ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

APLICACIÓN DE LAS NORMAS TÉCNICAS ISO/IEC 27001 E ISO/IEC 27002 PARA EL CUMPLIMIENTO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) EN LA INFRAESTRUCTURA DEL SISTEMA NACIONAL DE NIVELACIÓN Y ADMISIÓN (SNNA).

PROYECTO PREVIO LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

GUALOTUÑA GUATO HUGO FERNANDO

fernando.gualotuna@hotmail.com

QUILUMBAQUI MUENALA GEOVANNA MARGARITA

geova.qm@gmail.com

DIRECTOR: MSC. CARLOS MONTENEGRO

carlos.montenegro@epn.edu.ec

Quito, Abril 2016

DECLARACIÓN

Nosotros, Hugo Fernando Gualotuña Guato y Geovanna Margarita Quilumbaquí Muenala, declaramos bajo juramento que el trabajo aquí escrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultados las referencias bibliográficas que se incluye en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondiente 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.

Fernando Gualotuña

Geovanna Quilumbaquí

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el señor Hugo Fernando Gualotuña Guato y la señorita Geovanna Margarita Quilumbaquí Muenala, bajo mi supervisión.

MSc. Ing. Carlos Montenegro

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco Dios por darme salud y la fortaleza necesaria para culminar este período de estudios con éxito.

Al Ing. Xavier Salazar, Director de TIC's de la SENESCYT, por apoyo y confianza para la realización del proyecto de titulación.

Al ing. Milton Moya, Oficial de Seguridad de la SENESCYT, por ser guía y compartir su conocimiento y experiencia, que fue de mucha utilidad en el desarrollo del proyecto de titulación.

Fernando Gualotuña.

DEDICATORIA

Este trabajo lo dedico de manera especial a mis dos madres Blanca E. Guato Caisa, y María Concepción Caisa, que continuamente me dieron su bendición; y se encuentran cerca a pesar de la distancia muy cerca de mí.

A mi hijo Alexander aunque no esté conmigo, siempre lo llevo en mi corazón.

A mis hermanos Dexy, Verónica, Aldo, Nora, y Gaby.
Y finalmente a mi padre, Ángel Gualotuña; GRACIAS POR LA INSISTENCIA.

Fernando Gualotuña.

AGRADECIMIENTO

Agradezco a todas las personas que forman parte de mi vida que, con su apoyo, cariño y consejos, me fortalecen para cumplir mis metas y objetivos, de manera especial quiero agradecer:

A mi Madre, por su amor, comprensión y por ser fuente de motivación constante para alcanzar mis metas.

A mi hermana Blanca, gracias a su esfuerzo y su apoyo incondicional, tuve la oportunidad de culminar mis estudios.

A mi Padre, que sé que desde el cielo me cuida y me llena de bendiciones.

A Don Pedro de la Cruz, por confiar en mí y darme la oportunidad de conocer a personas destacables como el Ing. Xavier Salazar y el Ing. Milton Moya.

Al Ing. Xavier Salazar, Director de TIC's de la SENESCYT, por apoyo, confianza y gentil apertura para la realización del proyecto de titulación.

Al ing. Milton Moya, Oficial de Seguridad de la SENESCYT, por ser guía y compartir su conocimiento y experiencia, que fue de mucha utilidad en el desarrollo del proyecto de titulación.

Geovanna.

DEDICATORIA

Este trabajo lo dedico de manera especial a dos personas dignas de admiración y respeto, que constituyen los pilares de mi vida, mi madre Juana y a mi hermana Blanca, a quienes les debo todo.

Geovanna.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Instituciones del Estado y privadas, sus procesos de negocio se encuentra en sistemas de información, empezando desde el cobro de una factura hasta el registro para rendir un examen; simplemente con el fin de ser más productivas, ahorrar costos y poder realizar todas sus actividades en el menor tiempo posible, optimizando recursos.

Hace unos años atrás toda la información se encontraba en papel, pero hoy en día su porcentaje está reducido, debido a que ésta podía ser guardada en un lugar conocido, leerse, copiarse y destruirse a mano, pero el tiempo ha transcurrido; hoy en su mayor porcentaje se encuentra almacenada en algún medio electrónico tales como: memorias USB, discos duros, alojados en algún portal web, o servicio de almacenamiento, DVD etc. es decir; dispersa en forma de 0s y 1s, creando una gran diversidad de fuentes de información, que cada dueño es el encargado de protegerla, esencialmente la aquella de carácter privado y restringida.

1.1 INCIDENTES DE SEGURIDAD

Existe varios incidentes de seguridad a nivel mundial, lo que va del año 2015 y 2016 por solo un ejemplo se ha resumido los siguientes:

Abril 30 de 2015 Mattel casi pierde 3 millones de dólares debido a un correo enviado al departamento financiero suplantando al nuevo director ejecutivo, ordenando al banco chico el pago.

Su Bin, de 50 años, trató de acceder las redes de Boeing y contratistas para robar información militar sobre los Jets de combate F-22 y F-35 y avión de transporte C-17, de EEUU, condenado a 5 años de prisión con multa de 250.000$.

Hospital de Ottawa en Canadá fue infectado con ransomware:"*Es un tipo de malware que encripta la información de los equipos infectados y para ser accedidos los dueños debe para un rescate para obtener su datos de nuevo*", pero como solo fueron infectados 4 equipos de cerca de 10.000; debido a su política de seguridad de la empresas y la copia de seguridad de todos los sistemas y datos, pudo recuperarse del incidente.

El portal CIMD (Centre d´Identificacion des Materiels de la Defense) accedieron a información sensible, tales como datos de proveedores del ejercito e información de socios, credenciales de acceso a servidores FTP, ejecutada por el colectivo The Anonymus.

Hackers denominados DotGovs, consiguió acceder a la base de datos del departamento de justicia de EE.UU, haciendo uso de ingeniería social, filtrando datos personales de 20.000 agentes del FBI y 9000 empleados del departamento de seguridad nacional de ese país.

Fuente: Instituto Nacional de Ciberseguridad, Bitácora de ciberseguridad INCIBE, Web:https://www.incibe.es/technologyForecastingSearch/CERT/Bitacora_de_ciberseguridad/?p=1

USB KILLER, el pendrive, que al conectarse a un equipo de cómputo recibe corriente eléctrica en sus condensadores, luego la revierte liberando una descarga de 220 voltios, produciendo daño irreparable

ECUADOR, 16 de enero del 2016; sale a luz pública el caso de la SENESCYT, en el cual se registró 366 títulos Universitarios de manera fraudulenta, siendo funcionarios públicos que forman el listado de personas que pagaron a “hackers” para que registren dichos títulos; este delito es penado con 7 años de cárcel de acuerdo al Código Penal. Cuya anormalidad fue detectada en octubre del 2015. Fuente: El Comercio, Ecuador, portal web: http://www.elcomercio.com/actualidad/hackers-registraron-titulos-universitarios-falsos.html

De tal forma la SENESCYT posee información relevante sobre la Educación Superior del Ecuador en el proceso de Nivelación y Admisión, por lo que requiere ser protegida ante las amenazas.

El presente proyecto inicia con un estudio preliminar que permite conocer a la institución y la forma en la que se desempeña en materia de seguridad de la información. Para el análisis y la gestión del riesgo se utiliza la metodología MAGERIT, para ello; los activos de información se identifican, las principales vulnerabilidades y amenazas a las que están expuestos cada activo; el riesgo se valora y gestiona, tomando como referencia

la Norma Técnica ISO / IEC 27002; con el fin de reducir el riesgo a un nivel aceptable, para proporcionar a la institución seguridad y confianza para lograr que el proceso continúe y cumplir su misión.

DESCRIPCIÓN DEL PROYECTO DE TITULACIÓN

1.2 OBJETIVOS

Objetivo General:

Aplicar las Normas Técnicas ISO/IEC 27001 e ISO/IEC 27002 para cumplir con el Esquema Gubernamental de Seguridad de la Información (EGSI) emitida por la Secretaria Nacional de la Administración Pública de la Secretaria de Educación Superior, Ciencia, Tecnología e Innovación "SENESCYT".

Objetivos Específicos:

- Analizar el Acuerdo Gubernamental 166 (EGSI), para ser aplicado en la Infraestructura del SNNA.
- Realizar un análisis, identificación, evaluación y tratamiento de los riesgos que presenta la Infraestructura del SNNA

Elaborar Políticas y Procedimientos de Seguridad de la Información para el SNNA.

1.3 ALCANCE

El proyecto de titulación iniciará con el análisis EGSI emitido por la Secretaría Nacional de la Administración Pública con el fin de determinar los alineamientos aplicables a la Infraestructura del Sistema Nacional de Nivelación y Admisión de la Secretaria de Educación Superior, Ciencia, Tecnología e Innovación. Posteriormente, se identificarán los activos de información que posee la Organización, y se realizará un análisis y evaluación de los riesgos; con el propósito de establecer políticas y procedimientos sobre el manejo de la Seguridad de la Información, utilizando las Normas Técnicas ISO/IEC 27001 e ISO/IEC 27002.

1.4 JUSTIFICACIÓN DEL PROYECTO

La Secretaria de Educación Superior, Ciencia, Tecnología e Innovación "SENESCYT" posee información relevante sobre la Educación Superior del Ecuador en el área de Nivelación y Admisión.

Por este motivo es necesario analizar, identificar y evaluar los riesgos, vulnerabilidades y amenazas a la que está expuesta la información para tomar sus debidos controles de seguridad para el manejo y transmisión de la información en la Infraestructura del SNNA, basándose en las Normas Técnicas ISO/IEC 27001, 27002 con el fin de garantizar la confidencialidad, integridad y disponibilidad de la Información, para el cumplimiento del Acuerdo 166 emitido por la Secretaria Nacional de la Administración Pública.

Capítulo 1 GENERALIDADES E IDENTIFICACIÓN DE LA ORGANIZACIÓN

1.1 IDENTIFICACIÓN DE LA ORGANIZACIÓN

1.1.1 DESCRIPCIÓN DE LA ORGANIZACIÓN

1.1.1.1 SENESCYT

De acuerdo a la ley Orgánica de Educación Superior en el Artículo 182, dispone: "*a la Secretaria de Educación Superior, Ciencia, Tecnología e Innovación ejercer la rectoría de la política pública en el campo de la educación superior. Coordina el proceso de reforma de la educación superior en trabajo conjunto con el Consejo de Educación Superior (CES) y el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES); El Eco. René Ramírez Gallegos es el secretario de Educación Superior Ciencia y Tecnología desde el 10 de del 2011 a la presente fecha; y la Magister María del Pilar Troya es la Subsecretaria General de Educación Superior*".

Dirección: Whymper y Alpallana, Quito-Ecuador

Teléfono: 593-23829150

Portal Web: " *http://www.educacionsuperior.gob.ec* "

Con el fin de realizar el proyecto de titulación las Oficinas y dirección del Sistema Nacional de Nivelación y Admisión[1], es la siguiente:

Dirección: Av. La Prensa y Mariano Echeverría, Oficina 301, Quito-Ecuador

Teléfono: 023829150

Portal Web: "http://www.snna.gob.ec/ "

[1] SNNA. - Sistema Nacional de Nivelación y Admisión.

1.1.1.2 VISIÓN, MISIÓN, VALORES Y OBJETIVOS DE LA SENESCYT

Visión

"*…La Secretaría de Educación Superior, Ciencia y Tecnología es garante de la aplicación de los principios que rigen la educación superior; promotor de la investigación científica, innovación tecnológica y saberes ancestrales. Su trabajo se enfoca en mejorar las capacidades y potencialidades de la ciudadanía y se caracteriza por el empleo eficiente y eficaz de los recursos que gestiona, cuyos resultados son la semilla para el desarrollo del país*".

Misión

"*….Ejercer la rectoría de la política pública de educación superior, ciencia, tecnología y saberes ancestrales y gestionar su aplicación; con enfoque en el desarrollo estratégico del país. Coordinar las acciones entre el ejecutivo y las instituciones de educación superior en las aras del fortalecimiento académico, productivo y social. En el campo del a ciencia, tecnología y saberes ancestrales, promover la formación del talento humano avanzado y el desarrollo de la investigación, innovación y transferencia tecnológica a través de la elaboración, ejecución y evaluación de políticas, programas y proyectos*".

1.1.1.3 ORGANIGRAMA DE LA ORGANIZACIÓN

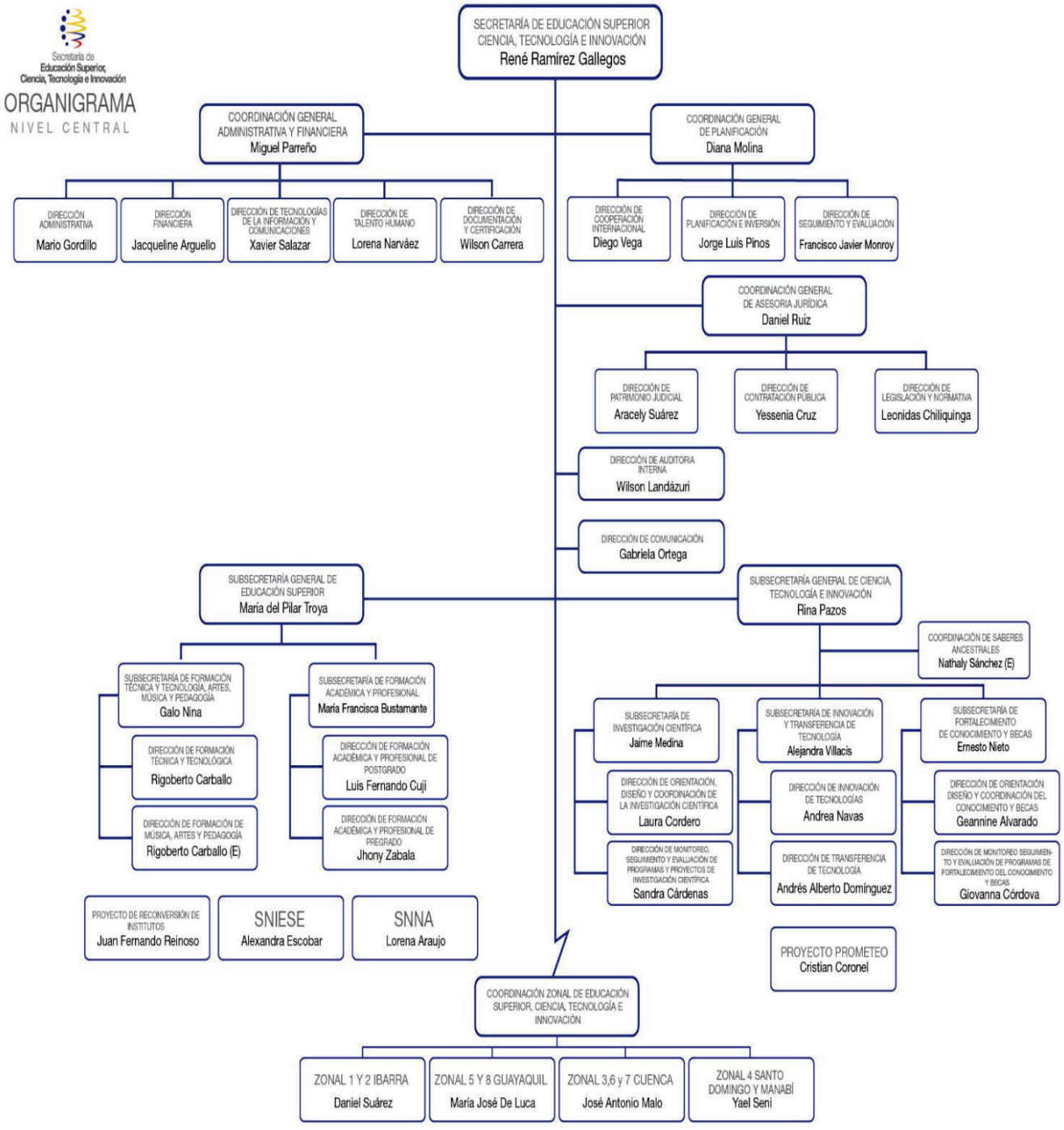


Figura N.- 1.1-1 Organigrama de la Institución.

Fuente: SENESCYT

1.1.2 PROCESOS PRINCIPALES DE LA ORGANIZACIÓN

La SENESCYT se compone de dos procesos principales y se los muestra en la **Figura N.-1.1.-2**.

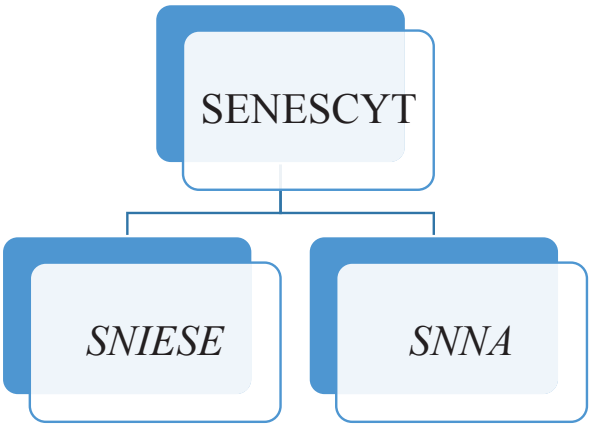


FIGURA N.- 1.1-2 PROCESOS DE LA SENESCYT.

La descripción de los procesos principales la cual posee la SENESCYT, se muestra en **Tabla 1.1.1**.

TABLA N.- 1.1-1 DESCRIPCIÓN DE LOS PROCESOS DE LA SENESCYT

Sistema Nacional de Educación Superior en el Ecuador	**Sistema Nacional de Nivelación y Admisión**
El SNIESE[2] es un sistema que brinda un servicio de información pública de educación superior para la rendición de cuentas y la toma de decisiones de la política pública cuyo objetivo es recopilar, analizar y difundir información de las IES[3] vigentes y acreditadas, para informar y orientar a los ciudadanos. **[1]**	El SNNA es un proceso que implementa y desarrolla un sistema único e integrado de inscripción, evaluación, selección y nivelación de bachilleres para el ingreso a las universidades y escuelas politécnicas públicas para la educación superior en el territorio ecuatoriano. [2] Bajo la LOES[4], en su artículo 81.

[2] SNIESE. - Sistema Nacional de Educación Superior en el Ecuador
[3] IES. - Instituciones de Educación Superior
[4] LOES. - Ley Orgánica de Educación Superior.

El presente proyecto de titulación está enfocado en el proceso del SNNA.

1.1.2.1 MISIÓN, VISIÓN Y OBJETIVOS DEL SNNA

Misión

"*…Diseñar, implementar y administrar un Sistema de Nivelación y Admisión a las Instituciones de Educación Superior públicas del Ecuador, que garantice la pertinencia de la oferta académica y la existencia de un sistema equitativo, transparente para todos los estudiantes aspirantes, basados en la aplicación de pruebas estandarizadas debidamente validadas*."

Visión

"*…Garantizar la pertinencia de la oferta académica pública y el acceso equitativo, transparente y meritocrático a todos los estudiantes aspirantes*."

Objetivo General

"*…Garantizar la igualdad de oportunidades, meritocracias, transparencia y el acceso a la Educación Superior del país*."

Objetivo Específico

"*Diseñar y financiar los sistemas de nivelación impartidos por las Instituciones de Educación Superior Públicas, que garanticen la igualdad de oportunidades y compensen las asimetrías formativas antes del ingreso a las carreras universitarias*".

1.1.3 DESCRIPCIÓN DEL PROCESO DEL SNNA

Para saber cómo funciona el proceso, es necesario identificar las actividades, personas y tecnología que se relacionan; para ello se utilizará el reglamento del SNNA [2] [3]; el mismo que se describe a continuación:

Cada ciclo lectivo, de acuerdo al calendario establecido, la SENESCYT debe solicitar a las IES públicas, cofinanciadas y autofinanciadas, la oferta de cupos de nivelación e inicio de primer semestre respectivo.

Esta información debe ser ingresada por parte de la IES al portal web del SNNA, para su posterior revisión, de acuerdo al cronograma establecido.

El SNNA proporciona los cupos emitidos por las IES en cada convocatoria al ENES[5], a los bachilleres a nivel nacional.

