para los activos de información de niveles moderado y bajo se deberá coordinar con los directivos para asumir como riesgo aceptable o si debe ser tratado. En el caso de identificar un riesgo crítico o grave y que la institución no pueda tratarlo se puede optar por la acción de transferencia del riesgo.

2.3.4.3. Implementación de controles:

En esta sección se toman los activos de información más relevantes dentro cada centro de investigación asociados al objetivo de control y controles recomendados y se documenta la forma en que se llevará el proceso de aplicación del control, indicando las entradas / habilitantes o condiciones actuales, limitaciones / restricciones del entorno, objetivos específicos del control y consecuencias si no se implementa adecuadamente dicho control. En la siguiente Tabla 2.27 se representa la información que debe constar en la implementación de controles en los activos de información para el tratamiento de los riesgos.

Tabla 2.27 Seguimiento al proceso de aplicación del control

Objetivo de Control ISO 27001	Entradas, habilitantes, condiciones actuales, limitaciones, restricciones del entorno	Objetivos específicos del control	Consecuencias	Estado: (aplicable, implementado, en ejecución)

Fuente: El Autor

El objetivo de implementar un control es reducir relativamente el riesgo sobre el activo de información considerando su costo de implementación; el control puede ser calificado como eficaz, insuficiente, injustificado o nulo, dependiendo del grado de capacidad para segmentar o eliminar la vulnerabilidad sobre el activo y la magnitud de impacto. En los centros de investigación pueden presentarse restricciones en la implementación de los controles debido a:

- Tiempo de vida útil de un activo

- Disponibilidad de recurso humano para el seguimiento de controles
- Financiamiento destinado a la implementación de controles
- Limitaciones por cumplimiento legal y política interna
- Complejidad en la aplicación de herramientas de seguridad en ambientes con diversidad de tecnología

2.3.4.4. Aceptación del riesgo y riesgo residual:

El proceso de aceptación del riesgo se obtiene del tratamiento de riesgos y el establecimiento de controles. El riesgo residual es tratado cuando este desborda los criterios de aceptación del riesgo y por lo tanto debe actualizarse la matriz de riesgos con un registro de cambios. El plan de tratamiento del riesgo y los riesgos residuales deben ser documentados y presentados por el comité de seguridad de la información a la Dirección del Centro de Investigación para su aprobación y deben ser socializados a nivel estratégico. Es muy importante señalar que para el modelo propuesto se establecen los siguientes criterios de aceptación para el tratamiento del riesgo.

- *Definición de criterios de Valoración:* Para el caso de los centros de investigación, una vez que se ha determinado la valoración del riesgo, se propone:
    - El tratamiento de los riesgos identificados con valoración Alta y muy Alta en el corto plazo para su mitigación.
    - Se considera riesgos aceptables sobre los activos de información a los que tengan una valoración Baja y Muy Baja
    - Para los riesgos identificados con valoración Media, deberán ser monitorizados en el mediano plazo y re categorizarlos como riesgos aceptables que asume la institución o si deben ser tratados para su mitigación.
- El comité de seguridad de la información debe coordinar con los directivos los criterios de valoración, el plan de tratamiento de riesgos, el estudio económico,

y garantizar el aval de la dirección sobre las decisiones tomadas en la gestión del riesgo.

- El riesgo residual deberá ser tratado cuando este desborde los criterios de aceptación del riesgo, esto implica modificar los controles implementados o las acciones para el tratamiento de dicho riesgo.

2.3.4.5. Estrategia de protección y Plan de mitigación:

Esta sección se basa en el modelo de gestión de riesgos OCTAVE para el desarrollo de estrategias y planes de seguridad, de donde se puede destacar los siguientes aspectos aplicables en el modelo SGSI para los centros de investigación:

- Documentar las estrategias de protección actual.- Consiste en el análisis de las áreas más críticas
- Seleccionar enfoques de mitigación
- Desarrollar planes de mitigación .- Establecer las prácticas para mitigación
- Establecer el plan de trabajo de acciones inmediatas y ciclo de evaluaciones.

Para el levantamiento de esta información se debe recurrir a la información obtenida en las secciones anteriores y que constituye la documentación habilitante, por lo cual es necesario tener disponible la siguiente información:

- Matriz de perfil del riesgo para los activos críticos
- Valoración de la Amenaza y árbol de amenazas
- Implementación de controles

2.3.4.6. Declaración de aplicabilidad:

Es el documento que identifica los objetivos y la aplicabilidad de cada control, es decir el cómo se implementarán dichos controles. Otra definición proporcionada en la metodología Magerit es: “Documento formal en el que, para un conjunto de

salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido" [21]

Se debe agregar que este documento formal o informe emitido por el equipo de seguridad de la información y autorizado por la dirección contiene las contramedidas que se consideran oportunas para defender el sistema de seguridad de la información propuesto para los centros de investigación, incluye el análisis técnico, operativo, económico, contiene la estimación de los recursos necesarios para la ejecución del SGSI, y debe estar disponible para el conocimiento de todos los funcionarios. A continuación se propone el formato de la aplicabilidad de controles de la norma ISO 27001.

Tabla 2.28 Justificación de la aplicabilidad de controles implementados en los centros de investigación

Controles seleccionados ISO 27001			Centro de investigación	
Objetivo de Control	**Referencia**	**Controles**	**Justificación de Aplicabilidad / Exclusión**	**Responsable**

Fuente: El Autor.

2.3.4.7. Comunicación del riesgo:

Debe ser transmitida por el comité de seguridad de la información mediante el plan de comunicación presentado a toda la organización desde el nivel estratégico hasta el nivel operacional, la comunicación debe ser continua y se debe asignar un vocero de la comunicación del riesgo, miembro del comité de seguridad de la información. La planificación de reuniones dentro de cada centro de investigación entre los Directivos, Comité de Seguridad y representantes de las unidades/áreas para los temas de seguridad de la información facilitarán la retroalimentación del SGSI.

A continuación se presenta los aspectos más importantes que debe contener el Plan de Comunicación del Riesgo:

Tabla 2.29 Plantilla para la presentación del Plan de Comunicación del Riesgo

Plan de Comunicación del Riesgo		
Fecha de aprobación:	**Versión:**	**Realizado por:**
Objetivos:		
Plan de Tratamiento del Riesgo:		
Estrategias de Protección y Plan de mitigación:		
Observaciones:		

Fuente: El Autor

2.3.4.8. Monitorización y Revisión del riesgo:

En esta sección se debe monitorizar los factores de riesgo y mejorar la gestión del riesgo, ya que los activos, controles, amenazas y vulnerabilidades son dinámicos y están en constante cambio, el proceso de mejora continua del SGSI depende de la efectiva monitorización y revisión del riesgo. La matriz de riesgo deberá ser actualizada, estos cambios generan la denominada matriz de riesgo final.

Las funciones principales que se deben llevar a cabo durante la monitorización y revisión del riesgo son:

- Analizar los criterios de medición del riesgo de forma continua y ajustarlos a los objetivos del SGSI y de mejora continua
- Analizar si las condiciones legales, políticas, ambientales y recursos son apropiados para el cumplimiento de los objetivos del SGSI
- Contribuir al mejoramiento de la gestión de riesgo y sustentar el conocimiento de mitigación del riesgo
- Comunicar a las autoridades competentes las medidas que se están implementando para el tratamiento del riesgo

- Actualizar permanentemente la matriz de riesgo y mantener el registro de cambios y actualizaciones.

En la siguiente tabla 2.30 se propone un formato para registrar los resultados de: monitorización y revisión del riesgo

Tabla 2.30 Plantilla para registrar los resultados de monitorización y revisión del riesgo

Monitorización y Revisión del riesgo								
	Actuales	Fecha:	Agregados	Fecha:	Modificados	Fecha:	Eliminados	Fecha:
Activos de información								
Vulnerabilidades								
Amenazas								
Impacto			Variación				Fecha:	
Riesgo			Variación				Fecha:	
Incidentes Registrados:								
Incidente	Activos involucrados		Estado del Activo		Recursos utilizados / agregados		Observaciones	
Fecha de revisión:			Responsables:					

Fuente: El Autor

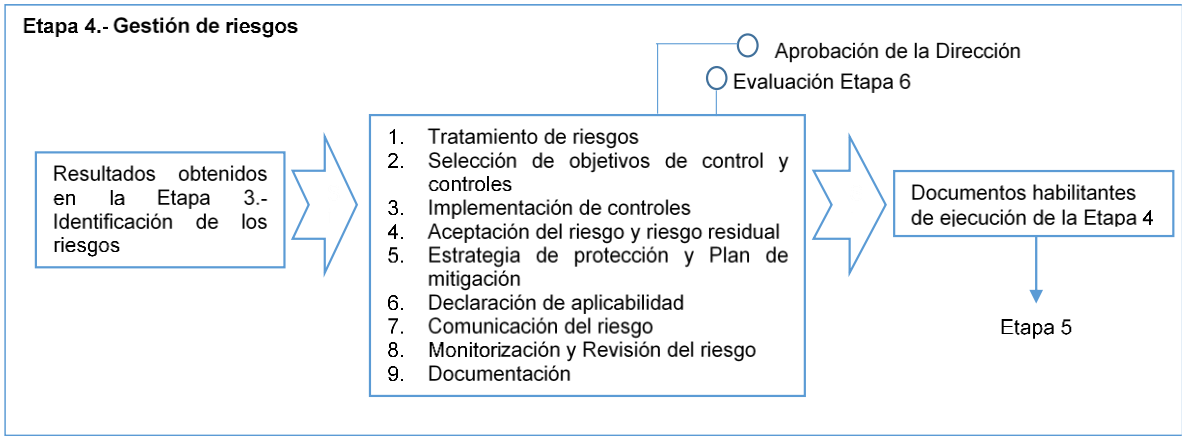
2.3.4.9. Documentación – Etapa 4: Entregables

La documentación que se requiere como entregables se menciona a continuación:

- Plan de tratamiento de riesgos
- Catálogo de controles y plan de implementación
- Aceptación del riesgo y riesgos residuales
- Monitorización y revisión del riesgo
- comunicación del riesgo
- Matriz de riesgo final
- Declaración de aplicabilidad

En la Figura 2.9 se representa los componentes de la Etapa 4:

Figura 2.9 Esquema de la Etapa 4



Fuente: El Autor

2.3.5. Etapa 5.- Componentes de gestión de seguridad de la información y objetivos de control en los centros de investigación

En esta etapa los componentes para gestionar la seguridad de la información en los centros de investigación se detalla a continuación:

2.3.5.1. Políticas de seguridad:

Como se indicó en la Etapa 2 en el Establecimiento del Modelo de Gestión de Seguridad de la Información sobre el desarrollo de la política de seguridad de la información, permite implantar la cultura de seguridad de la organización en todos los niveles de jerarquía de los centros de investigación.

La política de seguridad está orientada a garantizar el cumplimiento del SGSI en todas las etapas del modelo SGSI propuesto y la aplicación de sanciones conforme a lo establecido por la Dirección y comité de seguridad de la información.

Objetivos:

- Implantar las directrices, normas y procedimientos que garanticen la protección y uso de los activos de la información en los centros de investigación
- Promover los principios de la seguridad de la información (confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad) en los activos de los centros de investigación
- Garantizar la actualización y aplicabilidad de la Política de Seguridad de la información en los centros de investigación
- Difundir al personal de los centros de investigación la importancia de la seguridad de la información, y la necesidad de aplicabilidad del SGSI

Responsables: Alta Dirección, Jefaturas, Responsable de seguridad, Comité de seguridad de la información, Responsable del activo, Unidades de: TI, Talento Humano, Administración, Auditor

2.3.5.2. Aspectos organizacionales de la seguridad de la información:

Para la implantación del SGSI propuesto es necesario establecer la estructura organizacional en el área de seguridad que debe adoptarse en los centros de investigación, presentar las funciones principales que deben asumir para cada rol y designar los responsables en el área de seguridad de la información.

Se debe definir los acuerdos de confidencialidad de la información y deben ser reconocidos por todo el personal de los centros de investigación.

Establecer el tratamiento de la seguridad de la información con el ambiente externo a los centros de investigación, mediante acuerdos de nivel de servicio, control de cambios, instalaciones y mantenimiento de activos de la información. Por ejemplo, los usuarios externos deben sujetarse a la política de seguridad en cada centro de investigación

El intercambio de información con el medio externo es una actividad frecuente en los centros de investigación, por lo que se debe implementar las medidas necesarias

para proteger el acceso a los activos de información, se debe mantener un registro actualizado de los intercambios de la información, designación del responsable de los activos involucrados y la verificación del cumplimiento de las políticas de seguridad.

2.3.5.3. Seguridad en los recursos humanos:

La seguridad de la información respecto al recurso humano debe ser observada en los centros de investigación en tres fases: Antes del empleo, Durante el empleo, y en la Terminación de empleo. Se deberá dar a conocer y comprender a todo el personal las responsabilidades, los recursos asignados, el reconocimiento de las políticas implantadas, sanciones, metodología de SGSI utilizada, cumplimiento de controles, privilegios de acceso a la información y los procedimientos en el caso de registrarse incidentes de seguridad.

El personal deberá tener pleno conocimiento del acuerdo de confidencialidad para proteger los activos de la información de los centros de investigación, entendiéndose como confidencial a la información que afecte directa o indirectamente en las actividades de los centros de investigación.

El personal debe estar informado y capacitado de forma continua para que contribuya con el cumplimiento de las normas, políticas, procedimientos de seguridad y uso adecuado de los recursos.

En el caso de terminación del empleo, el coordinador de unidad/área conjuntamente con el equipo de seguridad de la información, deberán hacer una constatación del estado de los activos entregados y constatar que la información del centro de investigación que ha utilizado el empleado sea devuelta/eliminada, se suspenderá los accesos a la información, cuentas de correo, claves, tarjetas de acceso.

2.3.5.4. Gestión de activos:

Para asegurar el adecuado uso de los activos de información de los centros de investigación, es necesario que cada área/unidad y los responsables de cada activo mantengan el inventario actualizando el estado de funcionalidad de los activos y la valoración, monitorizar si los controles aplicados son efectivos para proteger los activos, clasificar a los activos de acuerdo a su grado de importancia y criticidad, contribuir a la actualización de la base de datos de control de activos gestionada por la unidad de TI y revisada por el comité de seguridad de la información.

De la misma manera en cada centro de investigación se deberá establecer lineamientos para uso de servicio de internet e intranet, correo electrónico, uso de aplicaciones y software especializado, uso de equipos de adquisición, almacenamiento, procesamiento, análisis e interpretación de datos.

2.3.5.5. Control de accesos:

Es el proceso que asegura el acceso a los sistemas de información (red, sistemas operativos, aplicaciones, dispositivos móviles, teletrabajo), mediante registros, privilegios, contraseñas y mecanismos debidamente contemplados y documentados en la política de seguridad de los centros de investigación. Gestionar el control de accesos implica también implantar nuevas políticas y criterios que mejoren la gestión del SGSI.

El equipo de seguridad de la información y el responsable de la unidad/departamento deberán trabajar continuamente en la asignación de privilegios, contraseñas y uso adecuado de los activos de información. Se deberá especificar las políticas de control de acceso lógico y físico, así como la comunicación de los controles implementados a los usuarios, propietarios de los activos.

Se debe establecer y documentar los procedimientos para acceso remoto a la red de los centros de investigación (autenticación, cifrado, protocolo SSH, VPN), las cuentas deberán ser registradas y reemplazadas periódicamente, se deberá

establecer límite de tiempos de conexión dependiendo del nivel de usuario y sistema requerido.

Los usuarios registrados para acceder a los sistemas de información deberán cumplir con el procedimiento de registro de usuario que establezca el administrador de red y el equipo de seguridad de la información, esta documentación debe ser socializada y aprobada, estableciendo los compromisos de responsabilidad, se debe actualizar continuamente cada cuenta, privilegios y contraseñas en función de las actividades y nivel del usuario.

2.3.5.6. Seguridad física y ambiental:

La gestión de seguridad física y ambiental comprende el establecimiento de normas de seguridad en infraestructura física y equipos que se encuentran dentro (instalaciones) y fuera de los centros de investigación (estaciones, repetidoras, observatorios), para proteger los activos de información de amenazas de origen provocado, accidental o ambiental.

Las funciones principales que deben desarrollarse en esta fase son: implementar los procedimientos y normas para controlar la seguridad física de la infraestructura y activos de información, mitigar los factores ambientales que pueden ocasionar daños en los activos de información, definir la periodicidad de mantenimientos que deben ejecutarse en los activos de información, establecer un plan de acción para los activos críticos encontrados.

Los responsables de los activos de información deberán implementar en el registro de activos el estado de funcionalidad del equipo y la valoración del activo. Los activos que se encuentran fuera de los centros de investigación, deberán llevar un estricto control de visitas, modificaciones, instalaciones y movimiento de los activos, se deberá implantar el registro físico y digital del inventario que consta en cada observatorio, estación y repetidora.

2.3.5.7. Seguridad en las operaciones y comunicaciones:

La seguridad en las operaciones y comunicaciones garantiza el cumplimiento de los siguientes objetivos:

- Implantar y mantener registros de procedimientos de operación de los sistemas de información.
- Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
- Gestionar entornos de pruebas, desarrollo y operación.
- Proteger los registros de información, establecer procedimientos para respaldo y copias de seguridad.
- Establecer procedimientos y acuerdos de intercambio de información con el medio externo.
- Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas o identificadas.

En el proceso de gestión de comunicaciones y operaciones se debe establecer los procedimientos de preparación de ambientes de prueba, desarrollo y operación para las estaciones de monitoreo, centro de datos, equipos de adquisición y procesamiento de datos, redes de transporte de datos y desarrollo de software propietario, que garanticen que los sistemas de información no sean afectados en sus funcionalidades.

Adicionalmente, se debe establecer controles para: software malicioso, monitoreo en los servicios de red, procedimientos de: respaldo de información, uso de medios externos de almacenamiento e intercambio de información.

2.3.5.8. Adquisición, desarrollo y mantenimiento de los sistemas de información:

En este proceso se establece los procedimientos para alcanzar los siguientes objetivos:

- Proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información por medios criptográficos.

- Garantizar la seguridad de los archivos de sistema.
- Implementar políticas de desarrollo de software y mantener la seguridad de aplicaciones.

En esta sección se contempla también los requisitos para aseguramiento de las comunicaciones en servicios a través de redes públicas.

2.3.5.9. Gestión de incidentes en la seguridad de la información:

En esta sección, se debe cumplir el aseguramiento de la comunicación para organizar las acciones correctivas oportunas frente a eventos de seguridad de la información y debilidades asociadas con los sistemas de información, garantizando un enfoque coherente y efectivo en la gestión de los incidentes de seguridad de la información.