La convocatoria se la realiza a través de la página web del SNNA, y medio de comunicación masiva, donde los aspirantes tienen un período de inscripción, el/la aspirante debe registrarse en la plataforma la misma quedará formalizada una vez que hayan cumplido con todos requisitos que la aplicación exige.

Finalizada la inscripción, el/la aspirante deberá presentarse a rendir el ENES con los documentos habilitantes cédula y comprobante de registro, de acuerdo a la información emitida por la SNNA a través de su cuenta personal.

La evaluación y calificación es responsabilidad de la SENESCYT, quien determinará la calificación mínima para las diferentes carreras ofertadas.

La comunicación de resultados del ENES, se realizarán a través de la cuenta personal de cada aspirante.

Los/las aspirantes tienen la posibilidad de solicitar una recalificación, si no está conforme con el resultado, para ello y su respectiva rectificación se adjunta las respuestas correctas en cada cuenta.

Una vez obtenido el resultado del ENES, el aspirante puede postularse a través de la plataforma web del SNNA a los cupos ofertados por las IES, conforme al puntaje mínimo y el cupo existente por carrera.

Si el aspirante acepta el cupo de carrera, el sistema generará un comprobante; caso contrario debe esperar al proceso de re-postulación para la selección de otra carrera con un mínimo de tres postulaciones caso contrario, el/la aspirante deberá rendir nuevamente el ENES.

Finalizada la postulación y re-postulación, el aspirante debe tomar el curso de nivelación de carrera, el cuál debe ser aprobado para ingresar a primer semestre de carrera. En el caso que el/la estudiante quiera rendir el examen EXONERA y si lo aprueba los aspirantes pueden pasar directamente a primer semestre.

[5] ENES: Examen Nacional de Educación Superior

En el caso que el/la estudiante obtenga un alto puntaje y sea seleccionado en el GRUPO DE ALTO RENDIMIENTO, serán aspirantes para postularse a universidades extranjeras.

En el siguiente diagrama se puede observar el proceso del SNNA. [3]

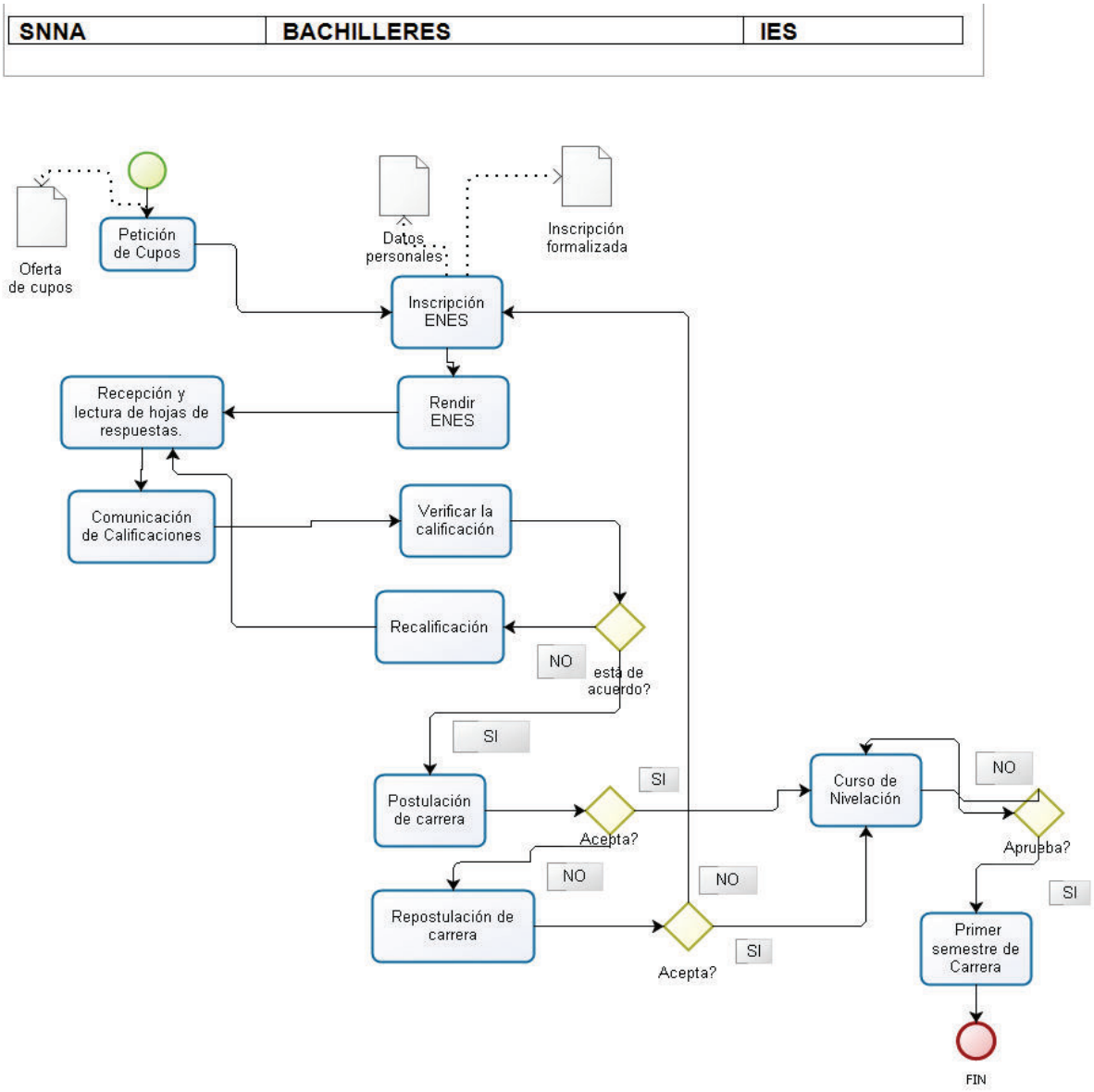


Figura N.- 1.1-3 Descripción completa del Proceso del SNNA

Fuente: Proceso SNNA-SENESCYT.

Figura N.- 1.1-4 Proceso de Lectura de Exámenes.

Fuente: SNNA

1.2 DESCRIPCIÓN DE LA NORMA TÉCNICA ISO/IEC 27000

La familia de Normas 27000 son de estándares creados por la Organización Internacional de Normalización[6], conjuntamente con la Comisión electrónica Internacional[7]; que constituyen un marco de trabajo para la gestión de la seguridad de la información, adaptable a todo tipo de institución pública o privada, grande o pequeña. [4]

La **Tabla N.-1.2.1** describe parte de la familia de las Normas Técnicas ISO/IEC 27000, que serán utilizadas en el presente proyecto de titulación.

TABLA N.- 1.2-1 FAMILIA DE NORMAS TÉCNICAS

FUENTE: ISO/IEC 27000 [5].

Norma ISO/IEC 27000	Comprende los conceptos básicos, el vocabulario del estándar para el sistema de gestión de seguridad de la información
Norma ISO/IEC 27001	Comprende los requisitos del sistema de gestión de seguridad de la información. Adopta un enfoque de gestión de riesgos y promueve la mejora continua.
Norma ISO/IEC 27002 o Anexo A de la Norma ISO/IEC 27002	Es una guía de buenas prácticas que describe los objetivos de control y controles sobre la seguridad de la información agrupados en 14 dominios
Norma ISO/IEC 27003	Es una guía para el diseño e implementación de un sistema de gestión de la seguridad de la información. Se utilizó el Anexo D: para estructurar una política de seguridad.

[6] ISO. – Organización Internacional de Normalización.
[7] IEC. - Comisión Electrónica Internacional.

Norma ISO/IEC 27005	Es una norma que proporciona recomendaciones y directrices para la gestión de riesgos de seguridad de la información. Se utilizó el Anexo B: que es la valoración de activos y evaluación del impacto. Anexo C: Ejemplos de amenazas típicas, Anexo D: vulnerabilidades y métodos de evaluación de las vulnerabilidades.

1.2.1 JUSTIFICACIÓN Y SELECCIÓN DEL ESTÁNDAR ISO/IEC 27000:2013

El SNNA constituye un macro proceso administrado por la SENESCYT, el mismo que está regulado por: "*La **Secretaría Nacional de Administración Pública**[8]; esta institución está encargada de establecer políticas, metodologías de gestión e innovación institucional y herramientas necesarias para mejorar la eficiencia, calidad y transparencia de todas las instituciones que se encuentran administradas bajo la función ejecutiva*". [6, p. 2]

El SNAP mediante el Acuerdo 166 o EGSI[9], dispone*: "el uso obligatorio de las Normas Técnicas ISO/IEC 27000 para la Gestión de la Seguridad de la información, con el fin de adoptar políticas, normas, estrategias, procedimientos tecnológicos para mantener la seguridad en la información que se genera y se mantiene custodiada en diferentes medios y formatos; este acuerdo fue realizado en base la norma NTE INEN ISO/IEC 27002: 2005*". [6, p. 3]

Además, en su **artículo 7**, determina que: "… *todas las instituciones realizarán una evaluación de riesgos y diseñaran un plan basado en la norma ISO/IEC 27005, tomando como referencia una metodología para la* Evaluación y Gestión de riesgos". [6, p. 3]

[8] SNAP. - Secretaría Nacional de Administración Pública
[9] EGSI: Esquema Gubernamental de la Seguridad de la Información

1.2.2 ANÁLISIS

El EGSI es una resolución del Gobierno Ecuatoriano, para saber cuál es el nivel de madurez de seguridad; para garantizar la confidencialidad, integridad y disponibilidad de la información en cada institución pública.

El EGSI establece cláusulas prioritarias y no prioritarias para la "*Gestión de la Seguridad de la Información*". El objetivo es determinar o diagnosticar cuál es la información más importante que existe dentro de una institución, y por otro lado ver como dicha información puede ser protegida; mediante el proceso de "Gestión del riesgo".

De acuerdo a la **Cláusula 3.2.1 de la Norma Técnica ISO 27000**, el SGSI [10], proporciona un enfoque sistemático para :"*Establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una Institución con el fin de alcanzar los objetivos de negocio*".

1.2.3 DESCRIPCIÓN DE LA NORMA ISO/IEC 27001:2013

De acuerdo a lo mencionado en 1.2.2 para el desarrollo del proyecto se requiere del uso de las siguientes normas:

La norma ISO/IEC 27001:2013 define los requerimientos y directrices para un Sistema de Gestión de **seguridad de la información**[11]; reúne todos los componentes del sistema de gestión, los documentos mínimos y los registros que permitirán evidenciar el buen funcionamiento; así conjuntamente se requiere el uso del anexo A (ISO/IEC 27002) para seleccionar controles y medidas de seguridad que serán adaptados en el proceso de implementación en función de las necesidades de la Institución.

Para la etapa de gestión de riesgos la ISO/IEC 27001 no cuenta con una metodología, por lo tanto; en base a un análisis de metodologías de gestión de

[10] SGSI**:** Sistema de Gestión de la Seguridad de la Información.
[11] Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la Información (de Acuerdo a la Norma Técnica ISO 27000, Cláusula 2.19)

riesgos se elegirá la más adecuado para el desarrollo del proyecto tomando como guía la Norma Técnica ISO/IEC 27005.

1.2.3.1 ENFOQUE A PROCESOS DE LA NORMA ISO/IEC 27001.

La Norma Internacional adopta el modelo de procesos **"Planificar-Hacer-Verificar-Actuar**" por sus siglas PHVA o "**Ciclo de Deming**" popularizado por William Edwards Deming (1900-1993), cuyo autor fue Walter Andrew Shewhart (1981-1967), queda definido por un proceso de 4 etapas. [7], [8, p. 43]. El ciclo PHVA es un enfoque de mejora continua implica planificar acciones, implementar lo planificado, revisar, corregir, y mejorar. A continuación se explica el modelo PHVA

PLANIFICAR es el proceso, dónde se establece la política de seguridad, los objetivos, los procesos relacionados con la gestión de riesgos y la mejora de la Seguridad de la Información para obtener un alineamiento con los objetivos de la institución, es decir; se realiza el diseño del SGSI, el alcance, la metodología para la gestión y evaluación de riesgos; y la ejecución del proyecto.

HACER es subproceso para implementar y operar el SGSI, basado en la política que se crea, y se implementada de acuerdo a la metodología de gestión y plan de tratamiento de riesgos; aplicando los dominios del Anexo A de la Norma técnica ISO/IEC 27001:2013; con el fin de realizar la sensibilización y capacitación sobre la gestión y el uso de los recursos necesarios para mantener el sistema de gestión.

VERIFICAR y Evaluar que el proceso para determinar si va por un buen camino estableciendo indicadores de medición para alcanzar lo declarado en el alcance; con el fin de informar los resultados a la Alta Dirección para su revisión posterior y mejora. Se debe monitorear y revisar los resultados para determinar si, éstos están alineados con los objetivos del negocio de la institución.

Finalmente se Mantiene y se busca mejorar el Sistema de Gestión a lo que se llama **ACTUAR**, sólo si existiera situaciones que no estén alineadas con los objetivos de del negocio con el fin de aplicar acciones correctivas y confirmar su efectividad; como por ejemplo si los procesos están siendo mal ejecutados y/o controles implementados son ineficaces o insuficientes. [9, p. 19]

En la **Figura N.-1.2.1**, se muestra el ciclo de Deming y sus tareas internas.

Figura N.- 1.2-1 Ciclo de Deming para el SGSI.

Fuente: Curso ISO 27001 Lead Implementer Official Course [8]

1.2.3.2 ESTRUCTURA DE LA NORMA ISO 27001:2013

La norma Técnica ISO/IEC 27001 versión 2013 se ajustó en todo su contexto al ANEXO SL “Este anexo describe como debe estructurarse una norma de gestión ISO”. [10]

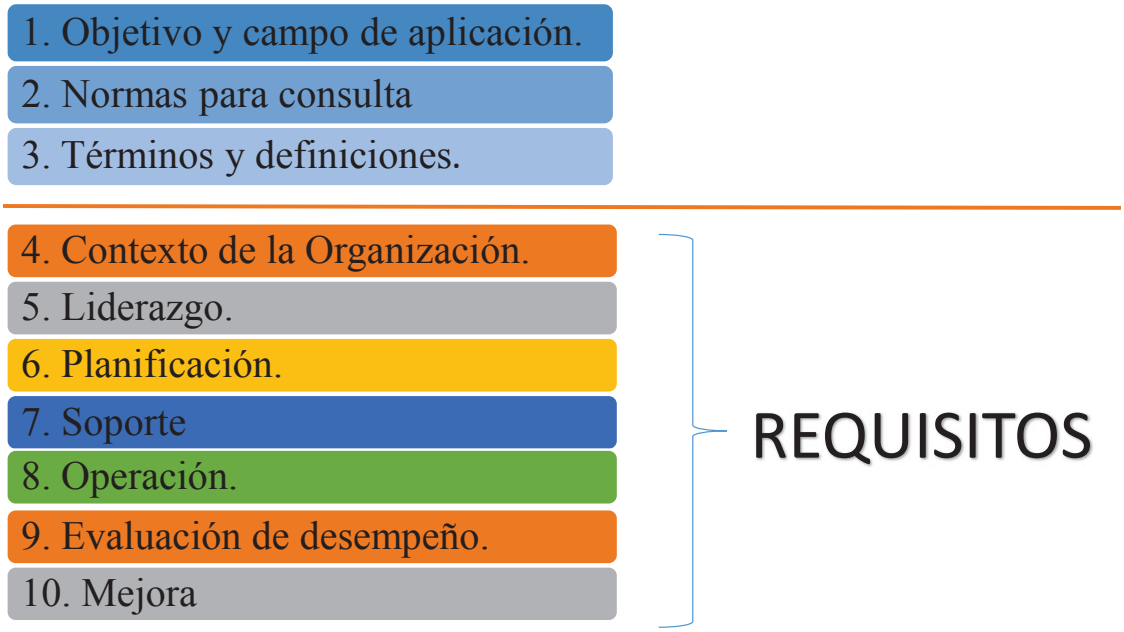


Figura N.- 1.2-2 Estructura/Pilares fundamentales de la Norma ISO/IEC 27001:2013

De acuerdo a la Norma los pilares fundamentales para establecer un modelo de mejora continua son:

4. **Contexto de la Organización**.

4.1 Conocimiento de la Organización y su contexto. - Se debe conocer el modelo de Negocio y el entorno el cuál se encuentra, este entorno puede ser **interno** (gobernanza, estructura organizativa, funciones y responsabilidades, políticas, objetivos y estrategias, si, normas, directrices) o **externo** (social y cultural, político, jurídico, reglamentario, tecnológico, entorno competitivo)

4.2 Entender las necesidades de las partes interesadas. - Es decir entender e identificar los clientes, socios, proveedores y a sus organismos de control con el objetivo de cumplir una serie de requisitos legales regulatorios, contractuales.

4.3 Determinar el Alcance. – Se define los límites del SGSI estableciendo que quiere proteger y por donde comenzar.

5. **Liderazgo**.

5.1 Liderazgo y compromiso. - La alta dirección de la SENESCYT debe demostrar: liderazgo, compromiso y garantizar los recursos necesarios para su implementación.

5.2 Roles responsabilidades y autoridades organizacionales.

6. **Planificación**.

6.1.2 Evaluación de los riesgos de Seguridad. - Se enfoca en: "*la definición de los objetivos de seguridad, define y aplica la metodología de gestión de riesgos, en la cual se elimina el término propietario del activo y adopta el término propietario de riesgo*".

7. **Soporte**.

7.1 Recursos. - La SENESCYT debe: "*determinar y proporcionar todos los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI*".

7.3 Concientización. - La institución deben tener conciencia y estar inmersos dentro del proceso de implementación, para que no tenga problemas o rechacen a los cambios.

7.1 Comunicación. - La Institución debe: saber **qué, quién y cuándo** se debe comunicar sobre el SGSI, para que el proceso sea efectivo.

8. Operación. – "*Todos los requisitos para medir el funcionamiento del SGSI, cumplir con todas las expectativas y realizar una retroalimentación. Se plantea y controla las operaciones y los requisitos de seguridad mediante la evaluación de riesgos".*

8.2. **Evaluación de los riesgos**. -se los deber realizar en intervalos planificados y controlados o cuando se den cambios notorios o hayan sufrido alguna alteración.

8.3. Tratamiento de los riesgos. - La institución debe implementar el plan de tratamiento de riesgos de seguridad y toda información generada la debe conservar con su respectivo versionamiento.

9. Evaluación de desempeño. Evalúa la seguridad de la información y la eficacia, mediante auditorías internas y son revidadas por la dirección, además todos los resultados obtenidos deben ser conservados y documentados.

10. Mejora. - Cuando se de una no conformidad, la SENESCYT está en la obligación de reaccionar ante ella y emprender accionas para controlar o corregir, con el objetivo de que no vuelvan a producirse haciendo cambios en el SGSI si fuese necesario.

1.2.3.3 GRÁFICA DE MODELO DE MEJORA CONTINUA ISO/IEC 27001:2013

La SENESCYT busca la certificación ISO 27001 debe cumplir con todos los términos definidos en las clausulas 4 a 10 de la Norma Técnica.

Figura N.- 1.2-3 Modelo de Mejora contínua de la Norma ISO/IEC 27001:2013

Fuente: Anexo LX páginas 130-137)

1.2.3.4 ANEXO A DE LA NORMA TÉCNICA ISO 27001

El Anexo A de la Norma ISO/IEC 27001, es una lista de controles y objetivos de control de seguridad; a continuación se explica en resumen cada una de ellas.

- **A5 Política de seguridad de la Información.-** especifica controles de cómo la política de seguridad está escrita, revisa o aprobada por la Alta Dirección.
- **A6 Organización de la seguridad de la información**.- determina controles sobre cómo se asignan las responsabilidades, y sobre dispositivos móviles y teletrabajo.
- **A7 Seguridad de los Recursos Humanos**.-determina controles previos, durante y después del empleo.

- **A8 Gestión de los activos**.-contiene controles relacionados con el inventario de activos, uso aceptable, clasificación de la información y manejo de medios.
- **A9 Control de Acceso**.- contiene controles para la política de control de acceso, gestión de usuarios hacia los sistemas y las responsabilidades del usuario.
- **A10 Criptografía**.- contiene controles sobre el cifrado y gestión de claves
- **A11 Seguridad física y de los medio ambiente.-específica controles** para la protección de seguridad física de instalaciones y medio ambiente, equipos, su eliminación o reutilización.
- **A12 Seguridad en las Operaciones**.- contiene controles para la gestión de TI (gestión del cambio, capacidad, seguridad, supervisión e instalación de software etc.)
- **A13 Seguridad en las Comunicaciones**.- contiene controles sobre la seguridad y segregación de las redes, servicios; y la transferencia de información por los diferentes medios.
- **A14 Seguridad en la Adquisición, desarrollo y mantenimiento de los sistemas de información**.- contiene controles que definen requisitos para la seguridad en el proceso de desarrollo, adquisición o mantenimiento de sistemas de TI.
- **A15 Relaciones con los proveedores**.-contiene controles como supervisar y gestionar la seguridad con los proveedores y prestadores de servicios.
- **A16 Gestión de incidentes de la seguridad de la información**.- contiene controles para informar, definir responsabilidades, encontrar respuestas y recogida de pruebas ante incidentes de seguridad.
- **A17 Aspectos de la Seguridad de la Información en la continuidad del negocio**.- contiene controles para planificar la continuidad del negocio mediante procedimientos de verificación, revisión o redundancias.
- **A18 Cumplimiento**.- contiene controles para la identificación de leyes, reglamentos que deben ser aplicables para la protección, y revisiones de la seguridad de la información.

En la **Figura. - 1.2-4**, son las cláusulas de la 5 a la 18 que deben ser utilizados en la implementación de controles de seguridad.

ISO 27002:2013 DOMINIOS		TOTAL DE CONTROLES
A5	Política de Seguridad de la información	**2**
A6	Organización de la Seguridad de la Información	**7**
A7	Seguridad de los RRHH	**6**
A8	Gestión de Activos.	**10**
A9	Control de Accesos.	**14**
A10	Criptografía.	**2**
A11	Seguridad física y ambiental.	**15**
A12	Seguridad en las operaciones.	**14**
A13	Seguridad en las comunicaciones.	**7**
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	**13**
A15	Relaciones con proveedores.	**5**
A16	Gestión de incidentes de seguridad de la información.	**7**
A17	Aspectos de seguridad de la información en continuidad del negocio.	**4**
A18	Cumplimiento.	**8**
TOTAL		**114**

Figura N.- 1.2-4 Anexo A de Norma Técnica ISO/IEC 27001

1.2.3.5 ETAPAS PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001

i. Identificar los Objetivos del Negocio.
ii. Obtener el patrocinio de la Alta Dirección.
iii. Establecer el Alcance del SGSI.
iv. Análisis de Brechas (Gap Análisis).
v. Asignar recursos y capacitar al equipo.

vi. Análisis y Evaluación de Riesgos de Activos de Información.
    a. Definir el método de análisis y evaluación.
    b. Definir los activos.
    c. Identificar las amenazas.
    d. Determinar la Probabilidad de ocurrencia de las amenazas.
    e. Determinar el impacto de las amenazas, con el objetivo de priorizar.
    f. Recomendar controles que disminuyan la probabilidad de los riesgos.
    g. Documentar el proceso.
vii. Gestionar el riesgo y elaborar un plan de tratamiento.
viii. Definir la forma de medir la efectividad de sus controles del SGSI haciendo uso de la Norma ISO/IEC 27004.
ix. Implementar controles y procedimientos de acuerdo a la matriz de riesgos, siendo estos priorizados.
x. Desarrollar e implementar programas de capacitación y concienciación a todos los funcionarios del SNNA.
xi. Monitorizar y medir la implementación.
xii. Prepararse para la Auditoria de Certificación.
xiii. Realizar auditorías internas periódicas.
xiv. La dirección debe realizar revisiones periódicas.
xv. Implementar medidas correctivas.

1.2.3.6 BENEFICIOS DE IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001

Proporciona un marco de referencia para la gestión de seguridad de la Información basada en riesgos, en el cual vela por el cumplimiento de los requisitos legales y reglamentarios, y el orden jerárquico es: ***Leyes Internacionales. Constitución, leyes nacionales, leyes seccionales, leyes locales y finalmente Normativa interna de la Organización.***

Figura N.- 1.2-5 Beneficios al implementar el SGSI

Fuente: Autores

A continuación, se menciona una lista de beneficios al implementar el SGSI.

i. Su gestión se enfoca en las personas, procesos y tecnología.
ii. Rendición de cuentas sobre las operaciones y prácticas dentro de la organización.
iii. Protección continúa sobre los activos de información.
iv. Adoptar la Gestión de Continuidad del Negocio para hacer frente ante cualquier eventualidad o desastre.
v. Mejora la confianza de los clientes,
vi. Mejora la imagen y reputación de la organización.
vii. Se reduce los costos de debido al adecuado tratamiento de incidentes de seguridad, reduciendo la probabilidad de que algo parecido sucediera en el futuro por la implementación de controles.
viii. Produce un cambio cultural organizacional debido a que se implementa y aplica controles, en las cuales por medio de la Unidad de Comunicación se realizan campañas de difusión y capacitación permanentes en toda la Organización, con el objetivo de tener una visión amplia de vulnerabilidades,

amenazas, riesgos y sobre todo las consecuencias que estos producen en la imagen y reputación Institucional.

1.3 METODOLOGÍAS DE GESTIÓN DE RIESGOS

En la actualidad existe una variedad de metodologías de gestión de riesgos que debe ser elegida según las necesidades de seguridad de la información que requiera la organización.
En esta sección se realizará una descripción de algunas metodologías de gestión de riesgos definiendo de forma breve cada una de ellas.

1.3.1 OCTAVE METODOLOGÍA PARA LA GESTIÓN Y EVALUACIÓN DE RIESGOS.

OCTAVE es una Metodología de identificación y evaluación de riesgos de seguridad de la información, desarrollado por el CERT/CC (Centro de investigación en seguridad en Internet del Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon), tiene por objetivo facilitar la evaluación de riesgo de una organización [11, p. 1].

Octave ayuda a las organizaciones a:

- Desarrollar criterios de evaluación de riesgo cualitativas.
- Identificar activos importantes de la organización.
- Identificar vulnerabilidades y amenazas.
- Determinar y evaluar las consecuencias si las amenazas se materializan.

1.3.1.1 DESCRIPCIÓN DE LA METODOLOGÍA

Octave está desarrollado en fases
Fase 1: El equipo analista identifica los activos importantes relacionados con la información y las estrategias actuales de los activos, se define los activos que son críticos de la organización, se define los requisitos de seguridad e identifican las amenazas.

Fase 2: El equipo analista realiza una evaluación de la infraestructura para completar el análisis de amenazas y define opciones de mitigación.

Fase 3: El equipo analista realiza actividades de identificación de riesgo y desarrolla un Plan.

Este método fue diseñado para adaptarse a cualquier tipo de organización, por lo que se muestra en la **Figura 1.3-1** las fases de esta metodología.

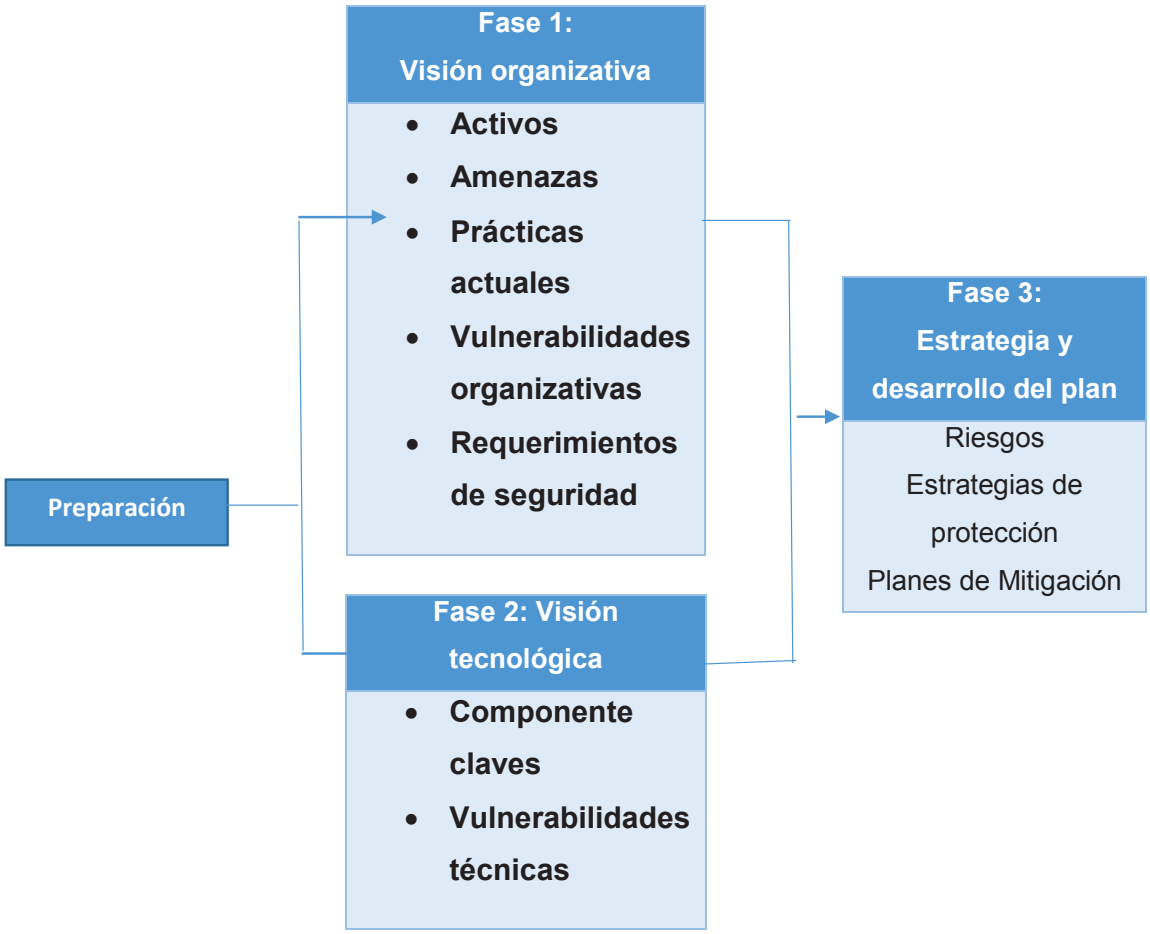


Figura N.- 1.3-1 Fases del Metodología

Fuente: Richard, A; James, F; Lisa, R; William, R. [12, p. 3]

1.3.1.2 OCTAVE-S

La creación del OCTAVE-S fue apoyado por el programa de inserción, demostración y evaluación de la tecnología del SEI, con el fin de llevar un enfoque a las pequeñas organizaciones que comprende entre 100 personas o menos.

OCTAVE-S es empleada por un equipo de analistas que tienen un amplio conocimiento de la organización, con esto ya no se requiere la recopilación de la información, porque el equipo es capaz de definir los activos, los requisitos de seguridad, amenazas y prácticas de seguridad de la organización, es decir; son miembros de la Unidad de Tecnologías de Información. OCTAVE-S está compuesto por conceptos de seguridad integradas a hojas de trabajo que guía al equipo analista. Además, incluye un examen limitado de riesgos de infraestructura a fin de eliminar la barrera para la adopción. [12, p. 3]

1.3.1.3 FASES DE LA METODOLOGÍA ALEGRO-S

La metodología está compuesta por 4 fases distribuidas en 8 pasos como se muestra en la imagen 1.3-2*:*

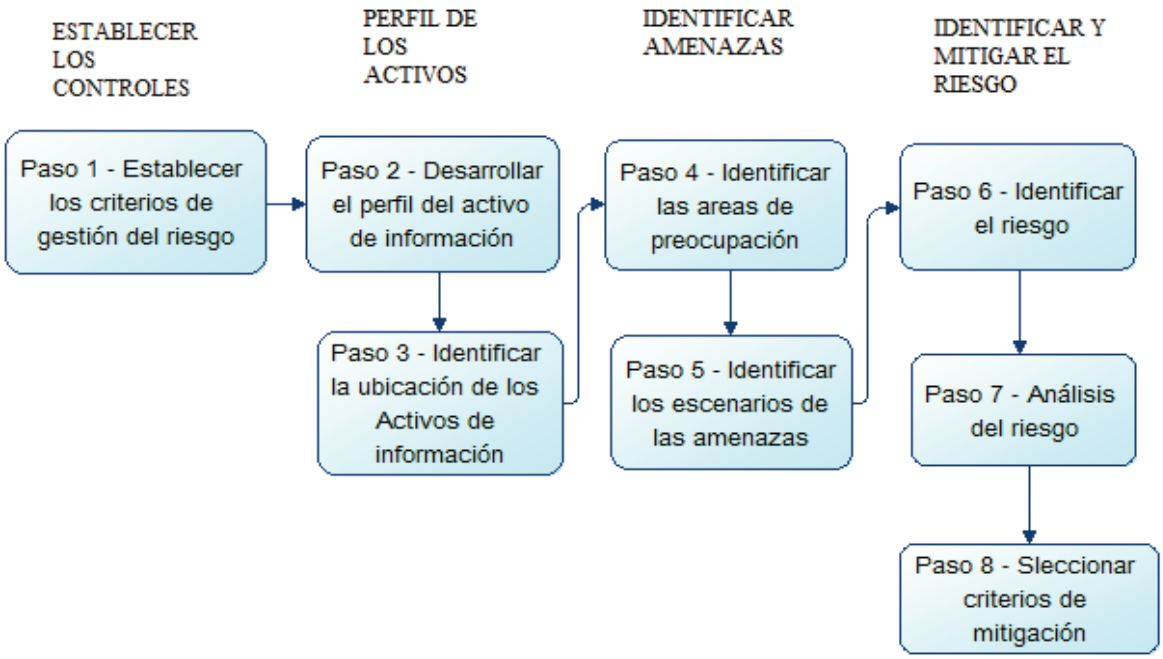


Figura N.- 1.3-2 Fases del Método OCTAVE Allegro

Fuente: Richard, A; James, F; Lisa, R; William*, R* [12]

En general, OCTAVE inicia su evaluación a partir de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para la empresa. Para su implementación es necesario un equipo mixto, compuesto por personas del área de negocios y de TI, con esto se

obtiene dos puntos de vista importantes para general una visión global de los riesgos de seguridad.

1.3.1.4 BENEFICIOS

- Identifica los riesgos de la seguridad de la información que pueden impedir la consecución de la misión de la organización.
- Enfoque de enseñanza que ayuda a evaluar los riesgos de la seguridad de la información.
- Crea una estrategia de protección con el objetivo de reducir los riesgos de seguridad de la información prioritaria.
- Ayuda a la organización a cumplir regulaciones de seguridad de la información. [12]

1.3.2 NIST 800-30 GUÍA DE GESTIÓN DE RIESGOS PARA LOS SISTEMAS DE TECNOLOGÍA DE INFORMACIÓN.

Es una guía desarrollada por Instituto Nacional de Estándares y Tecnología (**NIST**), denominada: “Guía de gestión de riesgos para los Sistemas de Tecnologías de Información – son recomendaciones del Instituto Nacional de Estándares y Tecnología”. Esta metodología ofrece una guía de para la gestión de riesgo basada en la evaluación, gestión, control y mitigación.

1.3.2.1 GESTIÓN Y EVALUACIÒN DEL RIESGO

Es una guía de gestión de riesgos, que encaja con las fases del ciclo de vida del software y las funciones de las personas que apoyan y utilizan el proceso.

La gestión de riesgos abarca tres procesos: Evaluación de riesgos, Mitigación de riesgos Evaluación y Valoración. Describe una metodología de evaluación de riesgos y los pasos básicos que conducen a una evaluación de riesgos de sistemas de TI. Se describen los 9 pasos básicos para la evaluación de riesgo como se muestra en la **Figura N.-1.3-3**:

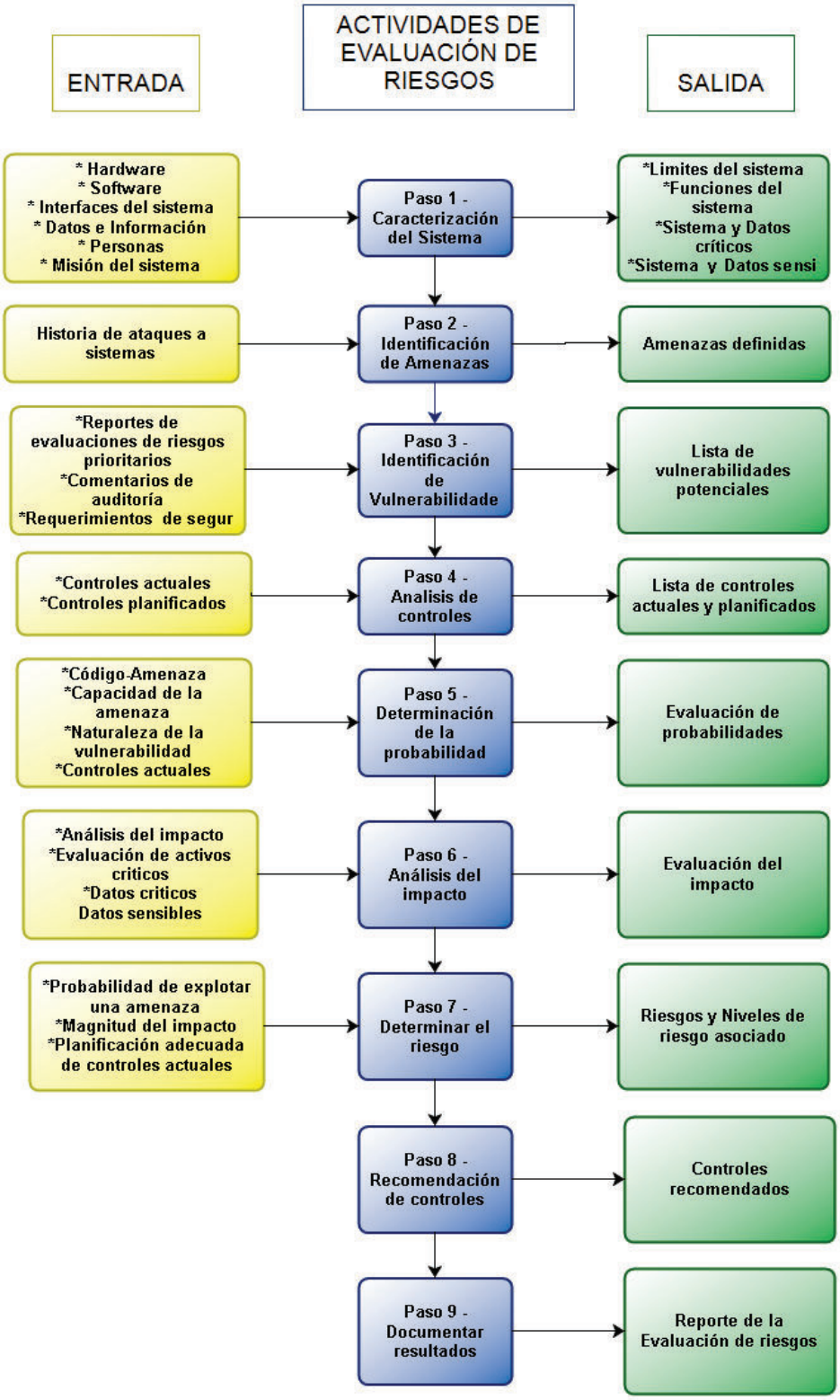


Figura N.- 1.3-3 Evaluación de riesgo según NIST 800-30

Fuente: G. Stoneburner, A. Goguen y A. Feringa, [13, p. 9]

Descripción de las Actividades de Acuerdo a la Figura N.-1.3-3

1. Caracterización del sistema, donde se identifica el alcance que tendrá la evaluación de riesgos, así como los recursos informáticos que constituyen el sistema.
2. Identificación de amenaza, se identifican y clasifican los tipos de amenazas con su probabilidad de ocurrencia.
3. Identificación de vulnerabilidades, se elabora una lista de vulnerabilidades del sistema a los cuales están expuestos los activos de información.
4. Análisis de controles, los cuales pueden ser que estén implementados o estén planteados para reducir al mínimo las amenazas del sistema.
5. Determinación de probabilidades, se determina la probabilidad de que una vulnerabilidad pueda ser ejecutada en un ambiente de amenaza relacionado.
6. Análisis de impacto, se determina el impacto desfavorable que tendría la ejecución de una amenaza sobre una vulnerabilidad.
7. Determinación de riesgo, se evalúa el nivel de riesgo de una amenaza o vulnerabilidad a través de la matriz de riesgos.
8. Recomendación de controles, de acuerdo al análisis se establece los controles adecuados para mitigar los riesgos.
9. Documentación de resultados, una vez terminada la evaluación de riesgos se proceda a documentar.