El personal en conjunto con el responsable de seguridad de la información, deben identificar las alertas y vulnerabilidades de los centros de investigación, notificarlas y registrar el incidente, para proceder con las acciones de mitigación o reasignar el caso a terceros, se utilizará un registro o base de datos que dispone el comité de seguridad para documentar los incidentes, las acciones de mitigación, y el aprendizaje obtenido.

2.3.5.10. Gestión de la continuidad del negocio:

Se debe implantar un marco de referencia (respuesta a incidentes y recuperación para acciones particulares) orientado a contrarrestar las interrupciones de las actividades en los centros de investigación y proteger los procesos críticos de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación. Permite identificar y reducir los riesgos, recuperar rápidamente la continuidad de las principales operaciones del centro de investigación.

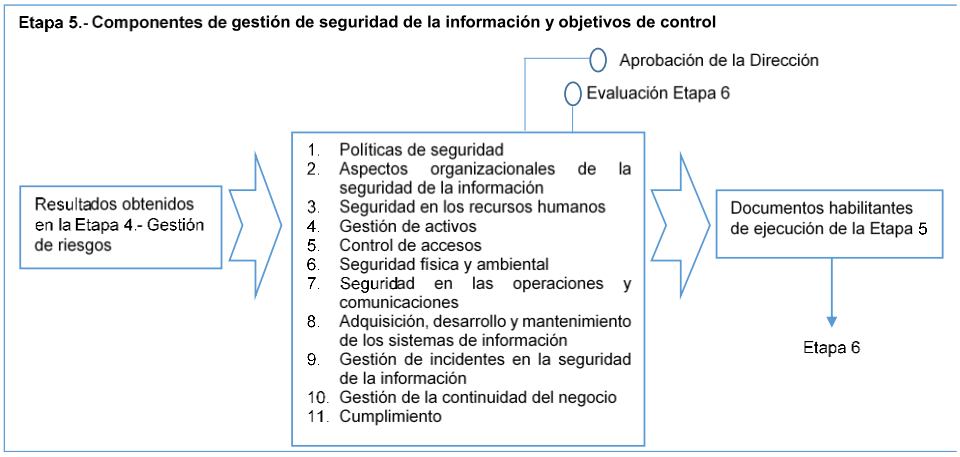
El plan de continuidad debe actualizarse y se debe probar su efectividad en coordinación con el responsable de seguridad y el comité de seguridad, finalmente la Dirección debe aprobar los planes de continuidad.

2.3.5.11.Cumplimiento:

Permite asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización, evitar infracciones a las leyes, obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad, asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización. Permite lograr que el proceso de auditoría de los sistemas de información alcance la máxima eficacia con las mínimas interferencias.

En la Figura 2.10, se representa los componentes de la Etapa 5:

Figura 2.10 Esquema de la Etapa 5



Fuente: El Autor

2.3.6. Etapa 6.- Operación del Sistema de Gestión de Seguridad de la Información

2.3.6.1. Operación del SGSI:

Para orientar la operación del SGSI se presenta en la Figura 2.13 un esquema de las etapas y componentes del modelo SGSI propuesto, que está fundamentado en la norma ISO 27001, ISO 27005, Magerit, Octave, NISTSP800-30, Coras, el mismo que está enmarcado dentro del ciclo de mejora continua PHVA.

2.3.6.2. Términos y definiciones:

En este componente se presentan los términos y definiciones que se utilizan durante el desarrollo del presente modelo, y es responsabilidad del equipo de seguridad de la información ampliarlos durante la operación del SGSI y mantener actualizaciones disponibles para consulta en caso de ser requeridas por los usuarios. Dichos términos se contemplan en el Anexo G.

2.3.6.3. Evaluación de la funcionalidad de las etapas modelo y medidas correctivas:

La evaluación de la funcionalidad es parte del ciclo de mejoramiento continuo del modelo SGSI propuesto, es el proceso que consiste en el monitoreo y revisión de los registros y documentación de seguridad de la información, con el objetivo de prevenir o corregir anomalías detectadas, resolver inconsistencias en la adopción del modelo y los lineamientos que se requieran para la creación de un componente en el modelo, ajustes en los controles, plantillas y contenidos de la documentación oficial para el cumplimiento del SGSI.

El Comité de Seguridad de la Información deberá verificar si la documentación generada (Entregables) en cada etapa del modelo SGSI, representa resultados favorables y aporta al levantamiento de la información necesaria para alcanzar los objetivos propuestos. De la misma manera, los Directivos deberán analizar si la aprobación del modelo y los avances en la ejecución de las etapas aportan al mejoramiento y organización de los sistemas de información en los Centros de Investigación. Los cambios y propuestas que se generan en este componente deben ser documentados y aplicados de manera inmediata para ajustar las etapas del modelo a los requerimientos de cada centro de investigación.

2.3.6.4. Establecimiento de programas de auditoría interna y externa:

Es el proceso en donde se realiza la revisión periódica de cumplimiento de las etapas del modelo SGSI propuesto, y donde se mantiene actualizados los

procedimientos de seguridad de la información aplicados, así como los aspectos que no se han ejecutado, los plazos de entrega y los requerimientos que deberán efectuarse en comparación con la normativa ISO 27001 para la certificación, si es el objetivo planteado por el centro de investigación. Así también, en este proceso deben presentarse los lineamientos para el informe de auditoría dirigidos a la alta dirección y a los empleados. Los aspectos considerados en la auditoría interna son:

- Las auditorías internas deben ser planificadas (plan auditor) y aprobadas por la dirección
- El equipo auditor debe conformarse por profesionales idóneos con experiencia y diferentes a los encargados de la implantación del SGSI en la organización.
- Se debe estipular un coordinador del equipo auditor.
- La auditoría se debe orientar hacia la correcta implantación de los controles de seguridad.
- Toda la organización debe conocer el alcance y la agenda estipulada para la auditoría interna.
- Los informes y resultados deberán ser conocidos por todo el personal de la organización involucrado dentro del alcance del SGSI
- De acuerdo al informe y/o resultados presentados en la auditoría interna, la organización debe estipular los planes para mejorar la efectividad del SGSI y realizar el procedimiento documentado de acciones correctivas y preventivas.

2.3.6.5. Revisiones y aprobaciones por parte de la Dirección:

La Dirección deberá verificar el SGSI en todo su contexto, los avances en cada etapa deberán ser documentados para estudio y aprobación de la Dirección, a través de sus revisiones deberá proponer las mejoras pertinentes y el compromiso en la implementación del SGSI. La Dirección debe establecer la periodicidad de las revisiones y aprobaciones, y para ello requerirá de los informes presentados en cada etapa.

2.3.6.6. Documento de Seguridad:

Esta información es generada y actualizada por el Coordinador de Seguridad de la Información y debe contener en forma global todos los aspectos del SGSI de los centros de investigación de desastres naturales.

A continuación se presenta la estructura general del documento de seguridad, tomando como referencia el formato propuesto por la Agencia Española de Protección de Datos [2]

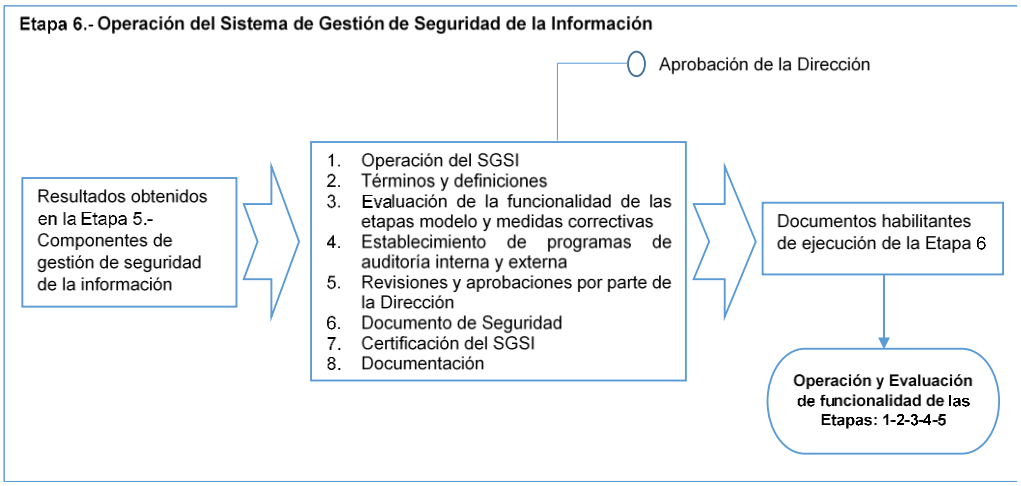
- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- Las medidas que sean necesarias adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o, la reutilización de estos últimos.
- La identificación del responsable o responsables de seguridad.
- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

2.3.6.7. Certificación del SGSI:

El proceso de certificación del SGSI bajo la norma ISO 27001 puede ser opcional para los centros de investigación, el nivel directivo podrá optar por certificarse con el objetivo de posicionarse de mejor manera respecto a organizaciones científicas del mismo fin, dedicadas a la investigación de desastres naturales.

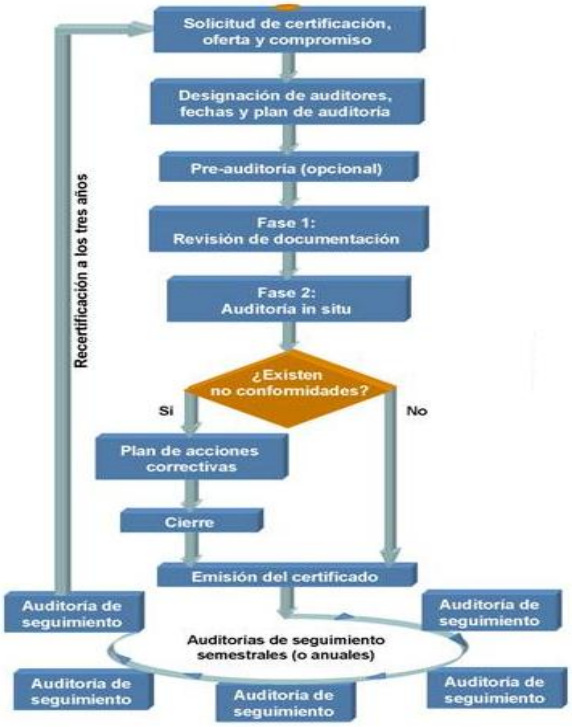
A continuación se presenta un esquema de los pasos para auditoría y obtención de la certificación ISO 27001. Una vez constituido el SGSI y en operación [24], se deberá solicitar a una entidad certificadora acreditada una auditoría, a partir de la que se inicia el proceso de certificación como indica la Figura 2.12, y de cumplir con los requisitos de la norma se obtiene la certificación. En la siguiente Figura 2.11 se representa los componentes de la Etapa 6:

Figura 2.11 Esquema de la Etapa 6



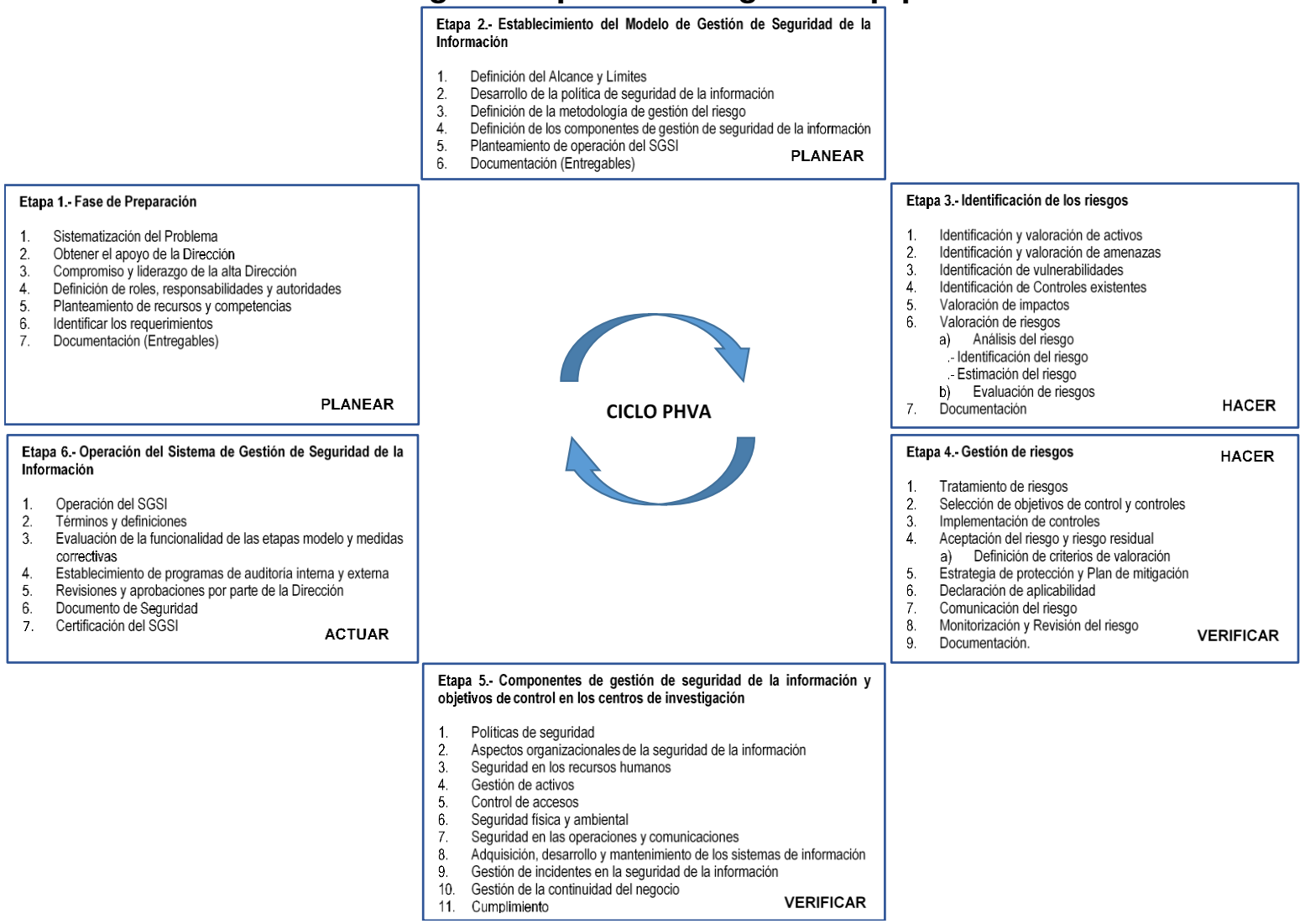
Fuente: El Autor

Figura 2.12 Proceso de auditoría para obtener una certificación, según ISO 27001



Fuente: [4]

Figura 2.13 Etapas del modelo de gestión SGSI propuesto



Fuente: El Autor. Diseño del Modelo de Gestión SGSI - Versión 1.1

2.4. Guía de Aplicación del Modelo de Gestión

Como resultado de la relación de normas y metodologías para estructurar el modelo de gestión SGSI que se detalla en el Anexo F y del diseño propuesto en el literal 2.3, se ha determinado la guía de aplicación que resume los aspectos fundamentales en cada una de las etapas:

Etapa de Preparación: Inicia con la identificación de necesidades actuales en seguridad de la información del centro de investigación o unidad/área, planteamiento de objetivos, para estructurar una propuesta de implementación del SGSI dirigida a la alta Dirección con el propósito de obtener su apoyo y compromiso, destinando esfuerzos y recursos en el área de seguridad de la información.

Etapa Dos: Establecimiento del modelo de gestión; permite organizar el modelo SGSI como tal, definiendo el alcance y límites, así también las políticas a implementarse, la metodología de gestión de riesgos, controles, requerimientos de operación y evaluación del SGSI.

Etapa Tres: Identificar los riesgos; permite identificar y valorar a activos, amenazas, vulnerabilidades, controles e impactos; obteniendo el análisis y evaluación del riesgo.

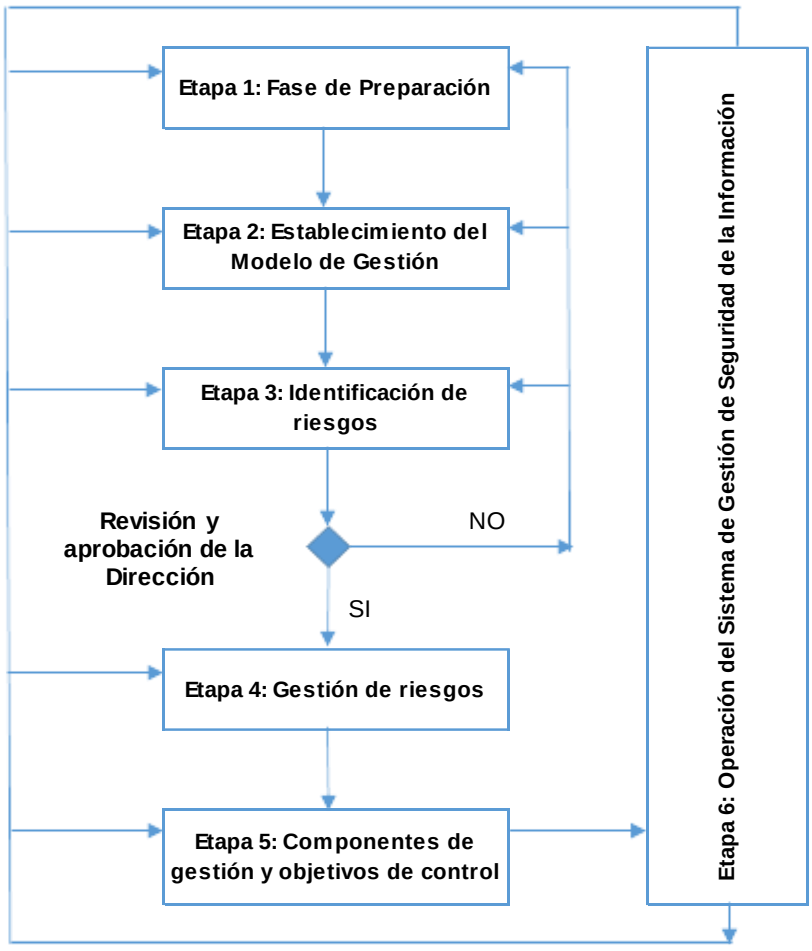
Etapa Cuatro: Gestión de riesgos; para la ejecución de esta fase es indispensable la coordinación y aprobación de la alta Dirección, en caso contrario no se podrá formalizar esta etapa y las consecuentes. En esta fase y con los resultados obtenidos de las etapas anteriores, se debe tomar la decisión por parte de los directivos si se procede al tratamiento de los riesgos identificados, implantar controles, plantear estrategias, planes de mitigación y revisiones de los riesgos.

Etapa Cinco: Se orienta al reconocimiento de los componentes de gestión, objetivos de control y controles que sugiere la norma ISO 27001:2013 en su anexo A, que pueden necesitarse implementar durante la ejecución del SGSI propuesto.

Etapa Seis: La operación del sistema de gestión de seguridad de la información permite el mejoramiento continuo del SGSI propuesto, mediante evaluación, revisión y aprobación de la funcionalidad de las etapas anteriores.

Los resultados obtenidos en cada una de las etapas indicadas anteriormente deben ser revisados, documentados y aprobados por la alta dirección, los mismos que servirán de base para continuar a la etapa subsiguiente.

Figura 2.14 Esquema del modelo de gestión SGSI propuesto

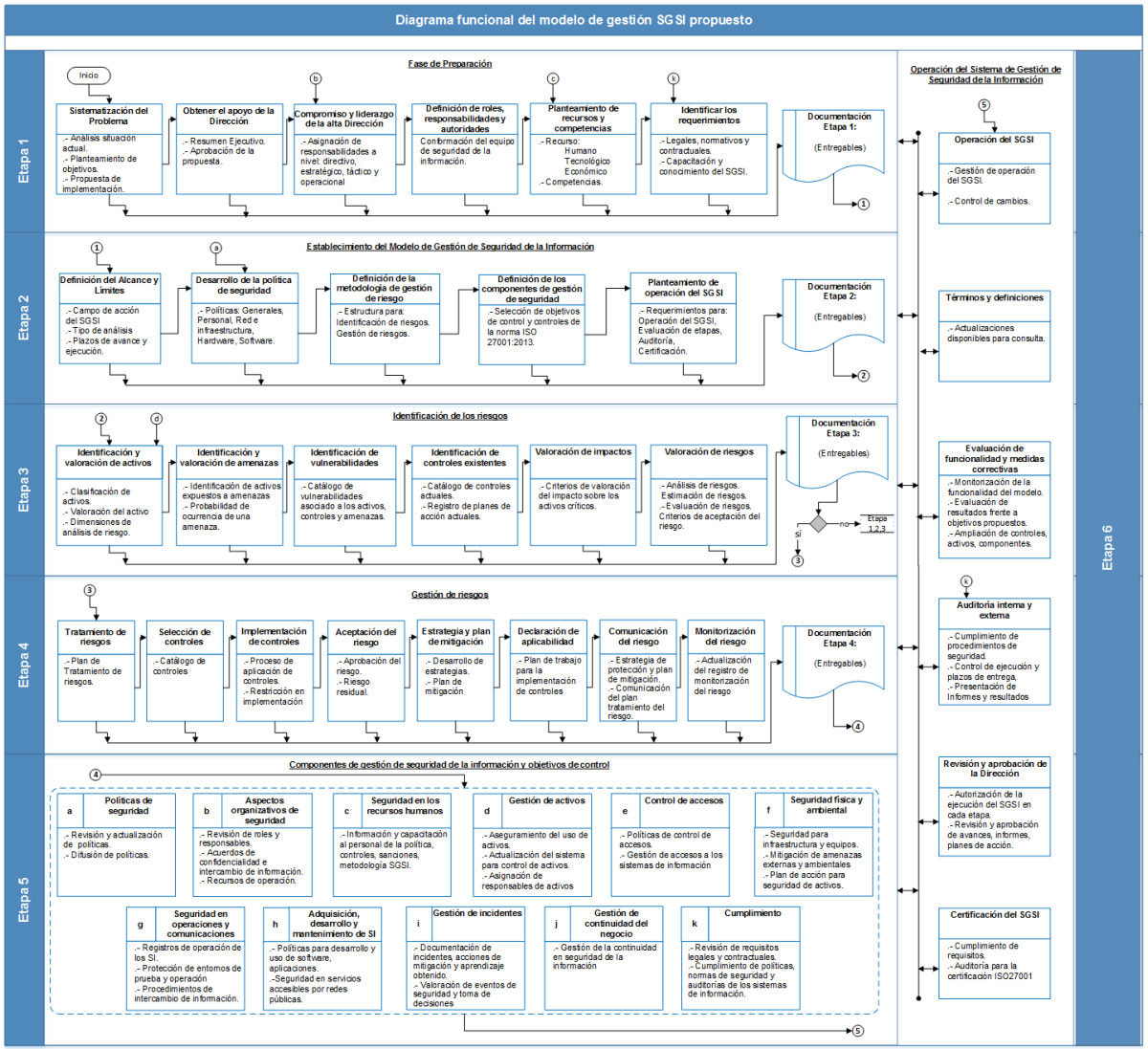


Fuente: El Autor

La Figura 2.14 muestra el esquema general del modelo de gestión SGSI propuesto y su interrelación en seis etapas. Para evidenciar el cumplimiento en cada etapa es necesario conformar una lista de documentos y formatos (Documentación - Entregables), con el objetivo de facilitar la gestión del SGSI y el seguimiento a los procesos que vayan ejecutándose. Estos "Entregables" pueden ser tomados del modelo SGSI propuesto y también de plantillas existentes que presentan las normas y metodologías de gestión de riesgos.

La Figura 2.15 representa el diagrama funcional del modelo de gestión SGSI con la relación de dependencias entre procesos, elementos y resultados de cada etapa. Así también se propone la evaluación de la funcionalidad de las etapas, en donde se tomarán las medidas correctivas y acciones que permitan el mejoramiento continuo del modelo y el ajuste de acuerdo a los requerimientos de la institución, unidad o departamento.

Figura 2.15 Diagrama funcional del modelo de gestión SGSI propuesto



Fuente: El Autor

CAPÍTULO 3. APLICACIÓN DEL MODELO EN EL CASO DE ESTUDIO

Para llevar a cabo la aplicación del modelo de gestión SGSI se ha tomado como referente al Instituto Geofísico, debido a que es un centro de investigación con trayectoria de más de 30 años como entidad dedicada al monitoreo e investigación científica de los fenómenos sísmicos y volcánicos en el Ecuador.

Durante este período la institución ha tenido un crecimiento organizacional muy importante los últimos 10 años, la presencia de fenómenos sísmicos y volcánicos que han causado impacto social, económico y científico, han llevado a la adopción de nuevos métodos, tecnologías y medidas de optimización de las TI.

3.1. Definición de alcance y restricciones de evaluación

Para determinar el alcance y restricciones de evaluación, previamente se ha analizado la situación actual del caso de estudio entorno a la seguridad de la información, identificando los activos de información (Literal 1.3.1), dimensionamiento orientado a procesos de mayor relevancia (Literal 1.3.2), revisión de la normativa legal vigente, políticas implementadas, factibilidad de aplicación de normas de la serie ISO 27000 y metodologías de gestión de riesgos (Literal 2.1).

Con estos antecedentes, a continuación se propone la aplicación del modelo de gestión SGSI, y se puntualiza en el literal 3.2.2.1 el alcance y límites para el caso de estudio.

3.2. Aplicación del modelo de Gestión SGSI

Dentro de las actividades que mantiene el Instituto Geofísico [25], se puede identificar servicios comunes relacionados al monitoreo, vigilancia, procesamiento y evaluación de peligros, debido a que se involucran directamente con el tratamiento de los datos sísmicos, volcánicos y con el acceso a la información. Es por ello, que

se ha planteado a la institución la aplicación del modelo SGSI propuesto en dos procesos identificados como:

- **Proceso 1: Gestión de datos sísmicos y volcánicos**
- **Proceso 2: Gestión del acceso a la información relacionada al monitoreo sísmico y volcánico.**

Estos procesos fundamentales y críticos actualmente no son gestionados en el ámbito de seguridad de la información, por lo cual se realizará un modelamiento para mejorar el sistema de seguridad de la información del Instituto Geofísico y validar la aplicabilidad del modelo SGSI propuesto.

El modelo de Gestión SGSI propuesto contiene seis etapas que serán evaluadas para los procesos anteriores indicados del caso de estudio.

3.2.1. Etapa 1: Fase de Preparación

Esta etapa inicial se orienta a la identificación del problema, plantea objetivos, propone una solución, se apoya en la aprobación y compromiso de la alta dirección, define roles, responsabilidades, recursos y plantea los requerimientos para gestionar el SGSI.

3.2.1.1. Sistematización del problema

Actualmente los procesos seleccionados son gestionados mediante procedimientos y actividades que sostienen el cumplimiento de requerimientos y demandas de disponibilidad de la información, el personal encargado de estas funciones realiza una ardua labor diariamente para mantener activos estos procesos principales; sin embargo, para el ámbito de seguridad de la información no existe documentación formal y operaciones basadas en metodologías para la protección de activos, no existe un proceso encargado de análisis y gestión de riesgos, propuestas de mejoramiento y gestión de incidentes. Por lo cual, se debe aplicar un estudio en los procesos escogidos para mejorar el sistema de seguridad de la información.

La propuesta de implementación del modelo de gestión SGSI para los procesos de gestión de datos sísmicos y volcánicos, así como la gestión del acceso a la información relacionada al monitoreo sísmico y volcánico permitirá lo siguiente:

- Establecer un plan de operación del SGSI que involucra desde el nivel directivo hasta el nivel operativo para reducir el riesgo de los activos de información.
- Mejorar la gestión de seguridad de la información en los procesos seleccionados y su interrelación con otros procesos también vitales, como son: Gestión del Centro de Datos, comunicación con el medio externo, disponibilidad de datos e información para usuarios internos y externos.

3.2.1.2. Obtener el apoyo de la Dirección

Como se ha indicado en el literal 2.3.1.2, para el Caso de Estudio se ha presentado la propuesta de implementación del SGSI a la Dirección del Instituto Geofísico. El documento formal (Anexo H) contiene: la sistematización del problema, los procesos que serán analizados, el establecimiento de los roles, responsabilidades, requerimientos y recursos.

Se ha conseguido la autorización parcial por parte de la Dirección para continuar con el levantamiento de la información, debido al re direccionamiento de los recursos necesarios para implementar el SGSI, quedando pendiente la aprobación formal de la propuesta.

3.2.1.3. Compromiso y liderazgo de la alta Dirección

Para la implementación del modelo SGSI en los procesos escogidos es fundamental contar a Nivel Directivo con la revisión y aprobación formal del Director del Instituto Geofísico; para el caso práctico el modelo se encuentra en proceso de revisión.

A Nivel Estratégico se ha propuesto la conformación del Comité de Seguridad de la Información y los roles definidos en el literal 3.2.1.4, así como el compromiso para dar asistencia en la coordinación, control y verificación de actividades durante la

implementación del modelo SGSI; para el caso práctico no se ha logrado mantener permanentes las actividades del comité de seguridad, debido a la carga laboral que desempeñan los funcionarios involucrados en este proceso, ocasionando retrasos en la coordinación de actividades del SGSI y revisión de la funcionalidad del modelo en cada etapa. Las actividades de coordinación de seguridad se han realizado de forma parcial, debido a que no existe personal asignado exclusivamente para cumplir estas funciones.

A Nivel Técnico se ha logrado el levantamiento de la información, con lo cual ha permitido el avance de las etapas de modelo propuesto, sin embargo durante el proceso de implementación existen etapas que requieren de la toma de decisiones a nivel estratégico y directivo, las mismas que no se han culminado, quedando como referencias y lineamientos.

3.2.1.4. Definición de roles, responsabilidades y autoridades

Para conformar el equipo de Seguridad de la Información en el Instituto Geofísico, se ha reasignado las funciones que debe asumir el personal en función del modelo propuesto, de acuerdo a la Tabla 3.1.

Tabla 3.1 Asignación de funciones del personal y descripción de responsabilidades

Funciones actuales del personal del Instituto Geofísico	Funciones en el equipo de Seguridad de la Información	Descripción
Jefe del Área de Sismología Jefe del Área de Volcanología Jefe del Área de Sistemas Jefe del Área Técnica	Comité de Seguridad de la información	Está conformado por representantes de las áreas de TI, área administrativa, y el oficial de seguridad de la información. Representan el principal medio de comunicación con la Alta Dirección y presentan las propuestas, avances y requerimientos del sistema de gestión de seguridad de la información del Centro de Investigación.
Auditor Interno (Funcionario del Área de Sistemas).	Promotor:	Un "promotor" no participa activamente en el mismo, interviene si el proyecto está paralizado. El coordinador debe informar regularmente al promotor del proyecto acerca del estado del mismo.

Funciones actuales del personal del Instituto Geofísico	Funciones en el equipo de Seguridad de la Información	Descripción
Funcionario con amplios conocimientos en Seguridad de la información. (Especialista en seguridad de la información).	Coordinador	La función es coordinar, garantizar la implementación ininterrumpida del SGSI dentro de los plazos establecidos y los recursos necesarios para la implementación, informar al promotor y altos directivos sobre el progreso del SGSI, realizar trabajos administrativos relacionados con el mismo.
Analistas de Redes nivel 2 y 3 Coordinador Representantes de Áreas	Equipo de análisis	Impulsar las acciones asociadas a la gestión de la seguridad de la información, se encarga de asignar personal para la conformación de equipos de trabajo multidisciplinarios, personal de documentación y formación. Establece el cronograma de trabajo del modelo SGSI. Análisis del riesgo, priorización, aceptación y tratamiento.
Analistas de redes nivel 1 Técnicos de TI Representantes de Áreas	Equipo de seguridad de la información:	La función es ayudar en la implementación del SGSI, ejecutar tareas preestablecidas y aportar en la toma decisiones que requieren un enfoque multidisciplinario.
Funcionario propietario o responsable del activo	Administrador:	Es el responsable del activo/información y procesos relacionados, así como gestionar los avances, evaluaciones, reportes y cambios. Se encarga de determinar el nivel de seguridad de la información del activo.
Analista de Redes nivel 2	Analista de seguridad del sistema:	La función es monitorizar las acciones de seguridad en el sistema de información, gestión y configuración de hardware y software, evaluación de medidas de seguridad del sistema y propuesta de cambios.
Funcionarios involucrados en el proceso 1 y 2	Personal técnico:	La función es el manejo de la información, administración de activos de información e implementación de soluciones de TI.

Fuente: El Autor

3.2.1.5. Planteamiento de recursos y competencias

Recurso Humano: Corresponde al personal que conforma el equipo de seguridad de la información indicado anteriormente y que ha sido autorizado por el Director del Instituto Geofísico y Jefes de Área.

Tecnológico: Comprende el uso del Hardware y Software disponibles en el Instituto Geofísico, así como software libre para la implementación del SGSI, auditoría, test de vulnerabilidades e incidentes.

Económico: Contempla los costos por horas laborables extendidas incurridas por el personal del Instituto Geofísico destinadas a la aplicación del modelo SGSI en los procesos escogidos, costos indirectos asociados al uso de los recursos tecnológicos y capacitación del personal involucrado.

Competencias: Se realizarán un cronograma de capacitación y conocimiento del SGSI a los empleados en el nivel de las habilidades necesarias y participación que tengan dentro del SGSI.

3.2.1.6. Requerimientos legales, normativos y contractuales:

De acuerdo a la normativa vigente en el Ecuador sobre las obligaciones que tienen las instituciones públicas como el Instituto Geofísico – EPN, en el tema de seguridad de los datos y de la información pública disponible, se menciona los siguientes reglamentos y leyes que abordan los procesos escogidos sobre gestión de los datos y acceso a la información:

- Constitución Política del Ecuador: Artículo 18.
- Normas de Control Interno de la Contraloría General del Estado: Norma 300 Evaluación del riesgo, 410-10 Seguridad de tecnología de información.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: Artículos 57, 202, 415.
- Ley del Sistema Nacional de Registro de Datos Públicos: Artículo 26.

- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP): Artículos 5, 10.
- Acuerdos - Secretaría Nacional de la Administración Pública (SNAP): Acuerdo Ministerial No 166 y No 309.
- Políticas dedicadas a varios procesos del área de seguridad de la información (políticas de respaldo de datos) establecidas por el Servicio Geológico de los Estados unidos USGS [26] y las indicadas en la Tabla 2.1.

3.2.1.7. Documentación – Etapa 1: Entregables

El siguiente compendio muestra los documentos habilitantes que servirán de respaldo y evidencia del avance de la Etapa 1 del modelo SGSI propuesto. Para el caso de estudio "Instituto Geofísico" la información que se ha generado en esta Etapa es incluida de la siguiente manera:

Tabla 3.2 Guía para la Documentación de la Etapa 1. Caso de estudio

Etapa 1: Entregables	Observaciones Información disponible en:	Verificación (Realizado SI / NO)	Estado (Revisión, Aprobación, Ejecución)
Propuesta de implementación del Modelo SGSI – Resumen Ejecutivo	Etapa 1: Fase de Preparación. Capítulo I: Literales 1.1, 1.2, 1.3. Sistematización del problema: Literal 3.2.1.1	SI	Revisión
Acta de compromiso por parte de los miembros del equipo de SGSI	Compromiso y liderazgo de la alta Dirección	NO	- -
Requerimientos	Requerimientos Tecnológicos y Administrativos Planteamiento de recursos y competencias • Recurso Humano • Tecnológico • Económico	SI	Revisión
Sustento legal, normativas y políticas gobernantes.	Requerimientos legales, normativos y contractuales	SI	Revisión
Programa de capacitación y conocimiento del SGSI	Planteamiento de recursos y competencias	SI	Revisión
Conformación del equipo de seguridad de la información	Definición de roles, responsabilidades y autoridades	SI	Revisión

Fuente: El Autor

3.2.2. Etapa 2.- Establecimiento del Modelo de Gestión de Seguridad de la Información

3.2.2.1. Definición del Alcance y Límites

El modelo de gestión SGSI para el centro de monitoreo e investigación científica de los fenómenos sísmicos y volcánicos "Instituto Geofísico - EPN", se orienta al mejoramiento de las actividades de seguridad de la información para los procesos de 1) gestión de datos sísmicos y volcánicos, y 2) gestión de acceso a la información relacionada al monitoreo sísmico y volcánico; con el objetivo de mejorar la gestión de seguridad de la información en los procesos más sensibles y que están relacionados a las áreas de Sismología, Volcanología, Sistemas y Técnica.

El modelo SGSI propuesto contempla equipos informáticos, infraestructura de red, infraestructura física, y personal involucrado en los procesos escogidos previamente del Instituto Geofísico. Se evalúan vulnerabilidades, se determinan los riesgos, se definen los objetivos de control y controles acordes a los requerimientos de seguridad identificados, se realiza la valoración y selección de controles, para desarrollar la guía de implementación que será aplicable en los procesos de gestión de datos sísmicos, volcánicos y en la gestión de acceso a la información relacionada al monitoreo sísmico y volcánico del instituto Geofísico.