1.3.2.2 MITIGACIÓN DE RIESGO

Describe el proceso de mitigación de riesgo, incluye opciones y estrategias, enfoques de aplicación de controles, categorías de controles, análisis costo-beneficio y el riesgo residual.

Para mitigar el riesgo esta metodología se enfoca en 7 pasos los cuales son:

Paso 1.- Prioriza acciones basadas en niveles en el reporte de evaluación.

Paso 2.- Evalúa nuevamente los controles de acuerdo a la evaluación del riesgo.

Paso 3.- Realiza un análisis costo-beneficio de controles implementados y no implementados.

Paso 4.- Se selecciona controles basados en el análisis costo-beneficio, estos controles pueden ser técnicos, operacionales, o elementos para la gestión del control de TI.

Paso 5.- Asigna responsabilidades a personal interno o externos quienes tienes las destrezas suficientes para implementar los controles seleccionados.

Paso 6.- Se desarrolla un Plan de salvaguardas tomando como referencia una re-evaluación del riesgo en el que se empieza por el primer paso de acuerdo a la figura

Paso 7.- Implementar los controles seleccionados, los mismos que puedes reducir el riesgo mas no ser eliminados. [13, pp. 29-31]

Para el uso de esta metodología se requiere la completa participación del grupo de TI, conjuntamente con el equipo que tiene experiencia para aplicar esta metodología de evaluación del riesgo, con el fin de hacer un análisis costo-efectivo para la implementación de controles.

1.3.3 MAGERIT METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS

Magerit es una metodología de análisis y gestión de riesgos de carácter público elaborado por el Consejo Superior de Administración Electrónica de España, como respuesta a la creciente dependencia de las tecnologías de información para el cumplimiento de su misión.

Esta metodología pública, es decir no requiere de una previa autorización para hacer utilizadas; está directamente relacionada con la información digital, y los sistemas o aplicaciones que las trata, permite saber cuan valiosos son, y ayuda como protegerlos de riesgo. [14, p. 7]

Magerit implemente el proceso de gestión de Riesgos; para que las instituciones de gobierno tomen decisiones basados en la evaluación del riesgo derivado por el uso de las tecnologías de información.

La primera publicación de Magerit fue en 1997, La segunda versión fue publicada en 2005, se planteó como versión constructiva, adaptándola al tiempo presente e

incorporando la experiencia. La tercera versión busca una nueva adaptación, no solo en la experiencia práctica sino también la evolución de las normas internacionales ISO que es un referente obligatorio. Apéndice 6 [14, p. 126].

1.3.3.1 OBJETIVOS

La metodología tiene objetivos directos e indirectos [14, p. 8].

Directos

- Concienciar a los responsables la existencia de riesgos y de la necesidad de ser gestionados.
- Ofrecer un método sistemático para analizar los riesgos por el uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento de forma oportuna los riesgos y tenerlos en un ambiente controlado.

Indirectos

- Preparar a la institución para ser evaluada, auditada, o esta espera ser certificada o acreditada.

1.3.3.2 PASOS DE LA METODOLOGÍA

Paso 1: Identificación y valoración de Activos de información, y determinación del riesgo.

El paso inicial está compuesto de las siguientes actividades:

- Identificar y definir los activos más relevantes
- Clasificar por el tipo de activo.
- Identificar relaciones existentes con otros activos.
- Determinar dimensiones de seguridad por activo.
- Calcular el valor del activo desde la perspectiva de la necesidad de proteger.

Dimensiones para valor son en base a su confidencialidad, integridad, y su disponibilidad.

Ejemplos de activos: Datos, servicios, aplicaciones, equipos informáticos, redes de comunicaciones, personas, e instalaciones.

Paso 2: Identificación de Amenazas y vulnerabilidades

En este paso está compuesto por las siguientes actividades:

- Determinar las amenazas a las que están expuestos los activos, que pueden afectar el cumplimiento de la misión de la organización.
- Determinar el impacto potencial derivado de la materialización de una amenaza a los activos.
- Determinar el riesgo potencial probable sobre los activos.
- Estimar el impacto.
- Estimar el riesgo.

> *"El objetivo de esta tarea es determinar la estimación de lo puede ocurrir y de la probabilidad que esto ocurra"* [14, p. 44]

Paso 3: Salvaguardas o Contramedidas.

Esta actividad busca definir qué salvaguardas ayudarán a tratar el riesgo de manera efectiva.

Para seleccionar la salvaguarda se debe tomar en cuenta:

- Tipo de activo
- Amenaza a la que está expuesta
- Dimensión de valor que es motivo de preocupación, centrarse en el más valioso
- Nivel de riesgo.

Para excluir una salvaguarda se debe analizar:

a) Si aplica. - porque técnicamente no es necesaria para el tipo de activo a proteger, frente a la amenaza en consideración
b) No se justifica. - cuando al aplicar la salvaguarda, es desproporcionada ante la amenaza, por lo tanto, se debe tener una declaración de aplicabilidad.

Paso 4: Impacto residual

El impacto residual es el resultado de un conjunto de salvaguardas desplegadas al impacto potencial.

Para su valoración se repiten los cálculos de impacto con salvaguardas hasta que el nivel de impacto sea insignificante.

Si el valor residual es igual al valor potencial, las salvaguardas no que se implementaron no sirven, teniendo en cuenta que este número representa lo que se debería hacer y no se ha hecho.

Paso 5: Riesgo residual

El riesgo residual es el resultado de un conjunto de salvaguardas desplegadas al riesgo potencial. Para su valoración se repiten los cálculos de riesgo con salvaguardas hasta que el nivel de riesgo sea aceptable para la organización. Magerit para realizar el análisis y evaluación de riesgo, cuenta con los pasos que se muestra en la **Figura N.-1.3-4,**

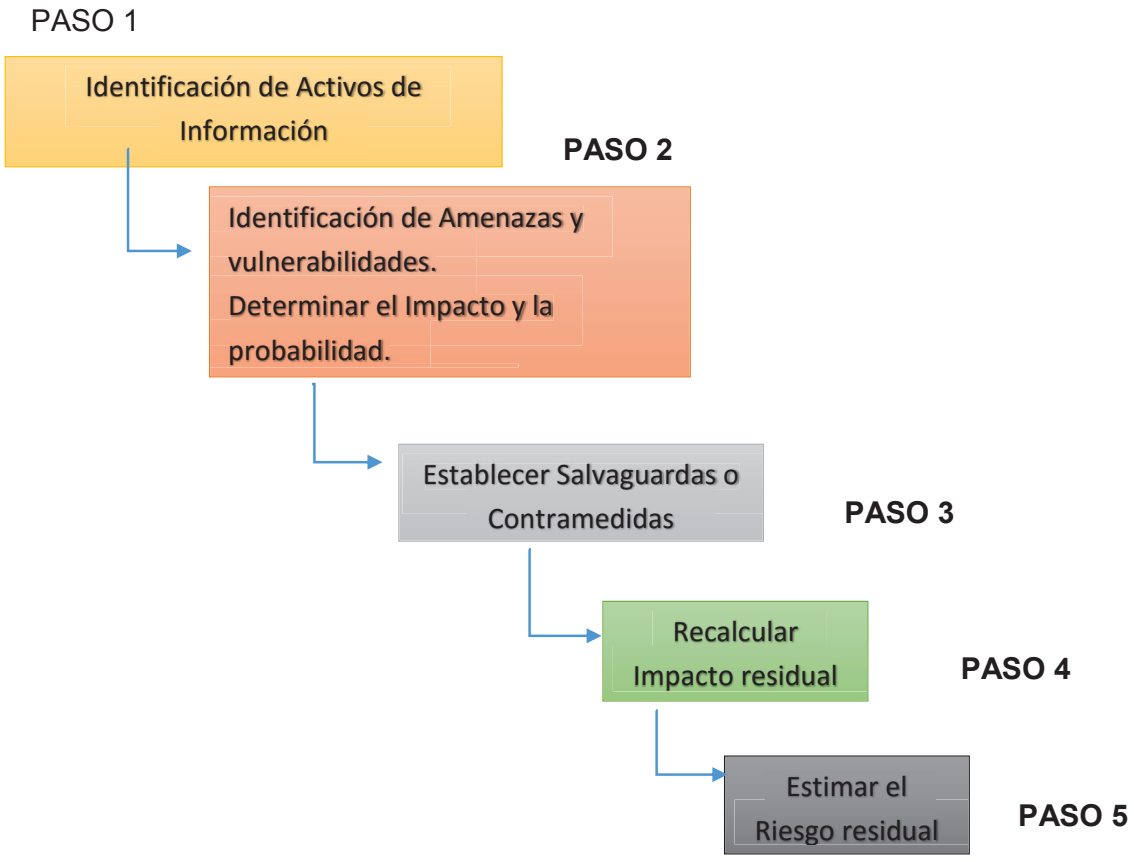


Figura N.- 1.3-4 Descripción de los pasos de la Metodología

Fuente: Magerit Libro I. [14, pp. 2-35].

1.4 COMPARACIÓN DE LAS METODOLOGÍAS PARA LA GESTIÒN DE RIESGOS.

TABLA N.- 1.4-1 COMPARACIÓN DE METODOLOGÍAS

FUENTE: ENISA [15]

CRITERIO	DESCRIPCIÓN	MAGERIT	OCTAVE ALEGRO	NIST 800-30
Fases de Apoyo para la Evaluación del riesgo	Para la fase de evaluación del Riesgo se debe considerar: -Valoración de Activos en términos de confidencialidad, integridad y disponibilidad. -Amenazas a los activos. -Vulnerabilidades -Probabilidad de ocurrencia de estas amenazas	Identificación del riesgo: Activos: identificación, clasificación, relaciones entre activos, y valoración. Amenazas: identificar la relación existente con los activos y vulnerabilidades. Controles: selección y evaluación. Análisis del riesgo: impacto y riesgo potencial. Evaluación del riesgo: de los riesgos técnicos en riesgos del negocio.	Identificación del riesgo: El equipo analista, define criterios de evaluación de riesgos. Análisis del riesgo: De acuerdo al criterio del equipo analista. Evaluación del riesgo: De acuerdo al criterio del equipo analista.	Identificación del riesgo: Activos: los clasifica y proporciona ejemplos, para definir los activos de la organización. Análisis del riesgo: proporciona un check-list y ejemplos. Evaluación del riesgo: proporciona una plantilla base.
Fases de Apoyo para la Gestión del riesgo	Elección de criterios objetivos para determinar un nivel de riesgo aceptable.	Evaluación del riesgo. Tratamiento del riesgo: se apoya en los escenarios: fases, proyectos de	Evaluación del riesgo Tratamiento del riesgo: De acuerdo al	Evaluación del riesgo Tratamiento del riesgo: detallado con diagramas de flujo y aspectos matemáticos.

		seguridad, objetivos a largo plazo. Aceptación del riesgo: indicadores de seguridad. Comunicación del riesgo: reportes de resultados y conclusiones del análisis y gestión del riesgo: modelos de valoración, mapa de riesgos, evaluación de salvaguardas, estado del riesgo, y plan de seguridad.	criterio del equipo analista. Aceptación del riesgo: De acuerdo al criterio del equipo analista. Comunicación del riesgo: Documentos de apoyo.	Aceptación del riesgo: incluye un capítulo de mitigación del riesgo.
Evolución	Modificaciones realizadas desde la primera versión hasta la actualidad.	Primera versión: Magerit v1, 1997 Última versión: Magerit v3, 2012	Primera versión: versión 0.9, 1999 Última versión: versión 2.0, Enero del 2005	Primera versión: 2002 Última versión: 2002
Idioma	Idioma del método, es esencial para dominar el vocabulario utilizado.	Español, inglés, italiano	Inglés	Inglés
Quienes pueden utilizar la metodología?	Metodologías orientadas al tipo de organización.	Instituciones del Gobierno Microempresa (empleados < 10) PYMES (11< empleados < 99) Grande empresa (empleados > 100) Organizaciones sin fines de lucro	PYMES	Instituciones del Gobierno Microempresa (empleados < 10) PYMES (11< empleados <99) Grande empresa (empleados > 100) Organizaciones sin fines de lucro

Enfoque del usuario		Gestión Técnico	Técnico	Técnico
Cumplimiento con estándares de TI	Las normas aquí mencionadas son solo referencias, únicamente la ISO/IEC 27001, la ISO 27002 e ISO/IEC 27005 se han utilizado para en el proyecto de titulación.	ISO/IEC 27001/2005 (Seguridad de la Información) ISO/IEC 15408 / 2005 (Tecnología de la información-Técnicas de Seguridad- Criterios de evaluación de la Seguridad de TI) ISO/IEC 27002 (Código de buenas prácticas para la seguridad de la información.) ISO/IEC 27005 (Gestión de riesgos).	ISO/IEC 27001/2005 (Seguridad de la Información)	ISO/IEC 27001/2005 (Seguridad de la Información)
Uso geográfico:	Uso de la metodología a nivel mundial, tomando como base la Unión Europea.	En estados miembros de la Unión Europea (UE): la metodología la utilizan varios países. Fuera de la Unión Europea (UE): la metodología la utilizan varios países.	En estados miembros de la Unión Europea (UE): no se ha encontrado registros de uso de la metodología. Fuera de la Unión Europea (UE): USA	En estados miembros de la Unión Europea (UE): no se ha encontrado registros de uso de la metodología. Fuera de la Unión Europea (UE): USA

Tomando en cuenta los criterios de gestión de riesgos especificados en la tabla anterior, se puede observar que existe diferencias y semejanzas entre las metodologías como:

- Para la Evaluación y Gestión del riesgo, Magerit ofrece una visión más amplia con pasos específicos a realizar, se basa en objetivos de seguridad de la información obteniendo como resultado un estado del riesgo junto con un plan de seguridad, por su parte Octave, deja todo el proceso de acuerdo a los criterios establecidos por el equipo analista, en cambio NIST 800-30 se basa en plantillas y ejemplos.
- Magerit es la metodología que tiene una evolución notable a diferencia de las otras mencionadas, por tanto, Magerit se acopla mejor a necesidades referentes a la gestión y evaluación de riesgos.
- Magerit fue desarrollado en idioma español, por su gran acogida se realizaron las traducciones al inglés e italiano, a diferencia de Octave y NIST 800-30 que se mantienen con el idioma inglés, en el que fueron desarrolladas.
- Tanto Magerit como NIST 800-30, pueden ser utilizadas por cualquier tipo de institución, organización o empresa, en cambio, Octave posee varios tipos como Octave-S, Octave Allegro, que deben ser utilizadas según el número de personas que laboran.
- En cuanto a enfoque del usuario Magerit posee un valor agregado, se basa en la gestión y la parte técnica. La gestión involucra a toda la información independiente del medio en que este, relaciona procesos, personas, tecnología, infraestructura; y un enfoque técnico permite proteger la infraestructura tecnológica y de comunicación de la organización.
- Magerit es la única metodología que cumple con ciertos estándares de la familia 27000, estos sirven de guía para establecer e implementar un SGSI.
- Magerit posee mayor acogida en varios países a nivel mundial.

1.5 JUSTIFICACIÓN DE LA METODOLOGÍA PARA LA GESTIÓN DE RIESGOS

El proceso de certificación y elaboración de un Sistema de Gestión de la Seguridad de la Información tiene como paso importante la elaboración de un Análisis y Gestión de Riesgos, para gestionarlos; con controles y políticas de seguridad.

En la actualidad existen varias metodologías de gestión de riesgos, le corresponde a cada organización seleccionar o identificar una que coincida con su enfoque de la gestión de riesgos.

En base a las metodologías y su comparación en la tabla 1.4.1; para el desarrollo del proyecto se utilizará la metodología Magerit, por las siguientes razones:

- Es una metodología que se basa en la seguridad de la información, a diferencia de las otras que se basan en seguridad informática; lo cual proporciona una visión amplia en cuanto a gestión y operación de la institución.
- Magerit cubre a mayor detalle la gestión de riesgos, guía específicamente las actividades y pasos que se tienen que realizar, no deja lugar a la improvisación, ni a la arbitrariedad de los analistas.
- Al ser una metodología pública incentiva a todo tipo de organizaciones públicas, privadas, pequeñas y grandes a ser conscientes de la importancia de la gestión de la seguridad de la información.
- Posee un nivel de madurez, ha evolucionado hasta la versión 3, y se basa en el proceso de gestión de riesgos de acuerdo a la NORMA ISO/IEC 31000.

1.6 ESQUEMA PARA EL PROYECTO DE TITULACIÓN

Para el desarrollo del análisis y gestión de riesgos es necesario el uso de la metodología MAGERIT libro I, II y III, junto con la Norma Técnica ISO/IEC 27005.

En resumen, nuestro esquema sigue de acuerdo a la siguiente gráfica.

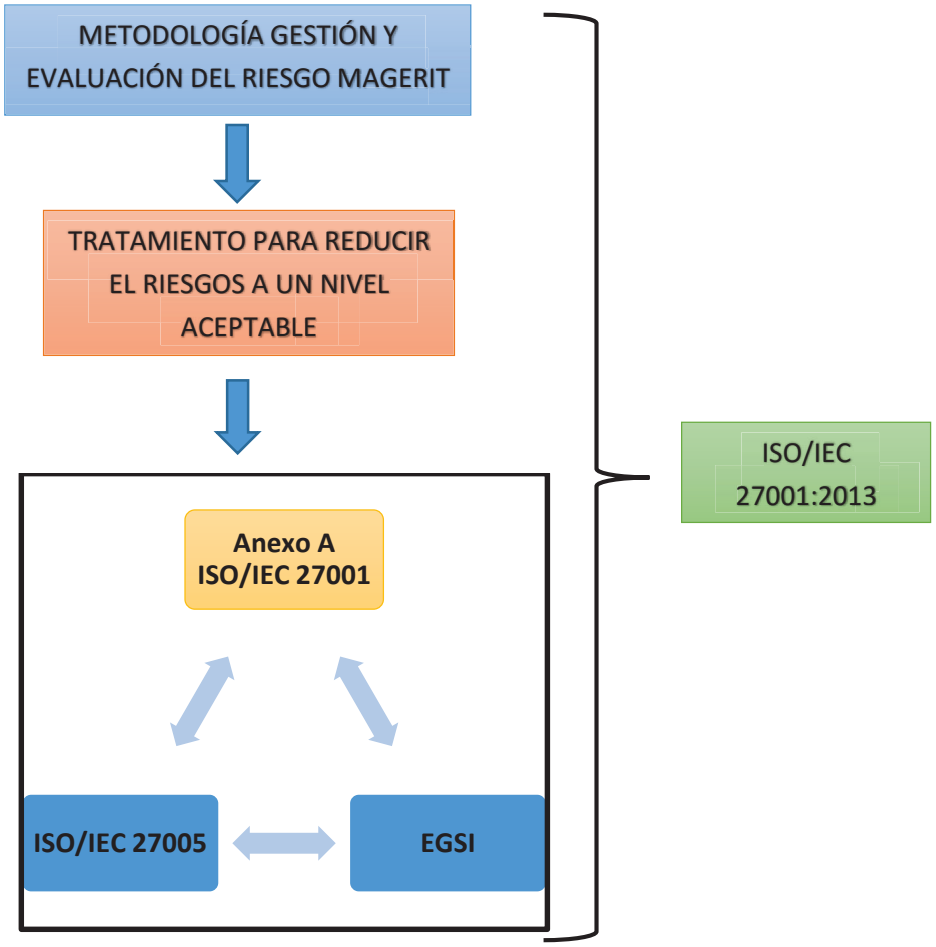


Figura N.- 1.5-1 Esquema de uso normas técnicas, acuerdos y metodología.

Fuente: Autores

Capítulo 2 ANÁLISIS Y GESTIÓN DEL RIESGO

La Gestión de riesgos de la Información es el proceso de identificación y evaluación, para reducir el riesgo a un nivel aceptable, o a su vez ser transferidos e implementar mecanismos de protección adecuados; no existe un entorno seguro al 100%.

La principal actividad es la identificación de las amenazas y su evaluación para determinar que estas, realmente ocurran y pudieran causar daño, y luego tomar las debidas medidas necesarias y adecuadas para reducir el nivel general del riesgo en el entorno de la organización la cuál establezca como aceptable.

De acuerdo K. Dejan y L. Rhand [16] , la seguridad de la información es parte de la gestión global del riesgo de una organización, y existe aspectos que se superponen con la ciberseguridad[12], con la gestión de la continuidad del negocio y con las tecnologías de la información.

Figura N.- 1.5-2 Figura de la Gestión del Riesgo y su intereacción con la Continudad del negocio, ciberseguridad, y la seguridad del información

Fuente: Dejan, Kosutic; Rhand, Leal [16]

[12] Ciberseguridad. - es la protección de activos de información a través de tratamientos de amenazas que ponen en riesgo la información que es procesada, almacenada, transportada por los sistemas de información.

Los riesgos de una Organización se encuentran en diferentes formas y no todos están relacionados con la Informática, cada Organización interactúa con otras con el fin de aumentar la productividad y la rentabilidad; por ejemplo, para aumentar una línea de productos, conlleva la necesidad de contratar personal, nuevas instalaciones, servicios básicos e instalar medios de comunicación interna y externa.

En la siguiente imagen se puede observar todo el proceso de análisis y gestión del riesgo, basado en la Norma Técnica ISO/IEC 27005 y la metodología Magerit.

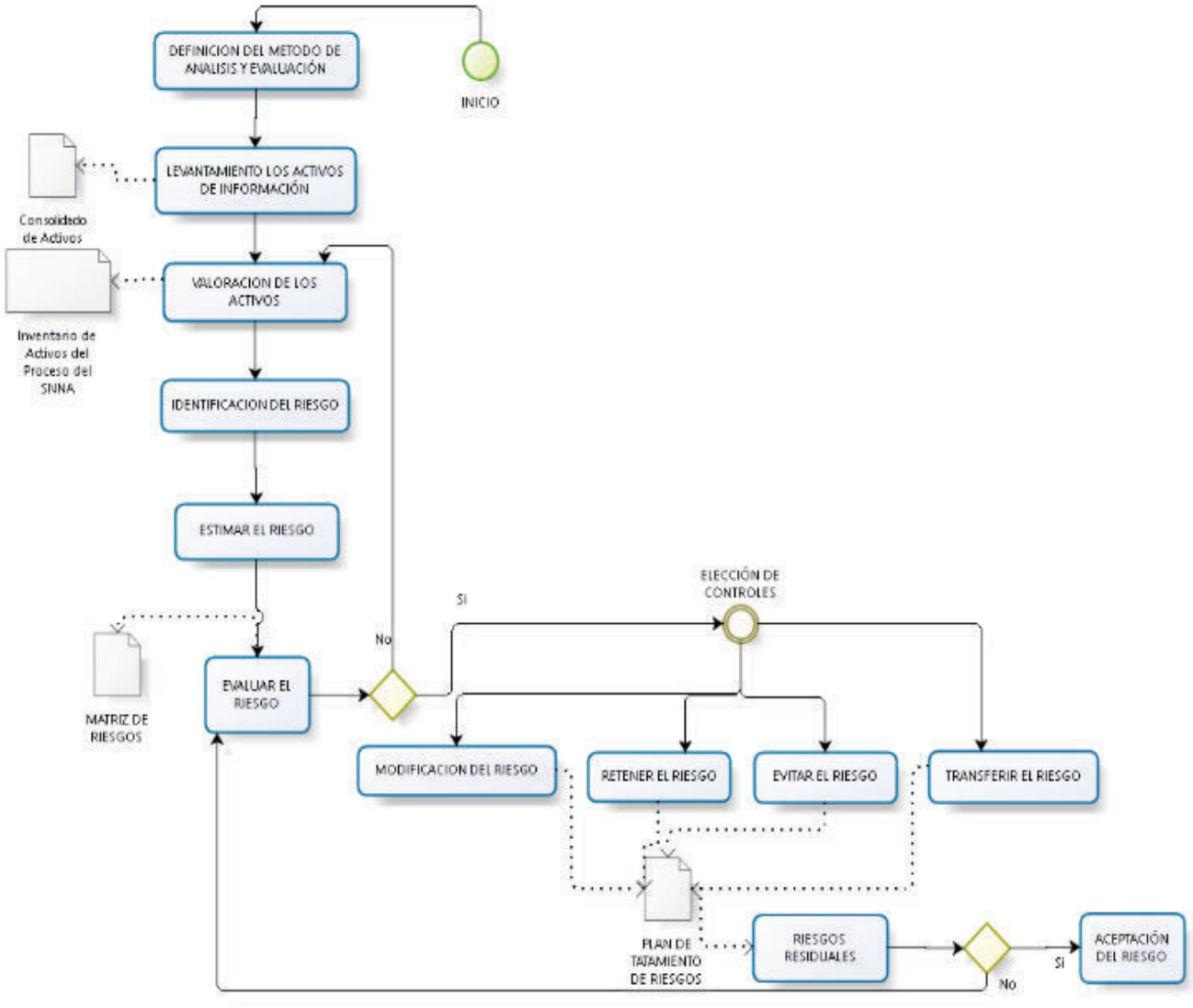


Figura N.- 1.5-3 Proceso de análisis y gestión del riesgo

Fuente: Norma Técnica ISO /IEC 27005, Magerit

2.1 ALCANCE DEL PROYECTO ACUERDO A LA NORMA ISO/IEC 27001:2013

Se utiliza la norma ISO/IEC 27001:2013 para determinar el alcance del proyecto de titulación como se muestre en la tabla N.-2.1-1, el proceso para el SGSI es extenso, se establece los límites, y las observaciones.

TABLA N.- 2.1-1 ALCANCE DEL PROYECTO DE TITULACIÓN

FUENTE: AUTORES

CLÁUSULAS	ISO/IEC 27001	ESTADO	OBSERVACIONES
4	**CONTEXTO DE LA ORGANIZACIÓN**		
4.1	Conocimiento de la Organización y su contexto	APLICA	Se describe todo el proceso del SNNA en 1.1 (Identificación de la Organización)
4.2 (a)	Regulaciones, y normas que debe cumplir	APLICA	Reglamentaciones establecidas por el SNAP.
4.2 (b)	Requisitos de cumplimiento establecidos en el Acuerdo Ministerial 166	APLICA	Se establecerá en las políticas de Seguridad de la Información de acuerdo al resultado de la valoración del riesgo.
4.3	**ALCANCE**		
4.3	Determinar los límites y aplicabilidad del Sistema de Seguridad de la Información conjuntamente con las cláusulas del Acuerdo Ministerial 166	APLICA	Proceso del SNNA.

4.4	**SGSI**		
4.4	Establecer, Implementar, mantener, y mejorar de manera contínua el SGSI	PARCIAL	Pero se aborda la parte inicial ; establecer
5	**Liderazgo**		
5.1	**Liderazgo y compromiso**		
5.1	La Alta dirección debe demostrar liderazgo y compromiso para el SGSI	PARCIAL	La máxima autoridad con el proyecto de Titulación es con el Director de TIC´s Ing. Javier Salazar, Oficial de Seguridad Ing., Milton Moya, Analista de Seguridad David Félix
5.2	**POLITICA**		
5.2	La Alta dirección debe establecer una política de seguridad de la información	NO APLICA	No se tiene acceso al documento físico.
5.3	**Funciones, responsabilidades y autoridad de la institución**		
5.3	Asignación y comunicación de las responsabilidades al equipo de seguridad de información	NO APLICA	La máxima autoridad con el proyecto de Titulación es con el Director de TIC´s Ing. Javier Salazar, Oficial de Seguridad Ing., Milton Moya, Analista de Seguridad David Félix
6	**Planificación**		
6.1	**Acciones para enfrentar los riesgo y las oportunidades**		
6.1.1	Diseñar el Plan de Seguridad	APLICA	Fase inicial del proceso de implementación que servirá como referencia inicial del proyecto para certificación ISO 27001.

6.1.2	Evaluación de los riesgos de seguridad de la información	APLICA	Se utiliza Magerit como metodología de Gestión y evaluación del Riesgo
6.1.3	Tratamiento de los riesgo	APLICA	Se utilizar ISO/IEC 27005, Anexo A de la ISO/IEC 27001, Acuerdo Ministerial 166
6.2	**Objetivos de seguridad y planificación para alcanzarlos**		
6.2	Establecer los objetivos de la seguridad de la información en relación a las funciones y niveles (La Institución debe, asignar recursos, designar responsables , establecer medidas de implementación)	PARCIAL	Por el tiempo insuficiente, pero la Institución busca certificarse y continuará con el proceso, se inicia en el proceso del SNNA.
7	**Soporte**		
7.1	**Recursos**		
7.1	Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI	NO APLICA	Debido a la decisión tomada por la Alta dirección.
7.2	**Competencia**		
7.2	Personal competente para el SGSI	PARCIAL	Se encuentra definido por la Alta dirección, y los estudiantes para realizar el proyecto de titulación.
7.3	**Concientización**		

7.3	Establecer programas de concientización	PARCIAL	Introducción sobre la seguridad de la información y cumplimientos legales,
7.4	**Comunicación**		
7.4	Determinar las necesidades de comunicación internas y externas (Qué, cuando , con quién y quién debe comunicar)	PARCIAL	Se encarga el oficial de seguridad, con las máximas autoridades, y comité de seguridad, la comunicación interna para entrevistas con cronogramas y tiempos establecidos por los funcionarios.
7.5	**Documentación de la Información**		
7.5.1	Estandarizar la documentación generada dentro del SGSI	APLICA	En las políticas.
7.5.2	Creación y actualización de la información documentada(Identificación y descripción, Formatos, revisión y aprobación)	PARCIAL	Se creará la documentación y será revisada por el Oficial de seguridad, para ser aprobada por el comité de seguridad y con la Máxima autoridad de la Secretaria.
7.5.3	Control de la Información documentada (protección y disponibilidad adecuada, almacenada, distribuida de la documentación generada del SGSI)	NO APLICA	Fuera del alcance del proyecto de titulación
8	**Operación**		
8.1	**Planificación y control operacional**		
8.1	Planificar, implementar y controlar los procesos necesarios para cumplir los	NO APLICA	Fuera del alcance del proyecto de titulación

	requerimientos de la seguridad de la información		
8.2	**Evaluación de los riesgos de la seguridad de la información**		
8.2	Evaluar los riesgos del SI en intervalos o cuando exista cambios significativos	NO APLICA	Fuera del alcance del proyecto de titulación
8.3	**Tratamiento de los riesgos de SI**		
8.3	Implementar el plan de tratamiento de los riesgo de la seguridad de la información	NO APLICA	Fuera del alcance del proyecto de titulación
9	**Evaluación de desempeño.**		
9.1	**Monitoreo, medición, análisis, y evaluación**		
9.1	Monitoreo, medición, análisis, y evaluación SGSI	NO APLICA	Fuera del alcance del proyecto de titulación
9.2	**Auditoria Interna**		
9.2	Plan de auditoria interna (Dirección en intervalos planificados)	NO APLICA	Fuera del alcance del proyecto de titulación
9.3	**Revisión por parte de la dirección**		
9.3	Revisión a intervalos establecidos para garantizar la continuidad del SGSI.	NO APLICA	Fuera del alcance del proyecto de titulación
10	**Mejora**		
10.1	**Acción correctiva y no conformidad**		
10.1	Identificar, corregir y tomar acciones de prevención de no conformidades y documentar dichas acciones.	NO APLICA	Fuera del alcance del proyecto de titulación

10.2	**Mejora continua**		
10.2	Desarrollar plan de mejora continua.	NO APLICA	Fuera del alcance del proyecto de titulación
	TOTAL	**27**	

De un 100% de los requisitos que establece la Norma Técnica en la TABLA N.-2.1-2., se muestra el 30% de aplicación total y un parcial del 26% en el proceso del SNNA, este porcentaje sumado es 56% establece como punto inicial, debido a las limitaciones dentro de la institución y decisiones que deben ser tomadas por funcionarios directores con la máxima autoridad de la SENESCYT, además como es un proceso de mejora continua es razón que a partir del cláusula 8 de Norma NO SE APLICA.

TABLA N.- 2.1-2 PORCENTAJES DE CUMPLIMIENTO

FUENTE: AUTORES

ESTADO	DESCRIPCIÓN	PORCENTAJES
NO APLICA	Fuera del alcance del proyecto de titulación	**44%**
APLICA	Objetivos del proyecto de titulación.	**30%**
PARCIAL	Cumple con un porcentaje de aportación para establecer el SGSI	**26%**
TOTAL		**100%**

2.2 ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SNNA

El análisis de brechas o GAP análisis es un estudio preliminar que permite conocer a la institución, la forma en la que se desempeña en materia de la seguridad de la información, en relación a las mejores prácticas reconocidas en la industria.
Análisis de Brechas permite determinar cuáles son los procesos para salvaguardar la seguridad de la información, y aquellos que necesitan mejorar, o cambiar si es necesario.
Este análisis permite diferenciar el desempeño actual y aquel que se desea alcanzar sugeridas por Anexo A del estándar ISO/IEC 27001; Este resultado se puede presentar mediante un informe en el que se muestra los indicadores sobre las deficiencias encontradas.

El SNNA es un macro proceso que se subdivide en dos subprocesos: Nivelación y Admisión, por tanto, para determinar la situación actual se realizó entrevistas a los líderes de los procesos y al personal de TI, respectivamente.

De acuerdo la Metodología Magerit Libro III [17] **Cláusula 3.6.1.-** Las entrevistas o reuniones se las realizaron por grupos de acuerdo a cada unidad involucrada en el proceso, es decir, se realizó una entrevista semi-estructurada, utilizando lenguaje común; para entender sobre las funciones y el subproceso que realizaba el/la funcionario/a público; se logró identificar qué tipo de información maneja, utiliza o produce, los servicios institucionales que utilizan para cumplir con los objetivos del negocio, los responsables de cada área y/o servicio el rol que posee dentro de la institución, y comparten situaciones en las cuales la seguridad de la información propia o institucional fue comprometida, altera o robada.

Este tipo de información fue recopilada con el fin de obtener información relevante para la realización de este proyecto de titulación, manteniendo reuniones a fechas y horas establecidas por los funcionarios/as y con autorización de los jefes inmediatos.

Para el desarrollo de esta sección fue necesario la utilización del ANEXO A, y la lista de cumplimiento de la norma ISO/IEC 27001. Halkyn Consulting Ltd [18].

Para llevar a cabo el análisis de brechas de acuerdo a PECB [8, pp. 141,142], se debe:

1. Identificar los procesos y controles de seguridad vigentes y sus características más relevantes.

2. Identificar los objetivos sobre la seguridad de la información que produce, maneja o intercambia con otras instituciones del estado o privadas.

3. Identificar las diferencias que pueden existir entre los controles de seguridad que la institución posee como buenas prácticas, los requisitos y objetivos de control de acuerdo a la Norma ISO/IEC 27001:2013.

En la **Tabla N.- 2.2-1** se muestra el valor de 1, si cumple con la pregunta de auditoría caso contrario se le asigna el valor de 0 para realizar el cálculo en porcentaje correspondiente.

TABLA N.- 2.2-1 VALOR DE CUMPLIMIENTO CONFORME A LA PREGUNTA DE AUDITORÍA

CUMPLIMIENTO	VALOR
SI	1
NO	0
CUMPLE EN 50%	0.5

Con el objetivo de obtener un porcentaje se sumarán todas las preguntas con valor 1 y se dividirá para el total de preguntas; es decir; se saca un promedio por cada pregunta al final de la tabla “ESTADO %” se obtendrá un porcentaje de acuerdo a los controles de cada dominio 100%.

En la **Tabla N.- 2.2-2** se muestra el cumplimento actual de la Norma ISO/IEC 27001:2013; de acuerdo a entrevistas realizadas y preguntas de auditoría, con el fin

de determinar qué porcentaje de cumplimiento poseen en cada dominio, todo el desarrollo se puede visualizar en el ANEXO A “Situación Actual”.

TABLA N.- 2.2-2 GAP ANÁLISIS PORCENTAJE POR DOMINIO

FUENTE: COMPLIANCE CHECK ISO [19]

POLÍTICA DE SEGURIDAD	PREGUNTA DE AUDITORÍA	CUMPLIMIENTO	ESTADO %	OBSERVACIONES
A.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN			30,00%	
A.5.1.1 Políticas para seguridad de la información	Existe una Política de Seguridad de la Información que es aprobada por la dirección, publicada y comunicada a todos los empleados?	0,5	0,1	La Institución posee una política de seguridad de la información, pero no ha existido un proceso de divulgación y concientización al personal.
	Establecen las políticas un compromiso de la Alta Dirección con relación a la gestión de la seguridad de la información?	1	0,2	La Alta Dirección tiene conocimiento sobre la importancia de la seguridad en la información que la institución posee, crea, y transmite. Teniendo en cuenta que cualquier filtración puede causar mala reputación de carácter público.
A.5.1.2 Revisión de las políticas para seguridad de la información	Las políticas de seguridad son revisadas a intervalos regulares, o cuando hay cambios significativos?	0	0	No son revisadas, solo se limitan a cumplir con buenas prácticas, referente al cambio se mantiene en su primera versión.
	Las políticas de seguridad tienen un propietario responsable del desarrollo, revisión y	0	0	No posee un responsable, pero como se está en la fase inicial, se asignaron responsabilidades, Por consiguiente la tarea es

	evaluación de la política de seguridad?			precisamente del Oficial de seguridad, para crearlas, revisar.
	Se obtiene la aprobación de la alta gerencia con relación a las políticas revisadas?	0	0	Desde su creación no se ha realizado una revisión de la política de seguridad de información.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			35,71%	
A.6.1.1 Roles y responsabilidades de seguridad de la información	Se han definido y asignado responsabilidades relacionadas a seguridad de la información?	1	0,143	La institución ha contratado especialistas capacitados y con experiencia para implementar el SGSI.
A.6.1.2 Segregación de deberes	Están establecidas las responsabilidades de protección de activos individuales y llevar a cabo procesos de seguridad específicos que estén claramente identificados y definidos?	1	0,143	Se ha evidenciado la existencia de un grupo de seguridad de la información, conformado por un oficial de seguridad y analista de seguridad, quienes con el CONSULTOR ejecutarán el Plan para el SGSI.
A.6.1.3 Contacto con autoridades	Existe algún procedimiento que describa cuando y quienes deben contactar a las autoridades competentes y cómo deben reportarse los incidentes?	0	0,000	Si existe un incidente critico el personal reporta a su superior, pero no existe un procedimiento formal.
A.6.1.4 Contacto con grupos de interés especiales	Existen los contactos apropiados con grupos especiales de interés, foros de seguridad o asociaciones profesionales relacionadas con seguridad?	0,5	0,071	La institución ha contratado a una consultora, que sirve de guía en la implementación de la ISO 27001, como se considera un proyecto interno no se puede hacer pública lo encontrado.