El entorno de aplicación del modelo SGSI propuesto se limita a analizar y evaluar cualitativamente los procesos determinados en el Alcance; los resultados obtenidos pueden ser un referente para programas de auditoría de la información y toma de decisiones a nivel Directivo. La aplicación y avances de las etapas del SGSI propuesto están sujetas a la revisión y aprobación del Comité de Seguridad de la Información y del Director del Instituto Geofísico; en caso contrario únicamente se establecerá lineamientos y guías para las etapas pendientes de aprobación.

3.2.2.2. Desarrollo de la política de seguridad de la información

Actualmente en el Instituto Geofísico las políticas de seguridad de la información no son debidamente documentadas, aprobadas y monitorizadas para el cumplimiento de los procesos en cuestión. Por ello, deben ser definidas por el equipo de seguridad de la información, jefes de Área y el Director, las mismas que deben ser presentadas para conocimiento y aplicación de todo el personal. Tomando como referencia el literal 2.6.2.2 sobre el Desarrollo de la política de seguridad de la información, se propone en términos generales las siguientes políticas para el caso de estudio:

- *Políticas generales:*
    - Dar cumplimiento a la normativa vigente en el Ecuador que se encuentra referenciada en el Literal 3.2.1.6 y en el Anexo B.
    - Implementar controles para la revisión de políticas, actualización y difusión de las mismas en la institución.
    - Establecer acuerdos del uso de los datos e información relacionada al estudio del comportamiento sísmico y volcánico en el Ecuador bajo los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad para proteger los sistemas de información que dispone el Instituto Geofísico.
- *Políticas para el personal:*
    - Dar cumplimiento a las responsabilidades asignadas para el equipo de seguridad de la información del Instituto Geofísico que se encuentran descritas en el Literal 3.2.1.4; así como los efectos que conllevaría el incumplimiento de las mismas.
    - Implementar controles de seguridad en los recursos humanos que propone la norma ISO 27001:2013 para la contratación de personal del Instituto Geofísico y que se contemplan en el literal 2.3.5.3 del modelo SGSI propuesto.
- Políticas de seguridad de red e infraestructura: Se refieren a las acciones que deben implementarse para el control de acceso a los sistemas de información e infraestructura, perímetros de seguridad física y de los equipos.

- Seguridad de la Infraestructura:
  - Establecer procedimientos y mecanismos de control para monitorizar el acceso al Centro de Datos y sala de monitoreo del Instituto Geofísico, tales como: sistema de cámaras de vigilancia, registro digital de accesos.
  - Dar cumplimiento a los controles que recomienda la norma ISO 27001:2013 y que se consideran en el modelo de gestión SGSI propuesto sobre seguridad física y ambiental, seguridad en las operaciones y gestión de incidentes de seguridad de la información.
- Seguridad de red:
  - Mejorar las operaciones de monitorización de la red interna y acceso a servidores y equipos destinados al tratamiento de datos sísmicos y volcánicos, potenciar la disponibilidad de servidores y servicios asignados para acceso a la información, implementar protocolos de autenticación en la red.
  - Implementar el registro de control de accesos de usuarios para los sistemas y aplicaciones destinados a los procesos en cuestión.
  - Implementar los controles de la norma ISO 27001:2013 contemplados para control de accesos, seguridad en las redes y sistemas de información, como se indican en el modelo de gestión SGSI propuesto.

- Políticas de seguridad de hardware:
  - Mantener los registros actualizados del hardware involucrado en el tratamiento de datos y la información, generar un registro para evaluación del estado de funcionamiento y los cambios realizados.
  - Generar informes de anomalías detectadas y notificarlas al personal encargado del análisis de seguridad del sistema de información.
  - Implementar los controles para gestión de activos de la norma ISO 27001:2013 y recomendaciones indicadas en el Literal 2.3.5.4 del modelo SGSI propuesto.

- Políticas de seguridad de software:
    - Implementar controles al software utilizado para los sistemas de adquisición de datos sísmicos, volcánicos y presentación de la información.
    - Definir políticas para el desarrollo de software y aplicaciones, entornos de prueba y actualizaciones requeridas en los procesos de adquisición de datos y procesamiento.
    - Generar informes de uso de software y aplicaciones, anomalías identificadas y comunicarlas al personal de seguridad de la información.

3.2.2.3. Definición de la metodología de gestión del riesgo

Se utilizará la metodología de gestión de riesgos para los centros de investigación de desastres naturales propuesta en la Tabla 2.12, aplicando a los procesos indicados en la definición del Alcance, y que se desarrolla en la siguiente etapas 3 (Análisis de Riesgos) y etapa 4 (Gestión de Riesgos).

3.2.2.4. Definición de los componentes de gestión de seguridad de la información

Para el caso de estudio, se utilizará los componentes de gestión de seguridad de la información establecidos en la norma ISO 27001:2013, como se ha mencionado en la Tabla 2.13.

3.2.2.5. Planteamiento de operación del SGSI

El modelo propuesto contempla la operación del SGSI y la evaluación del proceso de gestión de seguridad en su totalidad. En el caso de estudio se implementa los elementos indicados en la Tabla 2.14 que conforman la operación del SGSI, para los procesos en cuestión.

3.2.2.6. Documentación – Etapa 2: Entregables

Tabla 3.3 Guía para la documentación de la Etapa 2. Caso de Estudio

Etapa 2: Entregables	Observaciones.- Información disponible en:	Verificación (Realizado SI / NO)	Estado (Revisión, Aprobación, Ejecución)
Documento Alcance del SGSI	Definición del Alcance y Límites	SI	Revisión
Política de seguridad de la información	Desarrollo de la política de seguridad de la información • Políticas generales • Políticas para el personal • Políticas de seguridad de red e infraestructura	SI	Revisión
Estructura general del proceso de gestión del riesgo	Definición de la metodología de gestión del riesgo	SI	--
Componentes de gestión de seguridad de la información	Objetivos de control y controles para la seguridad de la información.	SI	Revisión
Planteamiento de operación del SGSI	Planteamiento de operación del SGSI	SI	Revisión

Fuente: El Autor

3.2.3. Etapa 3.- Identificación de los riesgos

3.2.3.1. Identificación y valoración de activos

En esta sección se determinan los activos de información del Instituto Geofísico, se identifican las amenazas, vulnerabilidades y se realiza la valoración de impactos, probabilidad de ocurrencia, riesgo, que están implicados en los procesos en cuestión; se ha utilizado la escala de valoración del activo en base a cinco dimensiones de análisis de riesgos (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad), y se presenta los resultados en la Tabla 3.4 para los activos relacionados a Servicios, Datos e Información, Software, Tecnología (Hardware, Comunicaciones, Soportes de información), Personal, Equipamiento auxiliar, Instalaciones, Intangibles.

Tabla 3.4 Identificación del activo de la información y valoración, aplicado al Caso de Estudio

Procesos involucrados: 1. Gestión de Datos (adquisición, almacenamiento, procesamiento, interpretación y análisis). 2. Gestión de Acceso a la Información (usuarios internos y externos)	Metodología de Gestión del Riesgo					**Versión:**	
	Etapa: 3	**Identificación de riesgos**				**Fecha:**	
	Sección 3.1	**Determinación de activos**				**Aprobado por:**	

TIPO DE ACTIVOS	**Descripción / Categoría**	**Clase (Reservado, Compartido, Público)**	**Valoración de Activos**					**Resultado Valoración**	**Responsable del Activo**
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
Servicios	Correo Electrónico	Compartido	2	4	3	3	3	3,0	Sistemas
	Gestión de la infraestructura de red y arquitectura	Reservado	3	3	4	4	4	3,6	Sistemas, Técnica
	Comunicaciones con el medio externo	Público	1	5	5	5	5	4,2	Dirección, Jefaturas
	Gestión de Información Documental	Compartido	2	5	4	4	4	3,8	Sistemas, Sismología
	Portal de servicios web	Público	1	5	5	4	4	3,8	Sistemas
	Gestión de Datos y Documentos del Centro de Datos	Reservado	4	4	5	5	4	4,4	Sistemas
	Gestión de Seguridad de la Información	Compartido	3	4	4	4	5	4,0	Sistemas, Técnica
	Gestión de Bases de Datos	Reservado	3	3	4	5	4	3,8	Sistemas

TIPO DE ACTIVOS	Descripción / Categoría	Clase (Reservado, Compartido, Público)	Valoración de Activos					Resultado Valoración	Responsable del Activo
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
Datos/Info	Datos adquiridos	Reservado	4	5	5	5	5	4,8	Técnica
	Datos procesados	Reservado	3	5	5	5	5	4,6	Sismología, Volcanología
	Datos almacenados	Reservado	3	5	5	5	5	4,6	Sistemas
	Datos analizados e interpretados	Compartido	2	5	5	5	5	4,4	Sismología, Volcanología
	Bases de datos	Compartido	3	4	5	5	4	4,2	Sistemas
	Directorio Activo	Reservado	3	3	2	2	4	2,8	Sistemas
	Documentación e información del sistema	Reservado	3	2	2	3	4	2,8	Sism, Volc, Técn, Sist
Software									
	Herramientas de Ofimática	Compartido	2	1	2	2	2	1,8	Sistemas
	Bases de Datos	Compartido	3	4	5	4	4	4,0	Sistemas
	Software de Sistema	Reservado	3	1	5	5	4	3,6	Sistemas
	Software de Aplicación	Compartido	3	3	5	5	4	4,0	Sistemas, Técnica
	Software Especializado	Reservado	4	5	5	5	5	4,8	Sistemas, Técnica
	Software Desarrollado localmente	Reservado	3	4	5	5	5	4,4	Técnica
Tecnología/ Hardware									
	Equipos de Computación fijos	Reservado	3	1	4	4	3	3,0	Sistemas
	Servidores de aplicaciones	Compartido	3	2	4	4	4	3,4	Sistemas
	Servidores del Centro de Datos	Reservado	4	3	5	5	5	4,4	Sistemas
	Servidores web	Compartido	4	3	5	5	4	4,2	Sistemas
	Instrumentación especializada para monitoreo sísmico-volcánico	Reservado	3	2	5	5	5	4,0	Sism, Volc, Técn,

TIPO DE ACTIVOS	Descripción / Categoría	Clase (Reservado, Compartido, Público)	Valoración de Activos					Resultado Valoración	Responsable del Activo
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
	Unidades de pantalla interactiva y proyección	Reservado	2	5	4	3	3	3,4	Sism, Voc, Ieon, Sist
Comunic	Redes de monitoreo sísmico, volcánico	Reservado	3	1	5	5	5	3,8	Técnica
	Redes de comunicación por voz y telefonía	Compartido	2	4	4	3	3	3,2	Técnica, Sistemas
	Equipos de infraestructura de Red (switchs, routers, firewall)	Compartido	3	2	5	5	5	4,0	Técnica, Sistemas
	Intranet	Compartido	3	2	4	4	4	3,4	Técnica, Sistemas
	Internet	Público	1	2	3	4	4	2,8	Técnica, Sistemas
	Redes de transporte de datos de monitoreo sísmico, volcánico	Reservado	3	1	5	5	5	3,8	Técnica
Soporte de infor	Discos de almacenamiento	Reservado	3	4	4	4	4	3,8	Sistemas
	Cinta magnética	Reservado	2	4	4	3	4	3,4	Sistemas
	Unidades de respaldo de datos	Reservado	2	3	4	3	4	3,2	Sistemas
Pers	Directivos	Reservado	2	5	5	4	4	4,0	Dirección, Jefaturas
	Administradores	Reservado	3	1	1	2	2	1,8	Administración
	Operadores	Reservado	3	5	4	4	4	4,0	Sism, Voc, Ieon, Sist
	Clientes	Público	1	5	4	2	3		–

TIPO DE ACTIVOS	Descripción / Categoría	Clase (Reservado, Compartido, Público)	Valoración de Activos					Resultado Valoración	Responsable del Activo
			Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
Equipam	Central telefónica	Público	1	1	2	3	1	1,6	Técnica, Sistemas
	Suministro de energía y sistemas de respaldo	Reservado	2	1	5	5	4	3,4	Técnica, Sistemas
	Cableado Estructurado	Reservado	3	1	4	5	4	3,4	Técnica, Sistemas
	Controles de acceso físico	Reservado	3	1	2	2	2	2,0	Administración
Instala									
	Oficinas, edificios…	Compartido	1	1	5	5	4	3,2	Administración
	Gestión de la infraestructura física	Compartido	2	1	4	3	3	2,6	Administración
	sucursales	Compartido	2	1	3	3	4	2,6	Administración
Intang									
	Dedicación de la organización	Público	1	5	5	5	4	4,0	IG
	Competencia en investigación	Público	2	5	5	5	4	4,2	IG
	Generación de conocimiento	Público	2	5	5	5	4	4,2	IG
	Capacidad de respuesta y operación	Público	1	5	5	5	5	4,2	IG

Fuente: El Autor

3.2.3.2. Identificación y valoración de amenazas

En esta sección se identifica las amenazas a las que están expuestos los activos que intervienen en los procesos escogidos como se muestra en la Tabla 3.5; en donde se realiza la valoración de la probabilidad de ocurrencia de la amenaza, mediante el catálogo de Amenazas propuesto en el modelo SGSI y aplicando al caso de estudio.

3.2.3.3. Identificación de vulnerabilidades

Las vulnerabilidades existentes en los activos de información del Instituto Geofísico, que han sido identificadas durante el proceso de aplicación del modelo SGSI propuesto deben ser analizadas por el equipo de seguridad de la información de la institución.

Para el caso de estudio, se ha asignado la valoración de los activos en la Tabla 3.4 y se ha determinado la probabilidad de ocurrencia de las Amenazas, estos procedimientos son para los activos que intervienen en forma directa o indirecta sobre los procesos escogidos previamente.

Utilizando el formato propuesto en el modelo SGSI para la identificación de vulnerabilidades en los centros de investigación, se presenta el cuadro de identificación de vulnerabilidades de los activos más críticos para el caso de estudio en la Tabla 3.6:

Tabla 35 Catálogo de amenazas y Probabilidad de Ocurrencia, aplicado al Caso de Estudio

Procesos involucrados: 1. Gestión de Datos (adquisición, almacenamiento, procesamiento, interpretación y análisis) 2. Gestión de Acceso a la Información (usuarios internos y externos)	Metodología de Gestión del Riesgo		Versión Fecha: Aprobado por:
	Etapa 3	Identificación de riesgos	
	Sección 3.2	Catálogo de Amenazas	

ACTIVOS			VALORACIÓN DE LAS AMENAZAS					
TIPO DE ACTIVOS	Descripción / Categoría	Resultado Valoración del Activo	De origen natural	Del entorno (origen industrial)	Defectos de las aplicaciones	Causadas por las personas de forma accidental	Causadas por las personas de forma deliberada	Probabilidad de Ocurrencia de Amenazas
Servicios	Correo Electrónico	**3,0**	1,0	1,0	1,0	2,5	5,0	**2,1**
	Gestión de la infraestructura de redy arquitectura	**3,6**	1,0	1,0	2,5	2,5	2,5	**1,9**
	Comunicaciones con el medio externo	**4,2**	2,5	2,5	2,5	2,5	7,5	**3,5**
	Gestión de Información Documental	**3,8**	1,0	1,0	2,5	2,5	2,5	**1,9**
	Portal de servicios web	**3,8**	1,0	1,0	2,5	2,5	5,0	**2,4**
	Gestión de Datos y Documentos del Centro de Datos	**4,4**	1,0	1,0	1,0	2,5	2,5	**1,6**
	Gestión de Seguridad de la Información	**4,0**	1,0	1,0	1,0	5,0	5,0	**2,6**
	Gestión de Bases de Datos	**3,8**	1,0	1,0	2,5	2,5	2,5	**1,9**
Datos / Información	Datos adquiridos	**4,8**	1,0	2,5	2,5	5,0	2,5	**2,7**
	Datos procesados	**4,6**	1,0	2,5	2,5	2,5	2,5	**2,2**
	Datos almacenados	**4,6**	1,0	2,5	2,5	5,0	5,0	**3,2**
	Datos analizados e interpretados	**4,4**	1,0	2,5	2,5	5,0	2,5	**2,7**
	Bases de datos	**4,2**	1,0	2,5	2,5	2,5	2,5	**2,2**
	Directorio Activo	**2,8**	1,0	1,0	2,5	2,5	2,5	**1,9**
	Documentación de información del sistema	**2,8**	1,0	1,0	1,0	1,0	1,0	**1,0**

TIPO DE ACTIVOS	Descripción / Categoría	Resultado Valoración del Activo	De origen natural	De entorno (origen industrial)	Errores de las aplicaciones	Causadas por las personas de forma accidental	Causadas por las personas de forma deliberada	Probabilidad de Ocurrencia de Amenazas
Software:	Herramientas de Ofimática	**1,8**	1,0	1,0	1,0	2,5	1,0	**1,3**
	Software de Bases de Datos	**4,0**	1,0	1,0	2,5	2,5	2,5	**1,9**
	Software de Sistema	**3,6**	1,0	1,0	2,5	2,5	5,0	**2,4**
	Software de Aplicación	**4,0**	1,0	1,0	2,5	5,0	2,5	**2,4**
	Software Especializado	**4,8**	1,0	1,0	2,5	5,0	2,5	**2,4**
	Software Desarrollado localmente	**4,4**	1,0	1,0	2,5	5,0	2,5	**2,4**
Tecnología:		**0,0**						**0,0**
Hardware:	Equipos de Computación fijos	**3,0**	2,5	2,5	1,0	2,5	1,0	**1,9**
	Servidores de aplicaciones	**3,4**	2,5	2,5	2,5	2,5	1,0	**2,2**
	Servidores del Centro de Datos	**4,4**	2,5	2,5	2,5	2,5	2,5	**2,5**
	Servidores Web	**4,2**	2,5	2,5	2,5	2,5	2,5	**2,5**
	Instrumentación especializada para monitoreo sísmico-volcánico	**4,0**	5,0	5,0	5,0	5,0	2,5	**4,5**
	Unidades de pantalla interactiva y proyección	**3,4**	2,5	2,5	2,5	2,5	1,0	**2,2**
Comunic	Redes de monitoreo sísmico, volcánico	**3,8**	7,5	7,5	5,0	5,0	1,0	**5,2**
	Redes de comunicación por voz y telefonía	**3,2**	5,0	2,5	1,0	2,5	1,0	**2,4**
	Equipos de infraestructura de Red (switchs, routers, firewall)	**4,0**	2,5	2,5	5,0	5,0	5,0	**4,0**
	Intranet	**3,4**	1,0	1,0	2,5	1,0	1,0	**1,3**
	Internet	**2,8**	2,5	2,5	2,5	1,0	2,5	**2,2**