A.6.1.5 Seguridad de la información en gestión de proyectos	Existe un procedimiento de seguridad de la información en la realización de proyectos?	0	0	No existe procedimiento.
A.6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO				
A.6.2.1 Política sobre dispositivos móviles	Existe una Política de seguridad y medios de seguridad de soporte para protegerse del riesgo generado por el uso de dispositivos móviles?	0	0	No existe la política formal sobre el uso, conexión a la red interna de los dispositivos móviles.
A.6.2.2 Tele-trabajo	Existe una Política o medios de seguridad de soporte para proteger la información a la que se tiene acceso y que es procesada o almacenada en los lugares en los que se realiza teletrabajo?	0	0	No existe la política de trabajo a distancia.
A.7 SEGURIDAD DE RECURSOS HUMANOS			**42,86%**	
A.7.1 ANTES DE ASUMIR EL EMPLEO				
A.7.1.1 Selección	Existe controles de verificación de antecedente para todos los candidatos a empleo, contratistas y proveedores son llevados a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes?	1	0,143	La Unidad de Talento Humano, es la encargada del cumplimiento de la selección adecuado del personal, sea estos por concurso de méritos y oposición o por prestación de servicios ocasionales. Proveedores por medio de la Unidad de Finanzas si han cumplido todo los requisitos en el portal de compras públicas.

A.7.1.2 Términos y condiciones de empleo	Firman los empleados, contratistas y proveedores, contratos de confidencial y acuerdos de no divulgación como parte inicial de los términos y condiciones de trabajo?	0,5	0,071	No todos los funcionarios han firmado un acuerdo de confidencial.
	Los acuerdos de confidencialidad y contratos cubren las responsabilidades de los empleados, contratistas y proveedores, haciendo referencia sobre las cláusulas , restricciones que cada uno de los anteriores tendrán al firmarlo.	0	0,000	Los acuerdos no están completamente redactados para los contratistas o proveedores de servicio.
A.7.2 DURANTE LA EJECUCIÓN DEL EMPLEO				
A.7.2.1 Gestión de responsabilidades	La dirección exige a los empleados y contratistas la aplicación de seguridad de la información de acuerdo a las políticas y procedimientos establecidos en la institución?	0	0,000	No Existe roles y responsabilidades de los funcionarios sobre el uso, manipulación y divulgación de la información generada en la Organización, desconocimiento del tipo de información que manejan durante el empleo.
A.7.2.2 Concienciación, educación y capacitación en seguridad de la información	Los empleados, contratistas y proveedores reciben la apropiada concientización, educación y formación permanente sobre la Seguridad de Información con respecto a sus	0	0,000	Los empleados, contratistas y proveedores no han recibido concientización por parte de la institución.

	funciones laborales especificas?			
A.7.2.3 Proceso disciplinario	Existe un proceso disciplinario para aquellos empleados que incumplan las políticas de seguridad?	0,5	0,071	Existe un documento CÓDIGO DE ÉTICA DE LA SENESCYT, donde incluye sanciones, para quienes incumplan con las condiciones laborales, no son aplicadas por ser sanciones leves, caso contrario serán escalados a los organismos correspondientes, según sea la gravedad.
A.7.3 TERMINACIÓN Y CAMBIO DE EMPLEO				
A.7.3.1 Terminación o cambio de condiciones del empleo	Las responsabilidades de procedimientos de terminación o cambio de empleo están claramente definidas y asignadas?	1	0,143	La Unidad de Talento Humano es el encargado de procedimientos de cese de funciones, y cambios de puestos por ascensos o encargos temporales, Su medio de comunicación es por medio informe físico; digital mediante QUIPUX firmada digitalmente con solo entrega a su destinatario.

2.2.1 ANÁLISIS DEL ESTADO ACTUAL Y DEL ACUERDO 166

En concreto se evaluaron un total de 114 controles de seguridad, repartidos en 35 objetivos, con este análisis GAP se pudo observar las áreas donde el proceso del SNNA no alcanza un nivel aceptable en porcentaje del estándar internacional para la gestión de la seguridad de la información.

El objetivo de la Tabla N.- 2.2-2 es conocer el estado en el que se encuentra el proceso del Sistema Nacional de Nivelación y Admisión, a nivel de medidas de seguridad, técnicas, organizacionales y legales.

De acuerdo a la **cláusula A.7**, presenta un 42.86% debido a que existe un reglamento de contratación de funcionarios y servicios, los mismos que están regulados por el Ministerio de Trabajo, y el SNAP.

Según la **Cláusula A.9** se evidencia un 36.86 %, este resultado se obtiene de acuerdo a buenas prácticas de gestión de control de acceso, pero el mismo no está normado, o documentado, si es el caso, por ejemplo, un funcionario deja de trabajar en la Institución inesperadamente, este no puede transferir el concomimiento o este no ha sido establecido en un proceso. La institución cuenta con una buena infraestructura y seguridad física, personal de seguridad externa adquirida como servicio; de lo más relevante se determina que no llevan un registro de visitantes, y por confianza no realizan revisiones internas del equipaje de los funcionarios/as que lleva y salen de su lugar de trabajo, permiten el acceso de personas que no pertenecen a la institución.

El porcentaje corresponde de la **cláusula A.17 18.75%**, no poseen un plan de continuidad operacional de las plataformas y demás servicios considerados críticos para el proceso, el mismo en que este se cae, o no responde con normalidad, no tienen establecidos tiempos mínimos de recuperación y/o el procedimiento de backup no se ha realizado pruebas funcionales.

En el caso del proceso de lectura y escaneo de exámenes los riesgos son por parte del personal, la información de las preguntas y respuestas puede ser vulnerada.

Por lo tanto, al analizar el Acuerdo 166, no es una guía de implementación de un Sistema de Seguridad de la Información, tan solo se limita a tener una correcta gestión en el cuál se han establecido directrices prioritarias que deben ser aplicadas e implementadas en un período de 6 meses, y las directrices no prioritarias en un período no mayor a 18 meses, este acuerdo debe ser aplicada en toda institución del estado, que esté bajo la función Ejecutiva sin excepción alguna.

Por lo tanto, el Acuerdo 166 (EGSI), es una referencia de buenas prácticas de la Norma Técnica ISO/IEC 27002 del año 2005, por lo que el SNAP debe actualizar a la nueva versión vigente si las instituciones del estado, optan por acreditarse en la Norma

ISO/IEC 27001, y se ha optado por seguir los documentos obligatorios y no obligatorios según la norma ISO/IEC 27001:2013.

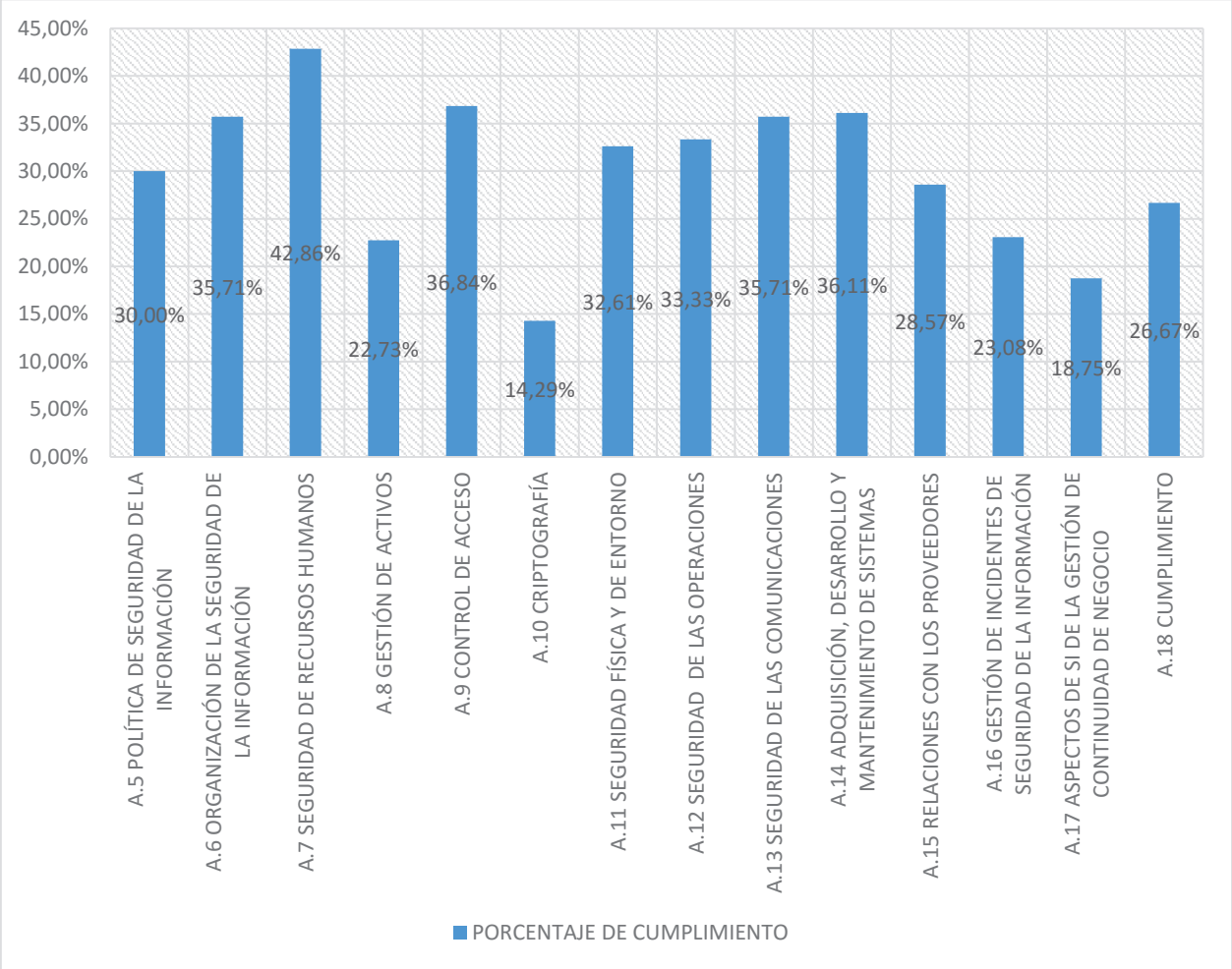


Figura N.- 2.2-1 Porcentaje de cumplimento de controles de la Norma ISO 27001:2013

Fuente: Autores

2.3 APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y VALORACIÓN DEL RIESGO

El análisis de riesgos permite determinar los activos importantes de la organización y las amenazas a las que están expuestas causando perjuicio o daño.

Al determinar los activos y sus amenazas, se procederá a definir medidas de protección o salvaguardas que disminuyan el daño que producen en la organización.

De acuerdo a INCOTEC, Norma Técnica Colombiana NTC 5254 Gestión del Riesgo [20]**;** ***Cláusula 4.3.1 Generalidades***.- El riesgo se analiza mediante la combinación de estimaciones de consecuencias y posibilidad en el contexto de las medidas de control existentes, decir se debe considerar las fuentes de riesgo, sus consecuencias y la posibilidad de que estas consecuencias ocurran.

Para realizar el análisis de riesgos se requiere de las siguientes actividades:

1. Determinar los activos, su interrelación y el valor que este tiene para la Organización.
2. Definir los activos hay que determinar las amenazas a que estos están expuestos.
3. Determinar los controles para gestionar el riesgo
4. Estimar el impacto y la probabilidad, es el daño y la posibilidad de que ocurra la materialización de la amenaza.
5. Estimar riesgo, posibilidad de que una amenaza explote una vulnerabilidad y cause daño.

2.3.1 PASO 1: IDENTIFICACIÓN DE ACTIVOS

La identificación de activos involucra varias actividades con el fin de recolectar y analizar datos, se los categoriza por tipo, y se los identifica mediante las relaciones con los demás activos, se determina las propiedades de seguridad y por último se valora cada una de las mencionadas propiedades.

Definición de Activo. - es cualquier cosa que sea de valor para la organización y por la misma razón necesita y debe ser protegida. [8, p. 74]

Para la identificación de un activo se debe tener en cuenta que un sistema de información consiste mucho más allá que su parte física Hardware o su parte lógica que es su Software.

Con el fin de identificar los activos de información se hace uso de la Norma ISO 27005, ANEXO B.- divide a los activos en dos categorías, estos son: Activos primarios, Activos secundarios

2.3.1.1 ACTIVOS PRIMARIOS

En esta categoría se encuentran los procesos de negocio; se los debe tener muy en cuenta en el análisis de riesgos.

Los activos primarios de la institución son los siguientes:

- Proceso “Sistema Nacional de Nivelación y Admisión”
- Subprocesos: Nivelación y Admisión.

2.3.1.2 ACTIVOS SECUNDARIOS - CATEGORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN

En esta categoría están: hardware, software, redes informáticas, personal, sitios y estructuras organizativas.

Para facilitar el análisis, los activos deben ser consolidados en grupos que tienen aproximadamente su misma característica y el mismo nivel de clasificación en términos de seguridad de la información.

Los activos de información que deben ser tomando en cuenta principalmente son aquellos que permitan a la organización cumplir con su misión.

Con la ayuda del “Catálogo de elementos” del libro II de Magerit Versión 3, se categoriza los activos de información según se muestra en la **Tabla. - 2.3-1**:

TABLA N.- 2.3-1 CATEGORÍA ACTIVOS DE INFORMACIÓN

FUENTE: MAGERIT LIBRO II PÁGINAS 7-13,

Grupo de activos	Descripción del grupo de activos
Datos/Información	*Activo de información esencial en medio físico o digital*. Tales como: Estructurada (DBMS) , No Estructurada (Excel, Pdfs, Docs., txts, htmls) Información en medio físico: documentos impresos, copias, hojas de respuestas, memorándums, etc. Información en medio Lógico (Carpetas Compartidas), informes de calificaciones, documentos digitales. Etc.
Software	*Equipamiento de software que permite gestionar e interactuar con los datos*. Sistemas de información del Negocio, Sistemas Operativos, DBMS, Antivirus
Sitio	*Instalaciones físicas, ubicación de los equipos informáticos y de comunicaciones*: Centros de cómputo y telecomunicaciones, Oficinas Superficies de trabajo normal.
Hardware	Equipo físico que alojan datos información o aplicaciones PC's, Servidores, Portátiles, Impresoras en Red, Medios de Almacenamiento, USB.
Red	*Equipos que permite el intercambio de datos e información entre los activos*. LAN, WAN,SWITCH, Firewall, ACCESS POINT
Recurso Humano	*Relacionado con las personas que operan, organizan y gestionan los servicios*: Roles Funcionales (usuarios) ,Roles de Soporte y Mantenimiento IT, Funcionarios ,Usuarios Externos Tercerizados, Tomadores de Decisión
Servicios	*Conjunto de activos de información que permite a la institución realizar actividades relacionadas con*: Internet, Directorio Activo, Correo Electrónico, Seguridad.

2.3.1.3 INVENTARIO DE ACTIVOS DE INFORMACIÓN

De la información recopilada del proceso del SNNA, mediante un análisis junto con el oficial y el analista de seguridad, se define la tabla de inventario de activos como se muestra en la **Tabla N.-2.3-2**:
El inventario completo de Activos de Información-Proceso Sistema Nacional de Nivelación y Admisión se encuentra en el ANEXO B "Gestión_Activos_SNNA" libro 2. Activos del proceso y libro 2b. Consolidado Activos.

TABLA N.- 2.3-2 INVENTARIO DE ACTIVOS DE INFORMACIÓN

FUENTE: AUTORES

CÓDIGO	PROCESO	SUBPROCESO	ACTIVOS	CATEGORÍA	DESCRIPCIÓN
Identificador del Activo de Información	Nombre del proceso que interviene o está vinculado el activo de Información	Subproceso que interviene o está vinculado el activo de Información	"Nombre del Objeto" Especificación del Activo (Sistema Operativo, persona, laptops, etc.)	Se especifica la categoría la que pertenece el activo de Información sea éste (Hardware, Software, Red, etc.)	Se especifica el Activo de Información, sea éste técnico o si se trata de algún Hardware o la función de un aplicativo.
A8	Sistema Nacional de Nivelación y Admisión	SNNA	Switch	Red	CISCO CATALYST 3750- X 48 PoE

2.3.1.4 ESCALAS PARA DETERMINAR EL VALOR DE LOS ACTIVOS DE INFORMACIÓN.

"La valoración se puede ver desde la perspectiva de la '**necesidad de proteger**' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes." [21]

Para el desarrollo del proyecto se realizó una combinación de una escala cualitativa y una escala cuantitativa.

- Escala Cuantitativa

  Se utiliza una escala con valores numéricos, permite realizar estudios económicos comparando lo que se arriesga con lo que cuesta la solución.

  La escala cuantitativa se muestra en la **Tabla N.-2.3-3** y se visualiza diferentes colores para cada uno.

TABLA N.- 2.3-3 ESCALA CUANTITATIVA PARA VALORAR LOS ACTIVOS DE INFORMACIÓN

FUENTE: MAGERIT LIBRO II PÁGINAS 19.

VALOR
1
2
3
4
5

- Escala cualitativa

Se utiliza una escala de condiciones de clasificación para describir la magnitud de las posibles consecuencias y la probabilidad de que esas consecuencias se produzcan, como se muestra en la **Tabla N.-2.3-4**.

TABLA N.- 2.3-4 ESCALA CUALITATIVA PARA DETERMINAR LOS VALORARES DE LOS ACTIVOS DE INFORMACIÓN

FUENTE: MAGERIT LIBRO II PÁGINA 19.

MUY BAJO
BAJO
MEDIO
ALTO
MUY ALTO

2.3.1.5 DESCRIPCIÓN DE LA ESCALA PARA LA VALORACIÓN DE ACTIVOS

Para la valoración de los activos de información de la Institución, se debe establecer dimensiones, estos son descritos a continuación:

- Confidencialidad (C)

Garantiza que la información va ser accesible solo por aquellas personas que poseen permiso, es decir:" *¿qué daño causaría que lo conociera quien no debe?"*
Esta valoración es típica para los datos. [14, p. 24]

La escala correspondiente a esta dimensión se muestra en la **Tabla N-2.3-5**:

TABLA N.- 2.3-5 DIMENSIÓN CUANTITATIVA Y CUALITATIVA PARA DETERMINAR LA CONFIDENCIALIDAD DE LOS ACTIVOS DE INFORMACIÓN

FUENTE: MAGERIT LIBRO II PÁGINAS 15.

ESCALA CUANTITATIVA	**ESCALA CUALITATIVA**	**DESCRIPCIÓN**
1	Muy Bajo	Activo de acceso público, la cual puede ser visto por cualquier funcionario.

2	Bajo	Acceso por funcionarios internos, y proveedores propio de la institución.
3	Medio	Acceso limitado solo a líderes del proceso.
4	Alto	Restringido por el comité de seguridad, y/o no puede ser divulgada ni compartida.
5	Muy Alto	Considerado como confidencial la cual tiene acceso la alta dirección.

- Integridad (I):

Garantiza que los activos estén completos y no exista modificaciones.

Esta valoración es típica para los datos, que pueden ser manipulados en su totalidad o parcial e incluso puede carecer de estos.

La escala correspondiente a esta dimensión se muestra en la Tabla **N-2.3-6**:

TABLA N.- 2.3-6 DIMENSIÓN CUANTITATIVA Y CUALITATIVA PARA DETERMINAR LA INTEGRIDAD DE LOS ACTIVOS

FUENTE: MAGERIT LIBRO II PÁGINA 15.

ESCALA CUANTITATIVA	**ESCALA CUALITATIVA**	**DESCRIPCIÓN**
1	Muy Bajo	Activo de acceso público, la cual puede ser modificado por cualquier funcionario.
2	Bajo	Acceso por funcionarios internos, y proveedores propio de la institución, cuya modificación no altere el proceso core.

3	Medio	Modificaciones solo lo realizan los líderes del proceso.
4	Alto	Restringido por el comité de seguridad, y puede ser modificada, tan solo por los dueños del proceso. y/o aprobados por los jefes de los departamentos.
5	Muy Alto	Considerado como confidencial, la modificación solo puede hacerse por parte de la Alta Dirección de la Institución.

- Disponibilidad (D):

Garantiza que sea accesible y utilizable por las personas que lo necesitan.

Esta valoración es típica de los servicios.

La escala correspondiente a esta dimensión se muestra en la Tabla **N-2.3-7**:

TABLA N.- 2.3-7 DIMENSIÓN CUANTITATIVA Y CUALITATIVA PARA DETERMINAR LA DISPONIBILIDAD DE LOS ACTIVOS INFORMACIÓN

FUENTE: MAGERIT LIBRO II PÁGINA 15.

ESCALA CUANTITATIVA	**ESCALA CUALITATIVA**	**DESCRIPCIÓN**
1	Muy Bajo	El activo no está disponible por el intervalo de tiempo de una semana.
2	Bajo	Tiempo de indisponibilidad 3 horas, y no afecta al proceso.
3	Medio	Tiempo de indisponibilidad 1 día, se presente interrupciones en el proceso.

4	Alto	Tiempo de indisponibilidad debe ser menor de 3 horas, se siente malestar para realizar las funciones del proceso.
5	Muy Alto	Disponibilidad del 100% operativo.

El valor del activo corresponde a la suma de los valores de la confidencialidad, integridad y disponibilidad, de acuerdo a la escala cuantitativa y cuantitativa.

Ecuación para calcular el valor de un activo de información es:

$$\boldsymbol{Valor\ de\ Activo = Confidencialidad + Ingridad + Disponibilidad} \quad [\boldsymbol{Ec.1}]$$

TABLA N.- 2.3-8 ESCALA DE VALORACIÓN DE UN ACTIVO DE INFORMACIÓN

FUENTE: MAGERIT LIBRO II, PÁG. 15-16.

INTERVALO	CUALIFICACIÓN	DESCRIPCIÓN (SE PRODUCE/ HACE DAÑO)
1 a 5	Bajo	Menor /leve
6 a 9	Medio	Importante
10 a 14	Alto	Grave
15	Muy alto	Desastroso o muy grave

2.3.1.6 VALORACIÓN DEL INVENTARIO DE LOS ACTIVOS DE INFORMACIÓN.

Con información obtenida se crea la matriz de inventarios de activos como se muestra en la **Tabla N.-2.3-9**:

TABLA N.- 2.3-9 INVENTARIO DE ACTIVOS DE INFORMACIÓN Y LA VALORACIÓN

FUENTE: AUTORES.

CÓDIGO	ACTIVOS	CATEGORÍA	DESCRIPCIÓN	UBICACIÓN	RESPONSABLE/DUEÑO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO C+I+D
A1	Plataforma (adminsiniv)	Software	Plataforma Core	Edificio Rendón	DIRECCIÓN DE TIC	**5**	**5**	**5**	**15**
A2	Plataforma Contac Center	Software	Plataforma Contac Center	Edificio Rendón	DIRECCIÓN DE TIC	**5**	**5**	**5**	**15**
A3	Plataforma Jóvenes	Software	Plataforma Jóvenes	Edificio Rendón	DIRECCIÓN DE TIC	**4**	**4**	**5**	**13**
A4	Plataforma chat	Software	Plataforma chat	Edificio Rendón	DIRECCIÓN DE TIC	**5**	**4**	**5**	**14**
A5	Oficinas SNNA	Sitio	Oficinas SNNA	Edificio Rendón	DIRECCIÓN ADMINISTRATIVA			**5**	**5**

2.3.2 PASO 2: AMENAZAS Y VULNERABILIDADES

Definición de Amenaza. - "… Es cualquier peligro potencial que está asociada con la explotación de una vulnerabilidad". [22].

Las amenas son situaciones que desencadenan en un incidente en la organización, realizando un daño materia o pérdidas inmateriales en los activos de información.

Definición de Vulnerabilidad. - *"…* Es una debilidad que de un activo de información o de control que potencialmente podría ser explotada por una o más amenazas". [22].

Identificadas las amenazas se procede a identificar las vulnerabilidades relacionadas a los activos de información.

Evaluar la vulnerabilidad puede resultar una actividad muy complicada debido a una percepción errónea de que las debilidades o deficiencias siempre están asociadas con características **negativas**, ejemplo: En el caso de un sistema de información donde los "**parches**" no se actualizan. Pero puede suceder en algunos casos que una vulnerabilidad puede estar asociada con una característica **positiva**, la cual puede tener efectos secundarios indeseables. Por ejemplo: La movilidad de los equipos portátiles es un beneficio por lo que una persona paga un precio muy alto, pero es una desventaja que los hace más propensos a ser robados.

2.3.2.1 IDENTIFICACIÓN Y CLASIFICACIÓN DE LAS AMENAZAS SEGÚN LA METODOLOGÍA MAGERIT

Una vez identificado los activos de información, se debe identificar las amenazas (cosas que ocurren), caracterizándolas por las estimaciones de ocurrencia (probabilidad) y el daño causado (degradación).

Magerit clasifica a las amenazas como se muestra en la **Tabla N.- 2.3-10.**

TABLA N.- 2.3-10 CLASIFICACIÓN DE LAS AMENAZAS

FUENTE: MAGERIT LIBRO I V 3., PÁG 27

AMENAZA	DESCRIPCIÓN
De origen natural	Causa directa o indirecta producida por la Naturaleza (terremotos, inundaciones, incendios…)
Del entorno (origen industrial)	Son sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana. Desastres Industriales (contaminación, fallos eléctricos, etc.)
Defectos de las aplicaciones	Defectos de diseño, implementación que conducen a consecuencias negativas sobre el sistema.
Causadas por las personas de forma accidental	Personas con acceso al sistema de información pueden causar daño no intencionado, típicamente por error o por omisión.
Causadas por las personas de forma deliberada	Personas con acceso al sistema de información, causan daño intencionalmente.

2.3.2.2 CATÁLOGO DE AMENAZAS SEGÚN LA NORMA TÉCNICA ISO/IEC 27005

Para desarrollo del catálogo de amenazas fue necesario el uso del ANEXO C de la norma ISO/IEC 27005 y el libro 2 de Magerit, capítulo 5 del “Catalogo de elementos”. En el catálogo, se define la amenaza, la propiedad de seguridad y el activo que son afectos directamente, como se muestra en la **Tabla N.-2.3-11**, el catálogo completo se encuentra en el ANEXO C Tratamiento del Riesgo libro T. Catálogo Amenaza

TABLA N.- 2.3-11 PARTE DEL CATÁLOGO DE AMENAZAS Y CATEGORÍA DE ACTIVOS DE INFORMACIÓN QUE SON DIRECTAMENTE AFECTADOS

FUENTE: MAGERIT LIBRO II, PÁG 25-48.

Código	Amenaza	Descripción	Propiedad de seguridad afectadas	Categorías	Categoría de Activos afectados por la Amenaza						
					Información	Software	Sitio	Hardware	Red	Recurso Humano	Servicios
Origen Natural											
T1	**Desastre Natural-Fuego/Incendio**	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos. Incendios: posibilidad de que el fuego acabe con recursos del sistema e infraestructura.	Disponibilidad	Información Sitio Hardware Red Recurso Humano Servicio	x		x	x	x	x	x

T2	**Desastre Natural-Daños por Agua**	Suceso de causa que puede ocurrir sin la intervención de los seres humanos. Ejemplo: inundaciones.	Disponibilidad	Información Sitio Hardware Red Servicio	x		x	x	x		**x**
T3	**Desastre Natural-Rayos, Tormenta Eléctrica**	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos. Fenómeno natural con efectos eléctricos	Disponibilidad	Información Hardware Red Servicio	x			x	x		**x**
T4	**Desastre Natural-Terremoto, Volcánico**	Suceso de causa directa o indirecta que pueden ocurrir sin intervención de los seres humanos. Fenómeno natural de movimientos fuertes de tierra	Disponibilidad	Información Sitio Hardware Red Recurso Humano Servicio	x		x	x	x	x	**x**

2.3.2.3 CATÁLOGO DE VULNERABILIDADES

De acuerdo al Estándar ISO/IEC 27005, **cláusula 8.2.1.5** se debe identificar las vulnerabilidades, que es una debilidad que por sí mismas no causa daño, pero puede dar paso a una amenaza que puede explotarla y causar daño a la organización.

El catálogo de vulnerabilidades fue diseñado en base al ANEXO D de la norma ISO/IEC 27005. El catalogo está compuesto por la vulnerabilidad y la amenaza relacionada; además se las agrupa de acuerdo al tipo de activo, como se muestra en la **Tabla N.-2.3-12**, el catálogo completo se encuentra en el ANEXO C Tratamiento del Riesgo libro V. Catálogo de Vulnerabilidades

TABLA N.- 2.3-12 CATÁLOGO DE VULNERABILIDADES ESPECÍFICAS POR ACTIVO O GRUPOS DE ACTIVOS

FUENTE: ANEXO D, E NORMA TÉCNICA ISO/IEC 27005.

	VULNERABILIDADES ESPECÍFICAS POR ACTIVO O GRUPO DE ACTIVOS		
	Código	**Vulnerabilidad se toma en términos de Falta ,ausencia, insuficiencia o falta de controles**	**Amenazas relacionadas**
Activos tipo SITIO/AMBIENTE	**V1**	Control de acceso físico a los funcionarios, y dentro de la organización, no existe autenticación al ingreso a la sala de servidores.	T37,T58,T59,T60
	V2	La institución no cuenta con un espacio para el consumo de alimentos y/o sala de estar.	T12
	V3	Abastecimiento de energía eléctrica alterno no existe.	T13
	V4	Carece de abastecimiento de aire acondicionado, y/o aire de precisión para la sala de servidores, produce sobrecalentamiento del	T14

		ambiente de componentes y equipos.	
	V5	Mantenimiento preventivo interno o correctivo de conexiones de energía, cajas térmicas y/o mediciones de corriente alterna.	T1-T4, T6-T9,
	V6	Edificación o instalaciones no apta para lograr con los objetivos del negocio, es una casa con espacio limitado para el uso de funcionarios, sin señalización y equipo en caso de algún evento de riesgo natural. (medio ambiente cómodo confiable)	T12
	V7	Prevención y detección contra incendio (equipo contra incendios, extintores caducados y no aptos para data center y demás instalaciones).	T1, T6, T59

"Se debe tener en cuenta que una vulnerabilidad no produce daño en el activo de información, debe existir una amenaza para explotarla".

En otras palabras, para la identificación de vulnerabilidades es la fase del proceso de gestión de riesgos en que se puede detectar las anomalías, errores, es decir; las vulnerabilidades son deficiencias de construcción o errores en el diseño, elaboración de un producto o servicio, o de un sistema.

2.3.2.4 DETERMINACIÓN DEL RIESGO

Para determinar una adecuada gestión de riesgos se debe conocer los siguientes términos:

Riesgo. - Es la probabilidad de sufrir un daño, una perdida, un impacto negativo como consecuencia de la existencia de un peligro o amenaza.

Impacto. - De acuerdo a la ***Cláusula 3.1 de la Norma Técnica ISO 27005***, es un cambio adverso importante en el nivel de los objetivos de negocios logrados.

Ejemplos de Impacto sobre la Confidencialidad.

- Invasión de la privacidad de los usuarios o clientes.
- Fugas de información confidencial.

Ejemplos de Impacto sobre la Integridad.

- Cambio accidental de los sistemas o configuraciones.
- Resultados incorrectos y/o incompletos.
- Perdida de datos.

Ejemplos de Impacto sobre la Disponibilidad.

- Degradación del rendimiento.
- Interrupción o denegación de Servicio.
- Interrupción de las operaciones.

Probabilidad. - Es el atributo que hace referencia a la posibilidad de que un riesgo se materialice, es decir, mientras un activo de información posee más vulnerabilidades, la probabilidad de ocurrencia es mayor.

Los requerimientos de seguridad se identifican mediante la evaluación de riesgos de seguridad, esto ayudará a guiar y determinar la acción de gestión apropiada para implementar controles para proteger los activos de información.

De acuerdo a la **Cláusula 2.61**, ISO 27000, El **Riesgo para la Seguridad de la Información**. - es la potencialidad de que una amenaza explote una vulnerabilidad, con el fin de causar daño a un activo o grupo de activos, es decir que el riesgo es la medida del daño probable de una amenaza sobre un activo.

El riesgo varía de acuerdo al impacto y la probabilidad, estos definen una gama de zonas de colores tal como se muestra en la siguiente figura:

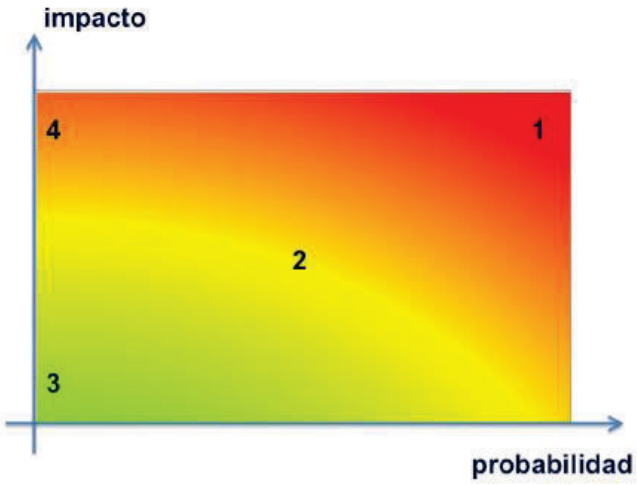


Figura N.- 2.3-1 Riesgo en función del impacto y la probabilidad

Fuente: Magerit Libro I, página 49.

De acuerdo a la Imagen anterior se especifica lo siguiente:

- **Zona** 1: franja roja, muestra riesgos muy probables y de alto impacto.
- **Zona 2**: franja amarilla, muestra riesgos improbables y de impacto medio.
- **Zona 3**: franja verde, muestra riesgos improbables y de bajo impacto.
- **Zona 4**: franja anaranjada, muestra riesgos improbables, pero de alto impacto.

2.3.2.5 VALORACIÓN DEL IMPACTO

El valor del impacto está relacionado con el valor y la importancia de los activos que pueden ser afectados por un incidente. El impacto causado puede afectar en uno o más activos o únicamente en parte del activo, por tanto, es importante definir el valor del activo y el valor del impacto resultante de un incidente.

La valoración del impacto para este proyecto se muestra en la **Tabla N.-2.3-13**.

TABLA N.- 2.3-13 VALORACIÓN DEL IMPACTO

FUENTE: OBJETIVO GUBERNAMENTAL DE AUDITORÍA AÑOS 2011 A 2014. PROCESO DE GESTIÓN DE RIESGOS [23, P. 61]

IMPACTO		DESCRIPCIÓN
Muy Bajo	**1**	Riesgo cuya materialización no genera pérdidas financieras $ ni compromete de ninguna forma la imagen pública de la institución y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos.
Bajo	**2**	Riesgo cuya materialización puede generar pérdidas financieras $ que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la institución y del Gobierno. Su materialización causaría un bajo daño en del desarrollo del proceso y no afectaría el cumplimiento de los objetivos.
Medio	**3**	Riesgo cuya materialización puede generar pérdidas financieras $ que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la institución y del Gobierno. Su materialización causaría un deterioro en del desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente de forma normal.
Alta	**4**	Riesgo cuya materialización puede generar pérdidas financieras $ que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la institución y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal.

Muy alto	**5**	Riesgo cuya materialización puede generar pérdidas financieras $ que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la institución y del Gobierno. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren.

2.3.2.6 VALORACIÓN DE LA PROBABILIDAD

La probabilidad es la posibilidad de que un incidente de seguridad de la información ocurra y la facilidad de explotación de la vulnerabilidad.

La valoración de la probabilidad de este proyecto se muestra en la **Tabla N.-2.3-14**:

TABLA N.- 2.3-14 VALORACIÓN DE LA FRECUENCIA O PROBABILIDAD

FUENTE: OBJETIVO GUBERNAMENTAL DE AUDITORÍA AÑOS 2011 A 2014. PROCESO DE GESTIÓN DE RIESGOS [23, P. 61]

FRECUENCIA / PROBABILIDAD	NIVEL NUMÉRICO	DESCRIPCIÓN
Casi Certeza	**5**	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente (90%-100%)
Probable	**4**	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad.
Moderado	**3**	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad.

Improbable	**2**	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 11% a 30% de seguridad.
Muy Improbable	**1**	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 1% a 10% de seguridad.

2.3.2.7 VALORACIÓN DEL RIESGO PARA LOS ACTIVOS DEL PROCESO DEL SNNA

La actividad de valoración de riesgos implica la identificación de los activos, la valoración de las vulnerabilidades y amenazas relacionadas a los activos, valoración del impacto y la probabilidad de ocurrencia. Los resultados de estas actividades se utilizan para evaluar riesgos y posteriormente definir un tratamiento.

La fórmula para calcular el riesgo es la siguiente:

$$\boldsymbol{RIESGO = VALOR\ DEL\ ACTIVO \times FACTOR\ DE\ EXPOSICIÓN} \qquad [\boldsymbol{Ec.2}]$$

En esta fase se evalúan los controles existentes, si están documentados, si son efectivos, para luego ser comparados en la etapa de identificación y análisis de los riesgos.

El cálculo de los intervalos se lo realizó mediante porcentajes, que definen el riesgo que corresponde, los valores de riesgo bajo son aquellos que se van aceptar, por tanto, lo que corresponde del riesgo máximo: valor del activo multiplicado por el FE (Impacto X Probabilidad) "$\boldsymbol{15x(5x5) = 375}$"; de éste valor se tomará el 10% y se lo considerará como riesgo bajo; se toma como intervalo del riesgo 1 a 37, y así sucesivamente. Para mejorar el entendimiento se lo muestra en la **Tabla N.- 2.3-15.**

TABLA N.- 2.3-15 CÁLCULO DEL RIESGO

FUENTE: AUTORES

PORCENTAJE %	INTERVALOS	DESCRIPCIÓN DEL RIESGO
10%	1 a 37	BAJO
20%	38 a 74	MEDIO
30%	75 a 111	ALTO
40%	112 a 375	CRÍTICO
100%	**TOTAL**	

La metodología de evaluación de riesgos se define de acuerdo al valor del activo (**VA)** por el factor de exposición (**FE),** en la **Tabla N.- 2.3-16**, se muestra los intervalos de valores para la evaluación del riesgo; mediante el método cuantitativo:

TABLA N.- 2.3-16 MATRIZ DEL RIESGO

FUENTE: AUTORES

	FE			
VA	1-37	1-37	1-37	38-74
	1-37	38-74	38-74	75-111
	1-37	38-74	75-111	75-111
	38-74	75-111	75-111	112 a 375

Si el resultado del este cálculo no está dentro de los parámetros aceptables, es decir que el resultado este dentro del cuadrante rojo de la matriz, el riesgo debe ser tratado mediante controles, los cuales están descritos en el Anexo A de la Norma Técnica ISO/IEC 27001 o en el Anexo del Acuerdo 166.

Definir un rango de valores de riesgo ayuda a la institución a la toma de decisiones, determinando los riesgos a tratar y la prioridad para la implementación del tratamiento.

TABLA N.- 2.3-17 DESRIPCIÓN DE LOS INTERVALOS

FUENTE: OBJETIVO GUBERNAMENTAL DE AUDITORÍA AÑOS 2011 A 2014. PROCESO DE GESTIÓN DE RIESGOS [23, P. 65], [24]

RANGO MÍNIMO	RANGO MÁXIMO	NIVEL DE RIESGO	DESCRIPCIÓN
1	37	Riesgo Bajo	La Institución Acepta el Riesgo.
38	74	Riesgo Medio	La Institución podría aceptar o No temporalmente este nivel de Riesgo, puede tener un impacto menor. Requiere atención a mediano plazo.
75	111	Riesgo Alto	La Institución NO acepta este nivel de Riesgo, puede tener un impacto significativo. Requiere una atención a corto plazo.
112	375	Riesgo Crítico	La Institución NO acepta este nivel de Riesgo, va a tener un impacto muy serio. Requiere atención inmediata.

En la siguiente tabla se muestran los factores que son necesarios para realizar el cálculo de riesgo, la tabla completa se encuentra en el ANEXO B “Tratamiento de riesgos SNNA”.