	Redes de transporte de datos de monitoreo sísmico, volcánico	**3,8**	7,5	5,0	2,5	5,0	2,5	**4,5**
TIPO DE ACTIVOS	**Descripción / Categoría**	**Resultado Valoración del Activo**	**De origen natural**	**Del entorno (origen industrial)**	**Errores de las aplicaciones**	**Causadas por las personas de forma accidental**	**Causadas por las personas de forma deliberada**	**Probabilidad de Ocurrencia de Amenazas**
Soportes de información:	Discos de almacenamiento	**3,8**	1,0	2,5	2,5	2,5	1,0	**1,9**
	Cinta magnética	**3,4**	2,5	2,5	2,5	2,5	1,0	**2,2**
	Unidades de respaldo de datos	**3,2**	2,5	2,5	2,5	2,5	1,0	**2,2**
Personal:	Directivos	**4,0**	1,0	1,0	1,0	1,0	1,0	**1,0**
	Administradores	**1,8**	1,0	1,0	1,0	1,0	1,0	**1,0**
	Operadores	**4,0**	2,5	2,5	1,0	1,0	1,0	**1,6**
	Clientes	**3,0**	1,0	1,0	1,0	1,0	1,0	**1,0**
Equipamiento auxiliar:	Central telefónica	**1,6**	1,0	1,0	1,0	1,0	1,0	**1,0**
	Suministro de energía y sistemas de respaldo	**3,4**	5,0	2,5	2,5	5,0	1,0	**2,2**
	Cableado Estructurado	**3,4**	2,5	2,5	2,5	2,5	1,0	**2,2**
	Controles de acceso físico	**2,0**	5,0	1,0	2,5	1,0	1,0	**2,1**
Instalaciones:	Oficinas, edificios…	**3,2**	2,5	2,5	2,5	1,0	1,0	**1,9**
	Gestión de la infraestructura física	**2,6**	1,0	1,0	1,0	1,0	1,0	**1,0**
	sucursales	**2,6**	2,5	2,5	2,5	1,0	1,0	**1,9**
Intangibles:	Credibilidad de la organización	**4,0**	2,5	1,0	2,5	2,5	5,0	**2,7**
	Competencia en investigación	**4,2**	1,0	1,0	1,0	2,5	1,0	**1,3**
	Generación de conocimiento	**4,2**	1,0	1,0	1,0	2,5	1,0	**1,3**
	Capacidad de respuesta y operación	**4,2**	2,5	2,5	5,0	5,0	1,0	**3,2**

Fuente: El Autor

Tabla 3.6 Cuadro de Identificación de vulnerabilidades en el Caso de Estudio

Procesos involucrados: 1. Gestión de Datos 2. Gestión de Acceso a la información	Metodología de Gestión del Riesgo		Versión: Fecha: Aprobado por:
	Etapa: 3	Identificación de riesgos	
	Sección: 3.3	Identificación de vulnerabilidades	

Activo	Vulnerabilidad	Origen de la Amenaza	Descripción de la Amenaza	Recomendaciones
Comunicaciones con el medio externo	No se han socializado los protocolos de comunicación y difusión de información	Causadas por las personas de forma deliberada	Las personas con acceso a sistemas de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Capacitaciones al personal interno y clientes
Portal de servicios web	No existen registros de gestión del servicio. Se desconoce las vulnerabilidades del portal	Causadas por las personas de forma deliberada	Las personas con acceso a sistemas de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Actualizar el registro de control de cambios. Realizar test programados de hackeo ético
Gestión de Seguridad de la Información	No se aplican procedimientos de cifrado en las BDD, no se aplica límite de intentos de acceso a los servicios	Causadas por las personas de forma deliberada	Las personas con acceso a sistemas de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Implementar un plan de control de accesos y actualización de permisos y contraseñas
	No existe planes de seguridad de la información en la institución	Causadas por las personas de forma accidental	Las personas con acceso a sistemas de información pueden ser causa de problemas no intencionados, por error o por omisión	Implementar el SGSI en la institución
Datos adquiridos	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	Las personas con acceso a sistemas de información pueden ser causa de problemas no intencionados, por error o por omisión	Establecer políticas de manejo de los datos
Datos procesados	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	Las personas con acceso a sistemas de información pueden ser causa de problemas no intencionados, por error o por omisión	Establecer políticas de manejo de los datos
Datos almacenados	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	Las personas con acceso a sistemas de información pueden ser causa de problemas no intencionados, por error o por omisión	Establecer políticas de manejo de los datos
Datos analizados e interpretados	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	Las personas con acceso a sistemas de información pueden ser causa de problemas no intencionados, por error o por omisión	Establecer políticas de manejo de los datos

Activo	Vulnerabilidad	Origen de la Amenaza	Descripción de la Amenaza	Recomendaciones
Software Especializado	Desconocimiento del funcionamiento de la herramienta	Causadas por las personas de forma accidental	Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, por error o por omisión	Programa de capacitación interna y asesoría de expertos en desarrollo y programación
Servidores del Centro de Datos	No existen registros válidos de acceso a los servidores	Causadas por las personas de forma deliberada	Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Implementar procesos de documentación del Centro de Datos
	Desconocimiento de las vulnerabilidades actuales en los servicios críticos	Causadas por las personas de forma accidental	Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, por error o por omisión	Realizar pruebas de vulnerabilidad y fallos de los servicios
Servidores Web	No existen registros válidos de acceso a los servidores	Causadas por las personas de forma deliberada	Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Implementar el registro de control de cambios.
	Desconocimiento de las vulnerabilidades actuales	Causadas por las personas de forma accidental	Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, por error o por omisión	Realizar pruebas de vulnerabilidad y fallos de los servicios
Instrumentación especializada para monitoreo sísmico-volcánico	No se ha implementado medidas de protección ante descargas atmosféricas en su totalidad	De origen natural	Accidentes naturales (terremotos, inundaciones, tormenta eléctrica).	Programar trabajos exclusivos de mejoramiento de la infraestructura tecnológica
	No se realiza el mantenimiento del sistema de energía alterno	De entorno (origen industrial)	Cortes del servicio de energía eléctrica e interrupción en las operaciones del centro de investigación	Realizar mantenimientos y pruebas de operación
	No se lleva un registro de actualizaciones y mantenimientos preventivos	De efectos de las aplicaciones	Problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación	Establecer planes de actualización de firmware y planes de mantenimiento programado
	Desconocimiento del funcionamiento de la herramienta	Causadas por las personas de forma accidental	Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, por error o por omisión	Programa de capacitación interna y asesoría de expertos en desarrollo y programación

Activo	Vulnerabilidad	Origen de la Amenaza	Descripción de la Amenaza	Recomendaciones
Redes de monitoreo sísmico, volcánico	No existen planes de mitigación del impacto ambiental en el equipamiento	De origen natural	Accidentes naturales (terremotos, inundaciones, tormenta eléctrica).	Establecer planes de mitigación y prevención ambiental
	No se realiza el mantenimiento del sistema de energía alterno	De entorno (origen industrial)	Cortes del servicio de energía eléctrica e interrupción en las operaciones del centro de investigación	Realizar mantenimientos y pruebas de operación
	No se lleva un registro de actualizaciones y mantenimientos preventivos	De errores de las aplicaciones	Problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación	Establecer procesos de control de calidad
	Desconocimiento del funcionamiento de la herramienta	Causadas por las personas de forma accidental	Las personas con acceso a sistemas de información pueden ser causa de problemas no intencionados, por error o por omisión	Programa de capacitación interna y asesoría de expertos en desarrollo y programación
Equipos de infraestructura de Red (switchs, routers, firewall)	No se realiza el mantenimiento del sistema de energía alterno	De entorno (origen industrial)	Cortes del servicio de energía eléctrica e interrupción en las operaciones del centro de investigación	Realizar mantenimientos y pruebas de operación
	No se lleva un registro de actualizaciones y mantenimientos preventivos	De errores de las aplicaciones	Problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación	Establecer procesos de control de calidad
	No existen planes de contingencia ante incidentes formales	Causadas por las personas de forma deliberada	Las personas con acceso a sistemas de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Diseñar, implementar el plan de contingencia en el área de TI y áreas involucradas
Discos de almacenamiento	No se lleva un registro de actualizaciones y mantenimientos preventivos	De errores de las aplicaciones	Problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación	Establecer políticas de manejo de respaldos, discos de almacenamiento portátiles, cintas magnéticas
	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma deliberada	Las personas con acceso a sistemas de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Establecer políticas de manejo de respaldos, discos de almacenamiento portátiles, cintas magnéticas
Credibilidad de la organización	No existen políticas de control de ingreso, permanencia y salida de empleados	Causadas por las personas de forma deliberada	Las personas con acceso a sistemas de información pueden ser causa de problemas intencionados: ataques deliberados, causar daños y perjuicios	Establecer políticas de contratación del personal, desarrollar programas de compensación del rol de la institución

Fuente: El Autor

3.2.3.4. Identificación de Controles existentes

Actualmente para los procesos en cuestión existen controles de acceso a los sistemas informáticos y controles de red, pero no son documentados, esto ocasiona que no se puedan desarrollar planes de acción constituidos, aprobados y actualizados, y los controles actuales no pueden ser evaluados. La gestión de datos y la gestión de acceso a estos datos es coordinada a nivel de actividades; en donde, los jefes de las áreas de sismología, volcanología, técnica y sistemas, establecen metas generales de cumplimiento de operaciones en cada área y el personal desarrolla soluciones, aplicaciones e implementa herramientas que permiten dinamizar e interrelacionar los procesos necesarios para la puesta en marcha de los servicios que entrega la institución.

Tabla 3.7 Catálogo de controles existentes

Activos		Controles Existentes			
Tipo	Activo	Control	Responsable	Estado de Operación	Observaciones
Software	Software Especializado	Acceso al sistema informático y aplicaciones	Administrador de Red	En ejecución	No existe documentación, No existe registro de cambios, historial de usuarios
Tecnología. Comunicaciones	Equipos de infraestructura de Red	Control de red	Administrador de Red	En ejecución	No existe registro de cambios, No existen guías y procedimientos de configuración actual No existe catálogo de incidentes de seguridad

Fuente: El Autor

La Tabla 3.7 sobre la plantilla del catálogo de controles existentes, se deberá actualizar después de implementar las etapas de identificación y gestión del riesgo, en donde se identificarán los controles necesarios para los procesos escogidos, que son el objetivo del estudio.

3.2.3.5. Valoración de impactos

En el literal 2.22 se propone la valoración del impacto para los centros de investigación. Para el caso de estudio, dicha valoración está relacionada a los activos críticos con sus vulnerabilidades, amenazas y probabilidad de ocurrencia, como se indica a continuación en la Tabla 3.8:

Tabla 38 Valoración del impacto para el caso de estudio

Procesos Involucrados: 1. Gestión de Datos 2. Gestion de Acceso a la Información		Metodología de Gestión del Riesgo Etapa: 3 Identificación de riesgos Sección 3.4 Valoración del Impacto				Versión Fecha: Aprobado por:	
Activos Críticos	Vulnerabilidad	Origen de la Amenaza	Probabilidad de ocurrencia de la amenaza	Escala de Probabilidad de Ocurrencia	Magnitud del Impacto (Porcentaje)	Escala de Impacto	Descripción del Impacto
Comunicaciones con el medio externo	No se han socializado los protocolos de comunicación y difusión de información	Causadas por las personas de forma deliberada	3,5	Baja	75%	Alto	Mayor impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Portal de servicios web	No existen registros de gestión del servicio. Se desconoce las vulnerabilidades del portal	Causadas por las personas de forma deliberada	2,4	Muy Baja	50%	Moderado	Moderado impacto medio sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Gestión de Seguridad de la Información	No se aplican propagimentos de cifrado en las BDD, no se aplica límite de intentos de acceso a los servicios	Causadas por las personas de forma deliberada	2,6	Baja	75%	Alto	Mayor impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
	No existen planes de seguridad de la información en la institución	Causadas por las personas de forma accidental	2,2	Muy Baja	75%	Alto	Mayor impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Datos adquiridos	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	2,7	Baja	75%	Alto	Mayor impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Datos procesados	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	2,2	Muy Baja	75%	Alto	Mayor impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Datos almacenados	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	3,2	Baja	75%	Alto	Mayor impacto alto sobre el valor del activo, afectando la disponibilidad, confidencialidad, integridad, autenticidad, trazabilidad

Activos Críticos	Vulnerabilidad	Origen de la Amenaza	Probabilidad de ocurrencia de la amenaza	Escala de Probabilidad de Ocurrencia	Magnitud del Impacto (Porcentaje)	Escala de Impacto	Descripción del Impacto
Datos analizados e interpretados	No existen políticas de eliminación de datos en medios electrónicos	Causadas por las personas de forma accidental	2,7	Baja	75%	Alto	Mayor, impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Software Especializado	Desconocimiento del funcionamiento de la herramienta	Causadas por las personas de forma accidental	2,4	Muy Baja	90%	Muy Alto	Crítico, impacto total sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Servidores del Centro de Datos	No existen registros validos de acceso a los servidores	Causadas por las personas de forma deliberada	2,5	Baja	50%	Moderado	Moderado, impacto medio sobre el valor del activo, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Servidores Web	No existen registros validos de acceso a los servidores	Causadas por las personas de forma deliberada	2,5	Baja	50%	Moderado	Moderado, impacto medio sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Instrumentacion especializada en monitoreo sismico volcánico	No se ha implementado medidas de protección ante descargas atmosféricas en su totalidad	De origen natural	4,5	Baja	75%	Alto	Mayor, impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Redes de monitoreo sísmico, volcánico	No existen planes de mitigación del impacto ambiental en el equipamiento	De origen natural	5,2	Media	50%	Moderado	Moderado, impacto medio sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Equipos de infraestructura de Red (switchs, routers, firewall)	No se realiza el mantenimiento del sistema de energía alterno	De entorno (origen industrial)	4,0	Baja	75%	Alto	Mayor, impacto alto sobre el valor del activo, afectando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
Discos de almacenamiento	No se lleva un registro de actualizaciones y mantenimientos preventivos	Defectos de las aplicaciones	2,2	Muy Baja	25%	Bajo	Menor, impacto leve sobre el valor del activo, afectando la disponibilidad, confidencialidad, integridad, autenticidad, trazabilidad
Credibilidad de la organización	No existen políticas de control de ingreso, permanencia y salida de empleados	Causadas por las personas de forma deliberada	2,7	Baja	25%	Bajo	Menor, impacto leve sobre el valor del activo, afectando la disponibilidad, confidencialidad, integridad, autenticidad, trazabilidad

Fuente: El Autor

3.2.3.6. Valoración de riesgos

Análisis del riesgo:

Partiendo de la definición de estimación de riesgo (pág. 82), la propuesta de probabilidad de ocurrencia de una amenaza (Tabla 2.23) y la valoración del Impacto (Tabla 2.24) del modelo SGSI, se presenta la Matriz de Estimación del riesgo para los procesos escogidos del Caso de Estudio.

De las tablas anteriores se ha realizado el cruce de información y se presenta como criterio de evaluación del riesgo; tomando como referencia la Tabla 2.25 se recomienda evaluar el riesgo sobre los activos con estimación "Muy Alto" y "Alto" como se indica a continuación:

Tabla 3.9 Estimación del riesgo para el caso de estudio

Procesos involucrados:	**Metodología de Gestión del Riesgo:**				**Versión:**
1. Gestión de Datos	**Etapa: 3**	**Identificación de riesgos**			**Fecha:**
2. Gestión de Acceso a la Información	**Sección: 3.5**	**Estimación del Riesgo**			**Aprobado por:**
Activos Críticos	**Probabilidad de ocurrencia de la amenaza**	**Escala de Probabilidad de Ocurrencia**	**Magnitud del Impacto (Porcentaje)**	**Escala de Impacto**	**Estimación del Riesgo**
Comunicaciones con el medio externo	3,5	Baja	75%	Alto	Alto
Portal de servicios web	2,4	Muy Baja	50%	Moderado	Bajo
Gestión de Seguridad de la Información	2,6	Baja	75%	Alto	Alto
Datos adquiridos	2,7	Baja	75%	Alto	Alto
Datos procesados	2,2	Muy Baja	75%	Alto	Medio
Datos almacenados	3,2	Baja	75%	Alto	Alto
Datos analizados e interpretados	2,7	Baja	75%	Alto	Alto
Software Especializado	2,4	Muy Baja	90%	Muy Alto	Alto
Servidores del Centro de Datos	2,5	Baja	50%	Moderado	Medio

Activos Críticos	Probabilidad de ocurrencia de la amenaza	Escala de Probabilidad de Ocurrencia	Magnitud del Impacto (Porcentaje)	Escala de Impacto	Estimación del Riesgo
Servidores Web	2,5	Baja	50%	Moderado	Medio
Instrumentación especializada para monitoreo sísmico-volcánico	4,5	Baja	75%	Alto	Alto
Redes de monitoreo sísmico, volcánico	5,2	Media	50%	Moderado	Medio
Equipos de infraestrucura de Red (switchs, routers, firewall)	4,0	Baja	75%	Alto	Alto
Discos de almacenamiento	2,2	Muy Baja	25%	Bajo	Muy Bajo
Credibilidad de la organización	2,7	Baja	25%	Bajo	Bajo

Fuente: El autor.

Los resultados obtenidos indican que los activos críticos a ser evaluados y que intervienen en los procesos escogidos son:

- Comunicaciones con el medio externo
- Gestión de Seguridad de la Información
- Datos adquiridos
- Datos almacenados
- Datos analizados e interpretados
- Software Especializado
- Instrumentación especializada para monitoreo sísmico-volcánico
- Equipos de infraestructura de Red (switchs, routers, firewall)

Los posibles riesgos sobre los activos no contemplados son considerados como riesgo asumible o aceptable por el Instituto Geofísico, para lo cual deberá constar en un documento formal autorizado por el Director del Instituto Geofísico. Debido a que es un análisis preliminar, los activos no contemplados y que se indican a continuación, pueden ser sujeto de observación y monitorización por parte del equipo de seguridad de la información:

- Portal de servicios web
- Datos procesados
- Servidores del Centro de Datos
- Servidores Web
- Redes de monitoreo sísmico, volcánico
- Discos de almacenamiento
- Credibilidad de la organización

Evaluación de riesgos: La evaluación de riesgos consiste en definir el criterio de aceptación del riesgo, comparando los resultados obtenidos de la estimación de riesgos y la aplicación de otras herramientas que pueden aportar al tratamiento de riesgos identificando las vulnerabilidades, amenazas e impactos. Para el caso de estudio se utilizó como herramienta adicional la aplicación MSAT (Microsoft Security Assessment Tool), los resultados finales se encuentran en detalle en el Anexo E.

3.2.3.7. Documentación – Etapa 3: Entregables

Tabla 3.10 Guía para la documentación de la etapa 3 Caso de estudio

Etapa 3: Entregables	Observaciones.- Información disponible en:	Verificación (Realizado SI / NO)	Estado (Revisión, Aprobación, Ejecución)
Matriz de activos	Identificación y valoración de activos Tabla 3.4: Identificación del activo de la información y valoración, aplicado al Caso de Estudio	SI	Revisión
Catálogo de amenazas	Identificación y valoración de amenazas Tabla 3.5: Catálogo de Amenazas y Probabilidad de Ocurrencia, aplicado al Caso de Estudio	SI	Revisión
Catálogo de vulnerabilidades	Identificación de vulnerabilidades Tabla 3.6: Cuadro de Identificación de vulnerabilidades en el Caso de Estudio	SI	Revisión
Catálogo de controles existentes	Identificación de Controles existentes Tabla 3.7: Catálogo de Controles existentes.	SI	Revisión
Valoración de impactos	Tabla 3.8: Valoración del Impacto para el Caso de Estudio	SI	Revisión
Matriz de riesgo (niveles del riesgo)	Estimación del riesgo Tabla 3.9: Estimación del Riesgo para el Caso de Estudio	SI	Revisión
Informe de evaluación de riesgos	Estimación del Riesgo Resultados obtenidos con MSAT, ANEXO E	SI	Revisión

Fuente: Metodología Magerit [21]

3.2.4. Etapa 4.- Gestión de riesgos

3.2.4.1. Tratamiento de riesgos

Para el caso de estudio, el tratamiento de riesgos aplicable a los procesos en cuestión requiere de:

- Matriz de riesgos inicial, que se ha obtenido de la Estimación del riesgo.
- Criterios de aceptación del riesgo, definidos por la comisión de seguridad de la información y la Dirección.

Tabla 3.11 Tratamiento de riesgo aplicado al caso de estudio

ACTIVOS CRITICOS (procesos 1 y 2)	ACCIONES PARA EL TRATAMIENTO DE RIESGOS	CALIFICACIÓN DEL RIESGO [21]
Comunicaciones con el medio externo	Reducir el riesgo	grave en el sentido de que requiere atención
Gestión de Seguridad de la Información	Reducir el riesgo	grave en el sentido de que requiere atención
Datos adquiridos	Reducir el riesgo	crítico en el sentido de que requiere atención urgente
Datos almacenados	Reducir el riesgo	crítico en el sentido de que requiere atención urgente
Datos analizados e interpretados	Reducir el riesgo	grave en el sentido de que requiere atención
Software Especializado	Reducir el riesgo	apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento
Instrumentación especializada para monitoreo sísmico-volcánico	Reducir el riesgo	crítico en el sentido de que requiere atención urgente
Equipos de infraestructura de Red (switchs, routers, firewall)	Reducir el riesgo	grave en el sentido de que requiere atención

Fuente: Metodología Magerit [21]

3.2.4.2. Selección de objetivos de control y controles

A continuación se presenta los objetivos de control y controles aplicables en los activos críticos relacionados a los procesos 1 y 2 del Caso de Estudio. La información es obtenida del catálogo de controles del modelo SGSI propuesto para centros de investigación de desastres naturales.

Tabla 3.12 Catálogo de controles aplicado al caso de estudio

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
	Comunicaciones con el medio externo	9.2 Gestión de acceso de usuario. 11.2 Seguridad de los equipos. 12.1 Responsabilidades y procedimientos de operación. 12.4 Registro de actividad y supervisión. 13.2 Intercambio de información con partes externas. 14.1 Requisitos de seguridad de los sistemas de información. 15.1 Seguridad de la información en las relaciones con suministradores. 15.2 Gestión de la prestación del servicio por suministradores.	9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 12.1.1 Documentación de procedimientos de operación. 12.4.2 Protección de los registros de información. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros.
	Gestión de Seguridad de la Información	5.1 Directrices de la Dirección en seguridad de la información. 6.1 Organización interna. 8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 8.3 Manejo de los soportes de almacenamiento. 10.1 Controles criptográficos. 12.1 Responsabilidades y procedimientos de operación. 12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica. 13.1 Gestión de la seguridad en las redes. 13.2 Intercambio de información con partes externas.	5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información. 6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos. 8.1.3 Uso aceptable de los activos. 8.2.1 Directrices de clasificación. 8.3.1 Gestión de soportes extraíbles. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
	Gestión de Seguridad de la Información	14.1 Requisitos de seguridad de los sistemas de información. 16.1 Gestión de incidentes de seguridad de la información y mejoras. 17.1 Continuidad de la seguridad de la información. 18.1 Cumplimiento de los requisitos legales y contractuales. 18.2 Revisiones de la seguridad de la información.	12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2.1 Controles contra el código malicioso. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 13.1.1 Controles de red
			13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto. 14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 16.1.1 Responsabilidades y procedimientos. 16.1.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. 16.1.6 Aprendizaje de los incidentes de seguridad de la información. 16.1.7 Recopilación de evidencias. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 18.1.1 Identificación de la legislación aplicable. 18.1.3 Protección de los registros de la organización. 18.2.2 Cumplimiento de las políticas y normas de seguridad. 18.2.3 Comprobación del cumplimiento.
	Gestión de la infraestructura de red y arquitectura	9.1 Requisitos de negocio para el control de accesos. 9.2 Gestión de acceso de usuario. 9.3 Responsabilidades del usuario. 9.4 Control de acceso a sistemas y aplicaciones. 10.1 Controles criptográficos. 12.1 Responsabilidades y procedimientos de operación. 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.4 Registro de actividad y supervisión.	9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3.1 Uso de información confidencial para la autenticación. 9.4.1 Restricción del acceso a la información.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
	Gestión de la infraestructura de red y arquitectura	12.6 Gestión de la vulnerabilidad técnica. 13.1 Gestión de la seguridad en las redes. 13.2 Intercambio de información con partes externas. 14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte.	9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas. 10.1.2 Gestión de claves. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4.1 Registro y gestión de eventos de actividad.
			12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.6.1 Gestión de las vulnerabilidades técnicas. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto. 14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3 Protección de las transacciones por redes telemáticas. 14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas. 14.2.6 Seguridad en entornos de desarrollo. 14.2.7 Externalización del desarrollo de software. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Datos adquiridos Datos procesados Datos almacenados Datos analizados e interpretados	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 9.4 Control de acceso a sistemas y aplicaciones. 12.1 Responsabilidades y procedimientos de operación. 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
	Datos adquiridos Datos procesados Datos almacenados Datos analizados e interpretados	14.2 Seguridad en los procesos de desarrollo y soporte. 14.3 Datos de prueba. 17.2 Redundancias.	12.1.1 Documentación de procedimientos de operación. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.6.1 Gestión de las vulnerabilidades técnicas. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.3.1 Protección de los datos utilizados en pruebas. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
Software:	Software Especializado	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 9.1 Requisitos de negocio para el control de accesos. 9.2 Gestión de acceso de usuario. 9.3 Responsabilidades del usuario. 9.4 Control de acceso a sistemas y aplicaciones. 10.1 Controles criptográficos. 12.1 Responsabilidades y procedimientos de operación. 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.4 Registro de actividad y supervisión. 12.5 Control del software en explotación. 12.6 Gestión de la vulnerabilidad técnica. 12.7 Consideraciones de las auditorías de los sistemas de información. 14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3.1 Uso de información confidencial para la autenticación. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas. 10.1.2 Gestión de claves. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.5.1 Instalación del software en sistemas en producción. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
	Instrumentación especializada para monitoreo sísmico-volcánico, oceanografía y meteorología Servidores del Centro de Datos	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 11.1 Áreas seguras. 11.2 Seguridad de los equipos.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. 8.2.1 Directrices de clasificación.
		12.1 Responsabilidades y procedimientos de operación. 12.6 Gestión de la vulnerabilidad técnica.	8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software.
	Redes de monitoreo sísmico, volcánico, oceanografía, meteorología Redes de transporte de datos de monitoreo sísmico, volcánico, oceanografía, meteorología	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 8.3 Manejo de los soportes de almacenamiento. 9.1 Requisitos de negocio para el control de accesos. 9.2 Gestión de acceso de usuario. 9.3 Responsabilidades del usuario. 9.4 Control de acceso a sistemas y aplicaciones. 10.1 Controles criptográficos.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. 8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3.1 Uso de información confidencial para la autenticación. 9.4.1 Restricción del acceso a la información. 9.4.4 Uso de herramientas de administración de sistemas. 10.1.2 Gestión de claves.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
	Redes de monitoreo sísmico, volcánico, oceanografía, meteorología Redes de transporte de datos de monitoreo sísmico, volcánico, oceanografía, meteorología	11.2 Seguridad de los equipos. 12.1 Responsabilidades y procedimientos de operación. 12.6 Gestión de la vulnerabilidad técnica. 13.1 Gestión de la seguridad en las redes. 13.2 Intercambio de información con partes externas. 14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte.	11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto. 14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3 Protección de las transacciones por redes telemáticas. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software.
	Discos de almacenamiento Cinta magnética Unidades de respaldo de datos	8.3 Manejo de los soportes de almacenamiento. 9.4 Control de acceso a sistemas y aplicaciones. 11.2 Seguridad de los equipos. 12.1 Responsabilidades y procedimientos de operación. 12.2 Protección contra código malicioso. 12.3 Copias de seguridad.	8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 11.2.1 Emplazamiento y protección de equipos. 11.2.4 Mantenimiento de los equipos. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información.

Tipo de Activos	Descripción / Categoría	Objetivos de Control	Controles Seleccionados
	Suministro de energía y sistemas de respaldo	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 11.1 Áreas seguras. 11.2 Seguridad de los equipos. 12.1 Responsabilidades y procedimientos de operación. 12.6 Gestión de la vulnerabilidad técnica.	8.1.3 Uso aceptable de los activos. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.2.1 Emplazamiento y protección de equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
	Oficinas, edificios… Gestión de la infraestructura física sucursales	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 11.1 Áreas seguras. 11.2 Seguridad de los equipos. 12.1 Responsabilidades y procedimientos de operación. 12.6 Gestión de la vulnerabilidad técnica.	8.1.1 Inventario de activos. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 12.1.1 Documentación de procedimientos de operación. 12.6.1 Gestión de las vulnerabilidades técnicas.

Fuente: El Autor

3.2.4.3. Implementación de controles

A continuación se indica la plantilla del proceso de aplicación de controles para mitigar el riesgo sobre los activos de información más relevantes para los procesos analizados del Caso de Estudio y que son establecidos por el Comité de Seguridad de la Información de la institución. Se especifica las entradas/habilitantes o condiciones actuales, limitaciones/restricciones del entorno, controles seleccionados y consecuencias en caso de implementar adecuadamente dicho control y su valoración que refleja el grado de capacidad para segmentar o eliminar la vulnerabilidad sobre el activo y el impacto en los procesos escogidos. El resumen de esta información es presentado en la Tabla 3.13:

- ***Restricciones:*** En el Instituto Geofísico se ha identificado las siguientes restricciones para la implementación de los controles en los procesos escogidos previamente:
  - Disponibilidad del recurso humano para asumir roles asignados por el equipo de seguridad de la información del Instituto Geofísico.
  - Carga horaria adicional destinada a la implementación de controles.
  - Limitaciones por falta del establecimiento de la política interna de la institución.

- Complejidad en la aplicación de herramientas de seguridad en ambientes con diversidad de tecnologías.

Tabla 3.13 Plantilla para registro de implementación de controles para el caso práctico

Activos Críticos	Controles seleccionados ISO 27001	Entradas	Objetivos específicos del control	Consecuencias	Estado	Valoración del Control
		(condiciones actuales, limitaciones, restricciones del entorno)			(control no implementado / en proceso / implementado)	Eficaz Insuficiente Injustificado Nulo
	8.1.1 Inventario de activos. 8.2.3 Manipulación de activos. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	- Sistemas de adquisición de datos sísmicos y volcánicos en ejecución - No existe documentación de las acciones del personal y procesos informáticos en ejecución para la adquisición de datos	-Establecer los procedimientos de manejo de los datos -Monitorizar la infraestructura Hw/Sw para la adquisición de datos. -Administrar el inventario de datos y conocer el estado de movimiento de datos	-Asignación de responsables de los datos adquiridos -Control de Continuidad de arribo de datos -Registro de uso de datos -Control de disponibilidad y capacidad de los equipos de adquisición de datos	Control el proceso de evaluación	--

Fuente: El Autor

3.2.4.4. Aceptación del riesgo y riesgo residual

La aceptación del riesgo es responsabilidad de los Directivos y del comité de seguridad de la información; para llegar a un consenso de aceptación del riesgo en los procesos 1 y 2 se analizan los resultados reflejados de:

- La estimación del riesgo (ver Tabla 3.9: Estimación del Riesgo aplicada al Caso de Estudio)
- Tratamiento del riesgo (ver Tabla 3.11: Tratamiento de riesgos aplicado al Caso de Estudio)
- Controles que van a implementarse (ver: Tabla 3.12 y 3.16 Implementación de Controles aplicado al Caso de Estudio)
- Criterios de valoración (ver: Definición de criterios de valoración para centros de investigación, Capítulo 2, Etapa 4)

En este ámbito se evidencian los riesgos residuales y deben ser monitorizados para asegurar que no sobrepasen los criterios de aceptación, esta actualización debe apoyarse con el registro de cambios que se establece en la Etapa 6, en donde se realiza la operación del SGSI.

3.2.4.5. Estrategia de protección y Plan de mitigación

En esta sección se realiza un resumen que facilita la revisión y cumplimiento del planteamiento de las estrategias y planes de seguridad, que se implementarán para mitigar los riesgos sobre los activos críticos identificados en el Tratamiento de los riesgos para los procesos 1 y 2 del Caso de Estudio, y se sustenta con los siguientes documentos:

- Estrategias de protección actual y enfoque de mitigación.
- Documentación obtenida de la aceptación del riesgo.
- Establecer el plan de trabajo de acciones inmediatas y ciclo de evaluaciones.

Estos documentos se generan a partir de los acuerdos que definen entre la Dirección y el Comité de Seguridad de la Información.

Para el Caso de Estudio, no fue posible realizar reuniones y acuerdos entre los miembros involucrados en este componente; por lo cual solamente se han establecido como referentes.

3.2.4.6. Declaración de aplicabilidad

Como se indicó en el Capítulo 2, la declaración de aplicabilidad es un documento formal en el cual se propone el plan de trabajo para implementar los controles seleccionados. La siguiente plantilla contiene los elementos que representan la Declaración de Aplicabilidad para el Caso de Estudio.

Tabla 3.14 Plantilla para Declaración de aplicabilidad - caso práctico

Procesos involucrados: 1. Gestión de Datos 2. Gestión de Acceso a la Información		Metodología de Gestión del Riesgo:				Versión	
		Etapa: 4	Gestión de Riesgos			Fecha:	
		Sección: 4.4	Declaración de Aplicabilidad			Aprobado por:	
Objetivo de Control	Control	Activos involucrados	Aplicabilidad del Control	Estado	Valoración del Control	Estimación de Recursos	
		(Activos contemplados por el Control)	(Descripción de procedimientos)	(Control Implementado / Control No Implementado / Control en Proceso)	Eficaz / Insuficiente / Injustificado / Nulo		

Fuente: El Autor

3.2.4.7. Comunicación del riesgo

En el Caso de Estudio, El Plan de Comunicación del Riesgo para los procesos 1 y 2 que debe presentar el Comité de Seguridad de la Información y transmitirlo a todas las áreas del Instituto Geofísico, deberá contener mediante un documento formal los objetivos propuestos en el análisis y gestión de riesgos, el plan de tratamiento, estrategias de protección y plan de mitigación.

3.2.4.8. Monitorización y Revisión del riesgo

En esta sección el objetivo es contribuir al ciclo de mejora continua del SGSI, y en el Caso de Estudio para los procesos escogidos previamente, el registro de cambios en los activos de información, vulnerabilidades, amenazas, impacto, riesgo e incidentes, deben ser documentados utilizando la plantilla de registro de monitorización y revisión del riesgo propuesta en el capítulo 2. (Tabla 2.30).

La plantilla propuesta debe ser actualizada continuamente, ya que los activos, controles, amenazas y vulnerabilidades son dinámicos y están en constante cambio, el proceso de mejora continua del SGSI depende de la efectiva monitorización y revisión del riesgo.

3.2.4.9. Documentación – Etapa 4: Entregables

Tabla 3.15 Guía para la documentación de la Etapa 4 caso de estudio

Etapa 4: Entregables	Observaciones.- Información disponible en:	Verificación (Realizado SI / NO)	Estado (Revisión, Aprobación, Ejecución)
Plan de tratamiento de riesgos	Tratamiento de riesgos	NO	--
Catálogo de controles y plan de implementación	Selección de objetivos de control y controles Implementación de controles	NO	--
Aceptación del riesgo y riesgos residuales	Aceptación del riesgo y riesgo residual Definición de criterios de valoración Estrategia de protección y Plan de mitigación	NO	--
Monitorización y revisión del riesgo	Comunicación del riesgo Monitorización y Revisión del riesgo	NO	--
Declaración de aplicabilidad	Declaración de aplicabilidad	NO	--

Fuente: El Autor

3.2.5. Etapa 5.- Componentes de gestión de seguridad de la información y objetivos de control

3.2.5.1. Políticas de seguridad

Las políticas de seguridad para los procesos escogidos previamente en el Caso de Estudio actualmente no son eficientes, no existe documentación formal o actualizada por el área de TI. El objetivo del modelo propuesto es orientar a la institución a la creación de políticas de seguridad. En el Capítulo 2 se indica dentro de las etapas 2 y 5, lo siguiente:

- La razón de implantar las políticas de seguridad en los centros de investigación
- Objetivos de las políticas de seguridad
- Asignación del personal responsable

De los resultados obtenidos en el Tratamiento de Riesgos, a continuación se puede recomendar se desarrollen las siguientes políticas de seguridad:

- Políticas de uso de correo electrónico
- Políticas de intercambio de información
- Políticas para usuarios de datos e información sísmica y volcánica
- Políticas de difusión de información y reportes de actividad sísmica y volcánica
- Políticas para el cumplimiento de las normas de seguridad establecidas, normativa legal vigente, requerimientos legales establecidos en la Etapa 1 del modelo SGSI propuesto.

La siguiente Tabla muestra los controles que recomienda la norma ISO 27001:2013 y los activos críticos asociados a los procesos del caso de estudio.

Tabla 3.16 Políticas de seguridad en los activos críticos

Dominio	Objetivos de Control y Controles	Activos Críticos
5. POLÍTICAS DE SEGURIDAD.	5.1 Directrices de la Dirección en seguridad de la información. 5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información.	Comunicaciones con el medio externo (medios de comunicación, observatorios externos, grupos de investigación). Presentar los productos y servicios asociados a gestión de datos y acceso a la información, mantener continuidad en la difusión de informes, reportes y datos hacia los interesados, mantener la imagen y credibilidad de la organización.
		Gestión de Seguridad de la Información. Establecer normas, procedimientos y coordinar la implementación del SGSI a nivel organizacional, recursos, accesos físicos y lógicos, comunicaciones, incidentes, garantizar la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de los activos.

Fuente: [4], El Autor

3.2.5.2. Aspectos organizacionales de la seguridad de la información

A continuación se menciona los aspectos organizacionales más relevantes que deben implantarse para sustentar el cumplimiento del SGSI propuesto en los procesos del Caso de Estudio.

- Formalización de responsabilidades en área de seguridad de la información asignadas a los empleados
- Definir las políticas de distribución de funciones
- Establecer el plan de difusión y concienciación de las políticas de seguridad
- Promover la asignación de recursos para fortalecer el sistema de seguridad de la información en la planificación de operaciones, inversión y proyectos de la institución
- Conformar el equipo de seguridad de la información definido en la Etapa 1: Definición de roles, responsabilidades y autoridades; y documentar formalmente las funciones asignadas.
- Generar el documento de confidencialidad para proteger la información sensible de la institución y establecer niveles de control de acceso a la información.
- Establecer los niveles de escalamiento para actuar en casos de presentarse incidentes de seguridad

La Tabla 3.17 presenta los aspectos organizativos en seguridad de la información para los activos críticos de los procesos en cuestión.

Tabla 3.17 Aspectos organizativos de seguridad de la información para activos críticos

Dominio	Objetivos de Control y Controles	Activos Críticos
6. Aspectos organizacionales de la seguridad de la información.	6.1 Organización interna. 6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos.	Gestión de Seguridad de la Información. Formalizar las responsabilidades de los Directivos, Jefes de área/unidad, Comité de Seguridad. Asignar formalmente responsables o propietarios de los activos, el modo de uso, mantenimiento y seguridad de los mismos. Efectuar acuerdos de confidencialidad y actualizaciones para proteger la información sensible de la institución.

Fuente: [4], El Autor

3.2.5.3. Gestión de activos

En el Caso de Estudio se puede evidenciar que el volumen de datos que arriba diariamente es muy importante para la generación de alertas tempranas; por lo que en los procesos 1 y 2 analizados los datos que se adquieren, almacenan, analizan e interpretan representan el activo de información más crítico. La gestión de activos se orienta al establecimiento de responsabilidad sobre los activos y a la clasificación de la información, como se indica a continuación en la Tabla 3.18:

Tabla 3.18 Controles para gestión de activos críticos

Dominio	Objetivos de Control	Activos Críticos
8. Gestión de activos.	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 8.3 Manejo de soportes de almacenamiento.	Datos adquiridos
		Datos almacenados
		Datos analizados e interpretados

Fuente: [4], El Autor

La gestión de activos promueve la asignación de un responsable para cada tipo de datos, que se encargará del uso del activo, así como, implementar los controles de seguridad para el activo, clasificar los activos, mantener el registro de inventario y definir los niveles de protección del activo.

Contribuye a monitorizar la valoración del activo y reportar los cambios, ya que puede afectar a los resultados del nivel de riesgo y las medidas de protección implantadas. Permite identificar los lineamientos de uso de datos adquiridos, datos almacenados, datos procesados y datos interpretados.

3.2.5.4. Control de accesos

El control de accesos a los datos e información en los procesos del Caso de Estudio, es administrado por el área de Sistemas, existen procedimientos para registrar el acceso remoto a los sistemas de información, estas medidas permiten controlar y registrar el uso de los datos y la información; sin embargo, se debe mejorar la

gestión aplicando registros de acceso, reemplazo de contraseñas de acceso y actualización de privilegios. Se deberá establecer políticas de control de acceso a los equipos remotos o portátiles

Tabla 3.19 Controles de acceso para activos críticos

Dominio	Objetivo de Control	Activos Críticos
9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos. 9.2 Gestión de acceso de usuario. 9.3 Responsabilidades del usuario. 9.4 Control de acceso a sistemas y aplicaciones.	Instrumentación especializada para monitoreo sísmico-volcánico
		Equipos de infraestructura de Red (switchs, routers, firewall)
		Comunicaciones con el medio externo
		Gestión de Seguridad de la Información
		Software Especializado
		Redes de transporte de datos de monitoreo sísmico, volcánico,

Fuente: [4], El Autor

Así también, es necesario implementar controles de acceso lógico en los servidores de adquisición, almacenamiento de datos, controles de acceso a la red, sistemas operativos y software especializado. Se debe implementar controles de acceso para la red de transporte de datos e instrumentación especializadas para monitoreo sísmico-volcánico, como se resume en la Tabla 3.19.

3.2.5.5. Cifrado

El comité de seguridad de la información presentará las políticas de criptografía y controles aplicables para los procesos del Caso de Estudio, designación de responsables del área de TI, conocimiento de uso de cifrado a los propietarios del activo, niveles de seguridad requeridos, métodos de cifrado apropiados para cada activo o grupos.

Las conexiones que se autoricen por acceso remoto a la red y a los servicios del centro de datos del Instituto Geofísico deben ser gestionadas mediante un registro de usuarios con autenticación y cifrado de datos.

La gestión de cifrado la realiza el responsable de seguridad, deberá implementar herramientas de administración de cifrado, registro de claves, entrega de claves segura, protección, actualización y eliminación de calves criptográficas.

3.2.5.6. Seguridad en las operaciones y comunicaciones

En el Caso de Estudio, para los procesos de adquisición de datos y acceso a la información se requiere mejorar la gestión en las operaciones y comunicaciones a través de la monitorización de procesos, procedimientos de respaldo de datos, controles de software dañino.

Estos aspectos se abordan con el cumplimiento de los controles establecidos en la ISO 27001:2013 en el dominio de seguridad de las operaciones y comunicaciones aplicados a los activos críticos obtenidos del tratamiento de riesgos, y se presentan a continuación en la Tabla 3.20.

Tabla 3.20 Controles de seguridad en las operaciones para activos críticos

Dominio	Objetivo de Control	Activos Críticos
12. Seguridad en las operaciones.	12.1 Responsabilidades y procedimientos de operación.	Instrumentación especializada para monitoreo sísmico-volcánico
	12.2 Protección contra código malicioso.	Equipos de infraestructura de Red (switchs, routers, firewall)
	12.5 Control del software en explotación.	Software Especializado
	12.6 Gestión de la vulnerabilidad técnica.	Redes de transporte de datos de monitoreo sísmico, volcánico.
13. Seguridad en las comunicaciones	13.1 Gestión de la seguridad en las redes	Soportes de información (Discos de almacenamiento, cinta magnética, unidades de respaldo de datos)
	13.2 Intercambio de información con partes externas	Suministro de energía y sistemas de respaldo
		Gestión de la infraestructura física

Fuente: [4], El Autor

Los propietarios de los activos deben contribuir a la gestión en las operaciones implementando un registro que contiene la configuración de los equipos y sistemas,

realizar respaldos de configuraciones, registrar los mantenimientos, cambios y actualizaciones.

El responsable de seguridad de la información debe monitorizar los procesos de seguridad en las operaciones, gestionar los procesos de respaldos de datos y verificar el cumplimiento de políticas para respaldar los datos, así también los controles de software dañino en los equipos que contienen software especializado para adquisición, almacenamiento, procesamiento e interpretación de datos.

3.2.5.7. Adquisición, desarrollo y mantenimiento de los sistemas de información

Los controles que se implanten son enfocados a los cambios del sistema de información, desarrollo de software, uso de aplicaciones que intervienen en los procesos de adquisición de datos y acceso a la información, como indica la Tabla 3.21 a continuación:

Tabla 3.21 Controles para sistemas de información

Dominio	Objetivo de Control	Activos Críticos
14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte.	Comunicaciones por redes públicas Software Especializado Software en desarrollo y aplicaciones Sistemas operativos Datos adquiridos, procesados, almacenados, analizados e interpretados Redes de monitoreo sísmico, volcánico y transporte de datos

Fuente: [4], El Autor

3.2.5.8. Gestión de incidentes en la seguridad de la información

En los casos de presentarse incidentes de seguridad de la información, estos deben ser comunicados oportunamente al responsable de seguridad de la información, cumpliendo con los niveles de escalamiento que establece el comité de seguridad de la información. En la Tabla 3.22 se indica los controles a ser aplicados que propone la norma ISO 27001:2013.

Tabla 3.22 Controles de gestión de incidentes para activos críticos

Dominio	Objetivos de Control y Controles	Activos Críticos
16. Gestión de incidentes en la seguridad de la información.	16.1 Gestión de incidentes de seguridad de la información y mejoras. 16.1.1 Responsabilidades y procedimientos. 16.1.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. 16.1.6 Aprendizaje de los incidentes de seguridad de la información. 16.1.7 Recopilación de evidencias.	Comunicaciones con el medio externo Gestión de Seguridad de la Información Software especializado

Fuente: [4], El Autor

Para los procesos en cuestión donde se han identificado las vulnerabilidades de los activos involucrados, se ha propuesto el registro de incidentes, y se ha establecido los roles del equipo de seguridad; es responsabilidad de la institución a través de sus áreas solucionar el incidente y reestablecer la disponibilidad de los activos involucrados.

- El responsable de seguridad deberá monitorizar que el incidente no produzca riesgos de seguridad adicionales y deberá mantener la actualización de los registros para tratamiento de riesgos.

- Los incidentes de seguridad y las soluciones deben ser documentados para que sean analizados por el responsable de seguridad y propietarios de los activos. Con ello, se promueve el aprendizaje ante incidentes de seguridad y se actualizan los controles implementados.

- Se debe actualizar el registro de incidentes que contenga toda la información del caso.

3.2.6. Etapa 6.- Operación del Sistema de Gestión de Seguridad de la Información. Aplicación al Caso de Estudio

3.2.6.1. Operación del SGSI

La operación del SGSI consiste en establecer un registro de **control de cambios** durante la aplicación del modelo de gestión de seguridad propuesto, en el que debe constar las actualizaciones en curso mientras se desarrolla cada etapa del modelo SGSI, con ello, se pretende realizar los ajustes del modelo al Caso de Estudio o Proyecto objeto de análisis.

El registro de control de cambios propuesto, permite monitorizar la gestión de la seguridad de la información desde un contexto organizacional.

Tabla 3.23 Registro de control de cambios para monitorización de la gestión de la seguridad de la información aplicado al caso de estudio

SGSI Utilizado:	Modelo de Gestión de Seguridad de la Información para centros de investigación, diagnóstico y prevención de desastres naturales	Fecha de Aprobación: Modificaciones: Responsables:		
Caso de Estudio:	Instituto Geofísico de la Escuela Politécnica Nacional			
Procesos/Áreas analizados	1) Gestión de datos sísmicos y volcánicos 2) Gestión del acceso a la información relacionada al monitoreo sísmico y volcánico			
Etapa 1: Fase de Preparación	✓ Obtener el apoyo de la Dirección ✓ Compromiso y liderazgo de la alta Dirección ✓ Definición de roles, responsabilidades y autoridades ✓ Planteamiento de recursos y competencias ✓ Identificar los requerimientos	Fecha de Aprobación:	Modificaciones	Responsables:
	Documentos habilitantes: ✓ Guía para la Documentación de la Etapa 1. Caso de Estudio			
Etapa 2.- Establecimiento del Modelo de Gestión de	✓ Definición del Alcance y Límites	Fecha de Aprobación:	Modificaciones	Responsables:

Seguridad de la Información	✓ Desarrollo de la política de seguridad de la información ✓ Definición de la metodología de gestión del riesgo ✓ Definición de los componentes de gestión de seguridad de la información ✓ Planteamiento de operación del SGSI			
	Documentos habilitantes: ✓ Guía para la Documentación de la Etapa 2. Caso de Estudio			
Etapa 3.- Identificación de los riesgos	✓ Identificación y valoración de activos ✓ Identificación y valoración de amenazas ✓ Identificación de vulnerabilidades ✓ Identificación de Controles existentes ✓ Valoración de impactos ✓ Valoración de riesgos ✓ Análisis del riesgo ✓ .- Identificación del riesgo ✓ .- Estimación del riesgo ✓ Evaluación de riesgos	Fecha de Aprobación:	Modificaciones	Responsables:
	Documentos habilitantes: ✓ Guía para la Documentación de la Etapa 3. Caso de Estudio			
Etapa 4.- Gestión de riesgos	✓ Tratamiento de riesgos ✓ Selección de objetivos de control y controles ✓ Implementación de controles ✓ Aceptación del riesgo y riesgo residual ✓ Definición de criterios de valoración ✓ Estrategia de protección y Plan de mitigación ✓ Declaración de aplicabilidad ✓ Comunicación del riesgo ✓ Monitorización y Revisión del riesgo	Fecha de Aprobación:	Modificaciones	Responsables:
	Documentos habilitantes: ✓ Guía para la Documentación de la Etapa 4. Caso de Estudio			

Etapa 5.- Componentes de gestión de seguridad de la información y objetivos de control en los centros de investigación	✓ Políticas de seguridad ✓ Aspectos organizacionales de la seguridad de la información ✓ Gestión de activos ✓ Control de accesos ✓ Cifrado ✓ Seguridad en las operaciones ✓ Adquisición, desarrollo y mantenimiento de los sistemas de información ✓ Gestión de incidentes en la seguridad de la información	Fecha de Aprobación:	Modificaciones	Responsables:
	Documentos habilitantes: ✓ Resultados obtenidos de los controles implementados			
Etapa 6.- Operación del Sistema de Gestión de Seguridad de la Información	✓ Operación del SGSI ✓ Términos y definiciones ✓ Evaluación de la funcionalidad de las etapas modelo y medidas correctivas ✓ Establecimiento de programas de auditoría interna y externa ✓ Revisiones y aprobaciones por parte de la Dirección ✓ Documento de Seguridad ✓ Certificación del SGSI	Fecha de Aprobación:	Modificaciones	Responsables:
	Documentos habilitantes: ✓ Actualizaciones			

Fuente: El Autor

3.2.6.2. Términos y definiciones

Esta sección debe ser complementada con los términos y definiciones que vaya requiriéndose dependiendo de la aplicación del modelo SGSI propuesto. El Anexo G, presenta un conjunto de definiciones tomadas de la metodología Magerit en el Libro 1 - Método, así también los términos y definiciones del centro de investigación Instituto Geofísico.

3.2.6.3. Evaluación de la funcionalidad de las etapas modelo y medidas correctivas

Para el caso de estudio, se ha evaluado las etapas del modelo que son aplicables a los procesos de adquisición de datos y gestión de acceso a la información. Durante la aplicación del modelo SGSI se obtuvieron resultados parciales, ya que a partir de la Etapa 4 sobre Gestión de riesgos, no fue posible conformar el equipo de seguridad oficial y por tanto la aprobación de la Dirección.

Se debió continuar la revisión de las etapas siguientes a manera de propuestas y lineamientos hasta conseguir acuerdos de reasignación de funciones para el personal en el tema de seguridad de la información.

Durante la aplicación modelo SGSI en el caso de estudio, se han propuesto formatos de diseño y se han agregado plantillas que faciliten la estructura y levantamiento de información del SGSI. El modelo propuesto permite la ampliación del alcance si fuese decisión de los Directivos de la institución debido a que está enfocado en el ciclo de mejora continua.

El objetivo de este componente ha sido identificar los conflictos durante la implementación del modelo SGSI y las causas negativas por las que no se ha cumplido una etapa, como son:

- Decisión de los Directivos en suspender temporalmente la implementación del SGSI debido al re direccionamiento del recurso humano, económico y tecnológico, frente a un fenómeno sísmico y/o volcánico de gran trascendencia, ocasionando el incumplimiento en las funciones asignadas al equipo de Seguridad de la Información.

Para el Caso de Estudio, los componentes de la Etapa 6 restantes relacionados a auditoría, revisiones y aprobaciones de la Dirección, documento de seguridad y lineamientos de certificación; han sido considerados procesos en espera de implementación, ya que dependen de la aprobación de las etapas anteriores y toma

de decisión de los Directivos, indispensable para culminar la implementación de cada etapa del modelo. En el Capítulo 2 se ha propuesto los lineamientos para la ejecución de todos los componentes de la Etapa 6, en el caso de tener la autorización de la Dirección para implementar el modelo SGSI propuesto.

3.3. Análisis de Resultados

El modelo de gestión SGSI aplicado al caso de estudio "Instituto Geofísico" ha representado un aporte valioso al área de TI a través del reconocimiento de los activos de información más críticos y la propuesta que debe adoptarse para identificar los riesgos y cómo gestionarlos.

Respecto a las funciones que realiza la alta dirección, esta ha reconocido la importancia de encaminar recursos humanos, tecnológicos y económicos generando una nueva perspectiva orientada en la gestión de seguridad de la información.

A nivel estratégico se ha valorado la importancia de implementar estándares y metodologías similares a las utilizadas por centros de investigación internacionales, esto contribuye a la inclusión de las redes locales de monitoreo sísmico y volcánico para que formen parte de redes mundiales dedicadas a la prevención de desastres naturales y gestión de riesgos.

La implementación del modelo ha requerido del respaldo de la Dirección, contar con la revisión y aprobación de los avances en cada etapa, e impulsar los roles del equipo de seguridad de la información. Estos requerimientos son indispensables y garantizan el cumplimiento de objetivos del SGSI; por tal motivo, en el caso práctico se obtuvo resultados parciales logrando el levantamiento de la información, identificación de activos, análisis de riesgos y únicamente el planteamiento de lineamientos para las etapas finales.

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

1. La implementación del modelo SGSI en el caso práctico confirma que para el cumplimiento de cada etapa se debe contar con la revisión y aprobación por parte de la Dirección y el Comité de Seguridad de la Información, esto permite consolidar los resultados de gestión de seguridad obtenidos. Sin ello, no es factible la ejecución del SGSI, comprobando que a partir de la Etapa 4 – Gestión de Riesgos, es indispensable revisar y aprobar los avances, caso contrario solo se podrá establecer lineamientos o referencias para las etapas siguientes como se ha demostrado en la aplicación del modelo en el Capítulo 3.

2. De acuerdo con la identificación del riesgo en la Etapa 3, se confirma que existen más procesos susceptibles de ser vulnerados y que participan como procesos de apoyo o son procesos estratégicos del Caso de Estudio.

3. Durante el estudio realizado en el capítulo I, se identificó que los centros de investigación de desastres naturales del Ecuador, mantienen sus sistemas de información y entrega de servicios de información en cumplimiento y con respuesta adecuada a las demandas de los usuarios. Sin embargo, la mayoría de estos procesos no están documentados, carecen de métodos y controles de seguridad de la información, lo cual, conlleva a tener sistemas de información vulnerables a amenazas como: pérdida de información, retardos de respuesta en la determinación de alertas tempranas, fallos en la infraestructura de red, daños en el hardware/software ocasionados por errores del personal, virus, software malicioso y hackers. El modelo de seguridad propuesto, puede ser utilizado como referente para la identificación de falencias en los sistemas de información de los centros de investigación, como se ha demostrado en la aplicación del modelo SGSI en las Etapas 1, 2 y 3.

4. En el modelo propuesto, para el establecimiento de controles en los sistemas de información se utiliza la guía de objetivos de control y controles de la norma ISO/IEC 27001:2013. Aplicándolos al caso práctico, se puede concluir que permiten una orientación a nivel de gestión de la seguridad de la información y permiten comprobar si los riesgos asociados a los activos de información conducen al establecimiento de las políticas para cada área de aplicación.

5. En el modelo propuesto las etapas de identificación de riesgos (Etapa 3) y gestión de riesgos (Etapa 4) contienen los aspectos más relevantes tomados de distintas metodologías de gestión de riesgos para consolidar un modelo propio aplicable a los centros de investigación de desastres naturales que asegure resultados integrales que comprenden varios aspectos para identificar y gestionar los riesgos en forma adecuada.

6. El modelo propuesto de seguridad SGSI permite agregar nuevos activos de información y registrar nuevos eventos de vulnerabilidad, riesgos, controles, con una adecuada documentación y control de cambios, a través de la monitorización y revisión del riesgo (Etapa 4) y en la evaluación de la funcionalidad y medidas correctivas (Etapa 6). Con ello se asegura la capacidad de mejoramiento continuo que propone modelo y lo distingue de los modelos y estándares existentes.

7. Durante la aplicación del modelo propuesto, en la identificación y análisis de riesgos se comprobó que la estimación del riesgo depende de las valoraciones previas de activos, vulnerabilidades, amenazas e impacto que se determinan con el equipo de seguridad de la información y los usuarios. Esto demuestra que para lograr una estimación de riesgo más cercana a la realidad en los activos de información de los centros de investigación, se debe realizar un consenso y el equipo de seguridad de la información deberá reunir varios criterios para definir su valoración.

8. Las metodologías de gestión de riesgos Magerit, Octave, NISTSP 800-30, Coras y norma ISO 27005 consideradas en el presente estudio contienen aspectos similares para llegar a la determinación de riesgos en seguridad de la información, por lo tanto, cada una ha aportado al desarrollo del modelo en las Etapas 3 y Etapa 4, en donde se ha logrado consolidar una estructura adaptable para los centros de investigación. Así también, tomando como referencia las metodologías OCTAVE y CORAS, se diseñó la Etapa 1: Fase de Preparación, pero no solo orientada a la gestión de riesgos sino a todo el contexto del Modelo de Gestión de Seguridad de la Información.

9. Para el Caso de Estudio, se ha identificado que no existe documentación de los procesos y cambios relacionados a la seguridad de la información que se ejecutan en todas las áreas, la infraestructura de red no tiene diagramas y documentos actualizados; por lo que, los recursos, tiempo y asignación de personal para implementar el modelo SGSI en todos los procesos de la institución serán mayores a los contemplados en la planificación, o, en su defecto se debe recurrir a la contratación de terceros para mejorar procesos puntuales del área de TI.

10. El estudio exploratorio de los modelos y estándares de seguridad realizado en el Capítulo II, se orienta a la selección de componentes que cubran las necesidades de los centros de investigación para gestionar los datos y el acceso a la información, obteniendo la conformación de etapas del modelo SGSI propuesto que no se presentan en ningún modelo/estándar existente.

4.2. Recomendaciones

1. El modelo de gestión de seguridad conformado en el Capítulo II contiene seis etapas para consolidar el ciclo de vida y mejoramiento continuo del SGSI, por lo que se recomienda implementar, controlar y monitorear las etapas mediante la Guía de Entregables y sustentar formalmente el cumplimiento de los procesos

de gestión de seguridad de la información con el respaldo y aprobación del Comité de Seguridad de la Información y los Directivos.

2. Los activos de información que se hayan definido como críticos deberán ser analizados en el corto plazo para establecer los planes de mitigación del riesgo, mientras que los riesgos asumibles deben ser monitoreados debidamente para controlar sus efectos en los activos de información y tratarlos a tiempo para garantizar la continuidad de las operaciones del centro de investigación.

3. Para mejorar la gestión del Centro de Datos del Instituto Geofísico se requiere establecer las políticas de seguridad para el centro de datos, implementar herramientas que faciliten los registros de los procesos ejecutados, control de cambios, control de accesos, documentación de los procedimientos operativos.

4. Como parte de la aplicación del SGSI en los centros de investigación es recomendable concientizar a todo el personal de estas instituciones en la adopción de una cultura de seguridad de la información mediante talleres de entrenamiento y capacitación.

5. Se debe fortalecer el conocimiento de seguridad en el personal de TI y analizar en las aplicaciones existentes las configuraciones que aporten en la administración y operación de la seguridad de los activos de información.

6. Para analizar y gestionar los riesgos de seguridad de la información en todos los procesos o solo los requeridos por la institución, se puede hacer uso del modelo SGSI propuesto ya que contiene los elementos necesarios adoptados de las normas ISO 27001, ISO 27005 y metodologías Magerit, OCTAVE, NIST_SP800, CORAS aplicados a los requerimientos de los centros de investigación de desastres naturales.

7. Como medida temporal se puede conformar el equipo de seguridad de la información haciendo uso del personal existente, asignando las responsabilidades y tareas de acuerdo a las competencias del personal y su

disponibilidad, considerar la redistribución de tareas y funciones, para lograr adaptar en la estructura organizacional de la institución las demandas establecidas en el alcance del SGSI.

8. El modelo SGSI propuesto puede ser un referente para auditorías de seguridad de la información, ya que ha sido estructurado en base a la norma ISO 27001, ISO 27005 y se han adaptado procesos de metodologías como Magerit, Octave, NISTSP 800-30, Coras. En el caso de ser aplicado puede ser orientado a la obtención de la certificación de la norma ISO 27001.

9. La implementación del modelo SGSI requiere del respaldo de los Directivos, aprobación y participación durante el desarrollo de cada Etapa, ya que implica la toma de decisiones, asignación de recursos, revisiones, aprobaciones y compromiso de la ejecución del plan de mejoramiento continuo del SGSI. De no cumplir con este rol por parte de la Dirección y Jefaturas de cada área / unidades no se conseguirá los resultados esperados y representará pérdida de recursos, esfuerzos para la institución, los riesgos y vulnerabilidades potenciales seguirán ocultos sin establecerse medidas de seguridad efectivas.

10. En el modelo de gestión de seguridad de la información también se considera como medida para el tratamiento de riesgos la posibilidad de transferir el riesgo, es decir que el comité de seguridad de la información en conjunto con la Dirección deberán analizar los factores económicos, financieros, tecnológicos que disponen para mitigar los riesgos de seguridad con un análisis más exhaustivo de la organización y apoyándose en el modelo SGSI propuesto, o destinar el riesgo a terceros para que sea gestionado adecuadamente.

11. El modelo SGSI propuesto fue enfocado para aplicarlo a centros de investigación de desastre naturales, se requiere revisar a detalle la funcionalidad de los componentes en cada etapa y mayor afinamiento para que constituya un modelo aplicable. Sin embargo en su estructura, es posible agregar mejoras y evaluaciones de funcionalidad del modelo que se han establecido en la Etapa 6: Operación del Sistema de Gestión de Seguridad de la Información.

REFERENCIAS

[1] Information Security Management Systems, «Sitio web de ISO» [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:ed-1:v1:en. [Último acceso: 08 Marzo 2015].

[2] Data Center, «Grupo GTD – Data Center,» [En línea]. Available: http://www.grupogtd.com/. [Último acceso: Diciembre 2014].

[3] Retos en la adopción de cloud computing, «Sitio web de Fundación IE» [En línea]. Available: http://www.ie.edu/fundacion_ie/Home/Documentos/Seguridad_en_la_Informaci%C3%B3n_Retail_y_GC_Fundaci%C3%B3n_IE_y_Ernst_&_Young_2.pdf, pág: 22. [Último acceso: 21 enero 2015].

[4] ISO 27000. (2015), «Sitio web de ISO 27000» [En línea]. Available: http://www.iso27000.es. [Último acceso: 03 septiembre 2015].

[5]. INOCAR, «Sitio web de Inocar» [En línea]. Available: http://www.inocar.mil.ec/web/index.php/institucion/. [Último acceso: 01 abril 2015].

[6] C.C.F.F.A.A., Estructura Orgánica, «Sitio web de CCFFAA » [En línea]. Available: http://www.ccffaa.mil.ec, [Último acceso: Abril 2015].

[7] COGMAR, Organigrama Estructural de la Fuerza Naval, «Sitio web de armada » [En línea]. Available: http://www.armada.mil.ec/organigrama, [Último acceso: 08 Marzo 2015].

[8] DIRTIC, Organigrama Dirección de Tecnologías de la Información y Comunicaciones, «Sitio web de armada» [En línea]. Available: http://www.dirtic.armada.mil.ec, [Último acceso: Marzo 2015].

[9] Plan 2015, Gobierno por Resultados INOCAR, «Sitio web de Inocar » [En línea]. Available: http:// http://www.inocar.mil.ec/web/images/lotaip/2015/literal_a/A.4_Metas_objetivos_ABR_2015.pdf, [Último acceso: Mayo 2015].

[10] Presentación Instituto Geofísico IG, «Sitio web de Instituto Geofísico » [En línea]. Available: http:// http://www.igepn.edu.ec/nosotros, [Último acceso: Diciembre 2015].

[11] INAMHI, Estado Ecuatoriano. (13 de octubre de 2013). Recuperado el 15 de Noviembre de 2015, «Sitio web de INAMHI » [En línea]. Available: http://www.serviciometeorologico.gob.ec/ejes-estrategicos/, [Último acceso: junio 2015].

[12] ISO Survey, World distribution of ISO/IEC 27001 certificates in 2014, «Sitio web de ISO Survey» [En línea]. Available: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=EC#countrypick, [Último acceso: Diciembre 2015].

[13] Kroll Ontrack. Empresa consultora, «Sitio web de Kroll Ontrack» [En línea]. Available: http://www.ontrackdatarecovery.es/sala-de-prensa/62386/los-fallos-en-el-disco-duro-son-la-principal/#.VrqmJvl_Oko, [Último marzo 2015].

[14] ISO 27001:2013, Diagrama del proceso de implementación y certificación de la norma ISO27001:2013, «Sitio web de normas iso» [En línea]. Available: http://www.normas-iso.com/iso-27001, [Último acceso: noviembre 2015].

[15] Claves del éxito para la gestión de riesgos, IsoTools Excellence, «Sitio web de» [En línea]. Available: https://www.isotools.org/2015/02/12/iso-27001-pasos-implantacion-politica-seguridad-procedimientos/, [Último acceso: julio 2015].

[16] Sistema de gestión de la seguridad de la información. UOC, Autores: D. Cruz A y S. Garre Gui. «Sitio web de unad» [En línea]. Available: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-14-agosto-2013/411_estructura_organizacional_en_seguridad_para_el_sgsi.html, [Último acceso: mayo 2015].

[17] Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 2005:2012, pág. 18-22, «Sitio web de normas inen ecuador» [En línea]. Available:http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO_2014/GAN/nte_inen_iso_iec_27005extracto.pdf [Último acceso: septiembre 2015].

[18] Dependencias: Activos en capas, Fuente: Magerit_V3_libro1, pág. 23

[19] Valoración y Dimensiones. Fuente: Magerit_V3_libro1, pág. 24

[20] MAGERIT, Libro 2, Catálogo de elementos, Criterios de Valoración, pág. 16 y 19

[21] MAGERIT, Libro 1, Método, Magerit_V3, Libro 1, pág. 22, 27, 28, 35, 45, 47

[22] ISO 27001, Identificación de amenazas

[23] NIST SP800-30, «Sitio web de csrc - nist» [En línea]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf, [Último acceso: diciembre 2015].

[24] Auditoría y Certificación ISO27001:2013, «Sitio web de iso27000» [En línea]. Available: http://iso27000.es/certificacion.html, [Último acceso: junio 2015].

[25] Servicios del Instituto Geofísico – EPN, «Sitio web de Instituto Geofísico» [En línea]. Available: http://www.igepn.edu.ec/servicios, [Último acceso: diciembre 2015].
[26] Interior, U. D. (28 de Septiembre de 2015). *Supporting and Enabling USGS Data Management*, «Sitio web de usgs » [En línea]. Available:http://www.usgs.gov/datamanagement/backup.php, [Último acceso: octubre 2015].

[27] RIESGOS ASOCIADOS AL CLOUD COMPUTING, pág.: 54-99, «Sitio web de cfnavarra » [En línea]. Available: http://www.cfnavarra.es/observatoriosi/pdf/estudio_inteco_cloud_computing_en_sector_publico/estudio_inteco_cloud_computing_en_sector_publico.pdf, [Último acceso: noviembre 2015].

[28] Cloud Computing. Retos y Oportunidades, pág.: 157, «Sitio web de ontsi » [En línea]. Available: http://www.ontsi.red.es/ontsi/sites/default/files/1_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf, [Último acceso: noviembre 2015].

[29] Recovery Labs. Compañía de seguridad informática, «Sitio web de recoverylabs» [En línea]. Available: http://www.recoverylabs.com/ayuda-y-soporte/data-recovery-white-papers/informes/principales-factores-que-causan-una-perdida-de-informacion/

[30] Grupo ALBE. Empresa de consultoría. Accounting Software, «Sitio web de grupo ALBE » [En línea]. Available: http://www.grupoalbe.com/beneficios-de-implementar-un-drp-disaster-recovery-plan-en-las-organizaciones-pymes/

[31] Cycorp. Empresa de tecnología, «Sitio web de cycorp » [En línea]. Available: http://cycorp.cl/bacula-enterprise/

[32] IT Users Tech&Business. Revista digital, «Sitio web de ituser» [En línea]. Available: http://www.ituser.es/seguridad/2015/06/perdida-de-datos-errores-mas-comunes-y-como-subsanarlos

[33] An Assessment Model of Information Security Implementation Levels, Stambul, M.A.M.; Centre of Software Technol. & Manage, «Sitio web de ieeexplore » [En línea]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6021561&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F6011492%2F6021499%2F06021561.pdf%3Farnumber%3D6021561

[34] Implementación efectiva de un SGSI ISO 27001, Autor: Rodrigo Baldecchi Q, «Sitio web de isaca » [En línea]. Available: http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

[35] Secretaria Nacional de la Administración Pública. (23 de enero de 2014). IMPLEMENTACIÓN, CONTROL Y SEGUIMIENTO DE LA SEGURIDAD DE LA ADMINSTRACIÓN CENTRAL E INSTITUCIONAL, «Sitio web de administración pública » [En línea]. Available:http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2015/04/PROYECTO-IMPLEMENTACION-CONTROL-Y-SEGUIMIENTO.pdf

[36] Agencia Española de Protección de datos. (7 de enero de 2016). Guía de seguridad de Datos, «Sitio web de agpd» [En línea]. Available: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf

[37] Baker, K. (14 de noviembre de 2007). U.S. Geological Survey Manual, «Sitio web de usgs» [En línea]. Available:http://www.usgs.gov/usgs-manual/600/600-5.html

[38] EPN, I. G. (14 de mayo de 2015). Cartera de productos y servicios IG, «Sitio web de EPN » [En línea]. Available: www.igepn.edu.ec

[39] Escuela Politécnica Nacional. (3 de enero de 2014). Plan estratégico de Desarrollo Institucional. «Sitio web de IG-EPN» [En línea]. Available: www.epn.edu.ec

[40] Instituto Geofísico. (18 de enero de 2015). Misión - visión. Recuperado el 7 de Enero de 2016, «Sitio web de IG-EPN» [En línea]. Available: www.igepn.edu.ec

[41] Interior, U. D. (28 de septiembre de 2015). Supporting and Enabling USGS Data Management, «Sitio web de usgs » [En línea]. Available: http://www.usgs.gov/datamanagement/index.php

[42] ISMS, C. (27 de enero de 2005). CTBTO Information Security Management System Support on Call-off Basis, «Sitio web de ctbto» [En línea]. Available: http://www.ctbto.org/fileadmin/user_upload/procurement/2008/RFP2010-0063-ANNEX_B-SOW.pdf

[43] Coras Project, “A Platform for Risk Analysis of Security Critical Systems”, Junio 2001, «Sitio web de Coras» [En línea]. Available: http://www2.nr.no/coras

[44] Ingelan. Soluciones de seguridad, «Sitio web de ingelan » [En línea]. Available: http://www.ingelan.com/?p=4683

[45] CTBTO. Information Security Management, «Sitio web de CTBTO » [En línea]. Available: http://www.ctbto.org/fileadmin/user_upload/procurement/2008/RFP2010-0063-ANNEX_B-SOW.pdf

[46] INAMHI. Organigrama, «Sitio web de INAMHI» [En línea]. Available: http://www.serviciometeorologico.gob.ec/organigrama/

[47] INOCAR. Estructura Orgánica 2014, «Sitio web de INOCAR» [En línea]. Available: http://www.inocar.mil.ec/web/images/lotaip/2014/seccion1/A._Estructura_organica_vigente_2014.pdf

[48] IG-EPN. Organigrama, «Sitio web de IG-EPN» [En línea]. Available: http://www.igepn.edu.ec/nosotros/organigrama

[49] OCTAVE. Enfoque Octave, «Sitio web Software Engineering Institute» [En línea]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546

ANEXOS

Los anexos mencionados a continuación se presentan en formato digital:

ANEXO A: Planes Estratégicos INAMHI, INOCAR, IG

ANEXO B: Marco Legal - Ecuador

ANEXO C: Información USGS

ANEXO D: Productos y Servicios INAMHI, INOCAR, IG

ANEXO E: Resultados de evaluación mediante MSAT

ANEXO F: Relación de normas y metodologías respecto al modelo SGSI propuesto

ANEXO G: Términos y Definiciones

ANEXO H: Propuesta de implementación - Resumen Ejecutivo

ANEXO I: Catálogo de controles para los centros de investigación