TABLA N.- 2.3-18 MATRIZ PARA EL CÁLCULO DEL RIESGO

FUENTE: ANEXO E TABLA E2. ISO/IEC 27005, PÁG 61

Activos						Factor de Exposición			RIESGO		
Código de Activo	**Activo**	**Valor de Activo (VA)**	**Código de la Vulnerabilidad**	**DESCRIPCIÓN DE LA VULNERABILIDAD**	**CÓDIGO DE LA AMENAZA**	**IMPACTO**	**PROBABILIDAD**	**Valor del Factor de Exposición (FE)**	**Cálculo del Riesgo (R) R=(VA*FE)**	**Nivel del riesgo**	**Opciones de tratamiento del riesgo**
A1	Plataforma (adminsiniv)	15	**V36**	Mantenimiento y seguimiento y compatibilidad de funcionamiento (sea por cambios, actualizaciones, parches, etc.)	T8, T9,T10, T16,T21,T22,T32, T33, T34,T35,T55,T57,T71	5	3	15	**225**	**Riesgo Crítico**	1. Elección de controles
A1	Plataforma (adminsiniv)	15	**V37**	Interface de usuario compleja	T18,T29,T46	2	2	4	**60**	**Riesgo Medio**	1. Elección de controles

A1	Plataforma (adminsiniv)	15	**V38**	Control de Acceso (Restricciones en el acceso al software y mecanismos de autenticación para el uso, actualización, o visualización de la información respecto a los usuarios establecido).	T18, T19, T27, T29,T38, T39,T50, T52, T55, T57, T70,T74	5	2	10	**150**	**Riesgo Crítico**	1. Elección de controles
A1	Plataforma (adminsiniv)	15	**V42**	Uso, fortaleza, complejidad, calidad y gestión de contraseñas de acceso al software	T27, T38, T39, T64.	5	2	10	**150**	**Riesgo Crítico**	1. Elección de controles
A1	Plataforma (adminsiniv)	15	**V43**	Tiempo de inactividad y tiempo de conexión de las sesiones	T27, T32,T39,	3	2	6	**90**	**Riesgo Alto**	1. Elección de controles
A1	Plataforma (adminsiniv)	15	**V45**	Encriptación por parte del software (encriptación de la aplicación o del motor de base de datos), gestión de las llaves de cifrado	T27,T54, T55, T56, T58, T70, T79	5	2	10	**150**	**Riesgo Crítico**	1. Elección de controles
A1	Plataforma (adminsiniv)	15	**V46**	Mecanismos de Monitoreo (ping, tracert, http,icmp)	T27, T38, T39, T49, T72.	4	2	8	**120**	**Riesgo Crítico**	1. Elección de controles

2.4 TRATAMIENTO DEL RIESGO DE ACUERDO A LA NORMA TÉCNICA ISO/IEC 27005

El análisis de riesgos permite llegar a conclusiones con fundamento y proceder a la fase de tratamiento.es decir; se puede determinar cuáles son los activos deben ser protegidos mediante un tratamiento de riesgos. [21]

El tratamiento de riesgo se lo realiza mediante la selección y la implementación de una o varias opciones/controles para modificar el riesgo como se muestra en la siguiente figura:

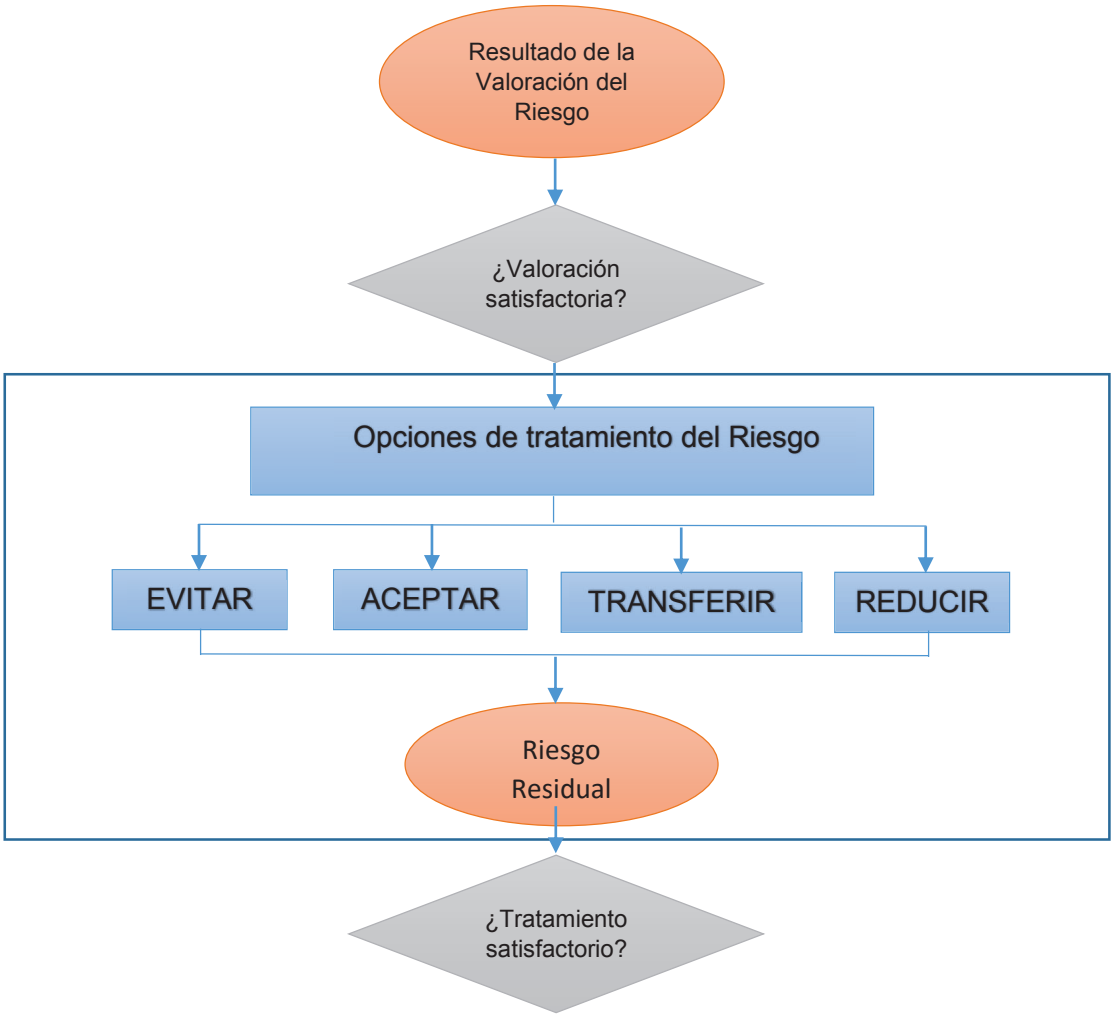


Figura N.- 2.4-1: Actividades del tratamiento de riesgo.

Fuente: ISO/IEC 27005 [24]

El tratamiento de riesgo es un proceso cíclico de:

- Evaluación.
- Decidir si los niveles de riesgos son tolerables.
- Si no son tolerables, generar un nuevo tratamiento del riesgo; y
- Evaluar la eficiencia de ese tratamiento.

2.4.1 OPCIONES DE TRATAMIENTO DE RIESGOS SEGÚN LA NORMA ISO/IEC 27005

Las opciones de tratamiento de riesgo deben ser seleccionadas en base a los resultados obtenidos en la evaluación, el coste esperado de la aplicación y los beneficios esperados.
El nivel de riesgo relativamente se puede reducir al nivel más bajo, pero al mismo tiempo puede existir otras opciones de mejora siendo estas rentables o no, para ello se debe establecer y decidir en pleno juicio con su debida justificación.

El tratamiento de riesgos debe permitir la gestión de riesgos de acuerdo a las siguientes opciones:

- Mitigar el riesgo

El nivel de riesgo puede ser administrado mediante la selección o modificación de controles de modo que le riesgo residual dé como resultado un riesgo aceptable.

- Aceptar el riesgo

Es posible que haya ciertos riesgos cuyos controles la organización no será capaz de identificarlos o que el costo de estos controles sea mayor al riesgo, en este caso se puede considerar su aceptación, por lo tanto, no es necesario implementar controles adicionales y el riesgo se puede retener.

- Evitar el riesgo

Cuando los riesgos identificados se consideran demasiado altos, o los costes de la aplicación de otras opciones de tratamiento se exceden los beneficios, se puede tomar una decisión para evitar riesgos por completo.

- Transferir el riesgo

Implica la decisión de transferir determinados riesgos a partes externas. La transferencia se puede hacer mediante subcontratación cuya función es monitorear el sistema de información y tomar acciones inmediatas para detener un ataque antes de que éste produzca y cause daño a la organización.
Cuando los riesgos de Acuerdo a Norma Técnica Colombiana NTC 5254 Gestión del Riesgo ***Clausula 4.5.1 literal d***.- Cuando se ha transferido los riesgos en forma parcial o total, la Organización ha adquirido un nuevo riesgo, debido a que la organización a la cual se le ha transferido el riesgo no pueda manejarlo en forma efectiva. [20, p. 17]

Opciones de tratamiento de riesgo.

De acuerdo con las opciones de tratamiento de riesgos se define la siguiente tabla:

TABLA N.- 2.4-1 OPCIONES PARA EL TRATAMIENTO DE RIESGO.

1. Elección de controles
2. Transferencia de riesgos a terceros
3. Evitar el riesgo
4. Aceptación de riesgo

Con el fin de minimizar los riesgos se toman controles o se acepta el riesgo debido a las imposiciones del SNAP como ente regulador y las decisiones tomadas por la Alta dirección

Los controles pueden ser preventivos o correctivos.

Control preventivo. - es aquel que actual para eliminar la causa del riesgo para prevenir su ocurrencia o se materialice.

Control correctivo. - es aquel permite reestablecer la actividad después de haberse detectado un evento de seguridad.

Un control se entiende por implementado una vez que ha sido:

- Documentado, firmado y aprobado
- Publicado dentro de la Institución
- El personal ha sido capacitado.
- Implementadas las medidas técnicas físicas u operativas que estén sujetas o soporten a lo que dice el documento.

El plan de tratamiento de riesgos, debe ser generado en base a planes de acción puntuales con todos los involucrados, se debe considera que son planes a corto plazo con entregables que deben ser revisados por el Oficial de Seguridad y Aprobados por el Comité de Seguridad de la Información.

2.4.2 PASO 3: SALVAGUARDAS / CONTRAMEDIDAS

Las salvaguardas o contramedidas constituyen procedimientos o mecanismos tecnológicos que reducen el riesgo.

Para el desarrollo de esta sección se requiere el uso del ANEXO A de la norma ISO/IEC 27001, Acuerdo Ministerial 166, de acuerdo al activo y la vulnerabilidad relacionada, se establece el control respectivo.

Los objetivos de control y los controles sirven de guía para implementar medidas de seguridad, por ello la selección de los controles se realiza en función de los resultados obtenidos en la evaluación de riesgos y el grado de implementación de cada control se lo realizará de acuerdo a las necesidades identificadas y los recursos provistos por la organización, el objetivo debe equilibrarse entre la seguridad y el coste que este conlleva. De acuerdo a la matriz una vez calculado el riesgo se escogerá una opción de acuerdo como se muestra en la **Tabla N.- 2.4-2.**

TABLA N.- 2.4-2 MATRIZ DE RIESGOS Y CONTROLES

VALORES ANTES DEL TRATAMIENTO						TRATAMIENTO DEL RIESGO	
Código del Activo	**Valor del Activo (VA)**	**Código de la Vulnerabilida**	**Valor del Factor de Exposición (FE)**	**Cálculo del Riesgo (R) R=(VA*FE)**	**Nivel del riesgo**	**Elección de opciones**	**Controles a implementar**
A1	15	V36	15	225	Riesgo Crítico	1. Elección de controles	A.14.2.2 Procedimientos para control en cambio de sistema A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma operativa. A.14.2.9 Prueba de aceptación del sistema
A1	15	V37	4	60	Riesgo Medio	1. Elección de controles	A.12.4.1 Registro de eventos
A1	15	V38	10	150	Riesgo Crítico	1. Elección de controles	A.9.1.1 Política de control de acceso A.9.2 Gestión de acceso a usuarios A.9.2.1 Registración y baja de usuarios A.9.2.2 Concesión de acceso de usuarios A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso del usuario A.9.2.6 Eliminación o ajuste de derechos de acceso
A1	15	V42	10	150	Riesgo Crítico	1. Elección de controles	A.9.4.3 Sistema de gestión de contraseñas A.10.1.1 Política del uso de controles criptográficos

A1	15	V43	6	90	Riesgo Alto	1. Elección de controles	A.9.1.1 Política de control de acceso
A1	15	V45	10	150	Riesgo Crítico	1. Elección de controles	A.10.1.1 Política del uso de controles criptográficos A.10.1.2 Gestión de las claves A.14.1.1 Análisis y especificación de los requerimientos de seguridad de la información A.14.1.2 Seguridad de servicios de aplicación en redes públicas A.14.1.3 Protección de transacciones de servicios de aplicaciones

Una vez tomada la decisión de acerca de la opción de tratamiento que se le dará a los riesgos, todas las actividades se deben formalizar en un Plan de Tratamiento de Riesgos. Eso significa que controles del Anexo A de la Norma ISO 27001 conjuntamente con el Acuerdo 166 van a ser implementados, se establece la persona responsable, fechas establecidas; con el fin de obtener y cumplir con el compromiso para la entrega.

El Plan de Tratamiento de Riesgos es la salida de todo proceso de gestión de riesgos, de tal manera que se debe seleccionar los controles más apropiados para reducir los riesgos que no estén en el margen de aceptación.

Las opciones de tratamiento de riesgo deben ser seleccionadas en base a resultados de la valoración de riesgo, el coste esperado de la implementación y los beneficios esperados de las opciones.

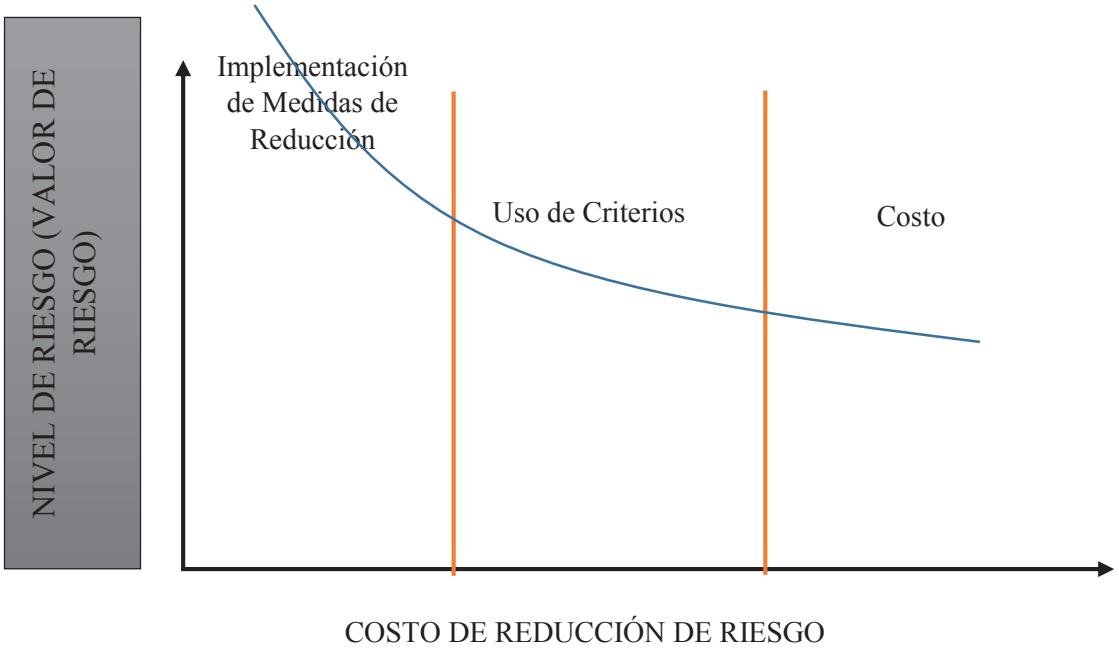


Figura N.- 2.4-2 Costos de las medidas de reducción de riesgo.

Fuente: NTC Gestión de riesgo, Cláusula 4.5.2 pág. 18

La selección de la opción para el tratamiento de riesgo es apropiada e incluye un equilibrio de costo de la implementación, deben estos ser proporcionales a los beneficios obtenidos.

Se debe tener en cuenta que un control no siempre genera los resultados esperados, por lo que se sugiere cambios y las buenas prácticas encontradas documentarlas, evaluar los cambios y así conseguir que los controles escogidos sean correctos.

2.4.3 PASO 4: IMPACTO RESIDUAL

El impacto residual es el resultado de un conjunto de salvaguardas desplegadas al impacto potencial. Para su valoración se repiten los cálculos de impacto con salvaguardas hasta que el nivel de impacto sea insignificante.

2.4.4 PASO 5: RIESGO RESIDUAL

Una vez que se haya definido e implementado el plan de tratamiento de riesgos como resultado se obtiene riesgos residuales, esto implica que se deber realizar una nueva iteración para valorar el riesgo. Si el riesgo residual no satisface los criterios de aceptación se recomienda realizar un análisis costo-beneficio, y a su vez establecer los controles y determinar si son aplicables.

Los controles se utilizan para garantizar que el comportamiento de los procesos de negocio se realice de forma segura para el intercambio de información.

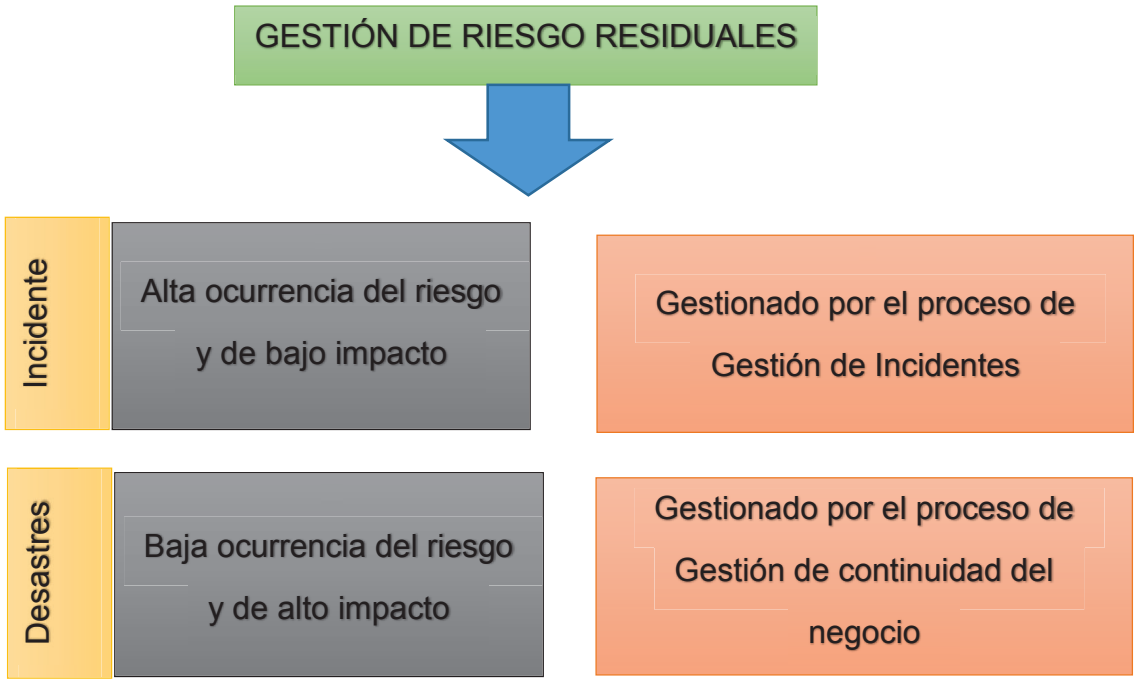


Figura N.- 2.4-3 Gestión de riesgos residuales

Fuente Autores.

Se debe tener en cuenta que el riesgo residual no desaparece, aquellos con alta incidencia y de bajo impacto son gestionados por el proceso de gestión de incidentes.

Los riesgos de baja incidencia y alto impacto conocidos como o desastres ocurridos en el core del negocio, son tomados en cuenta para generar planes de continuidad de operación. (PLAN DE CONTINUIDAD DEL NEGOCIO).

NOTA: El punto 2.4.3 y 2.4.4 no contempla dentro del proyecto de titulación

2.5 TIPOS DE POLITICAS

Una **política** según la norma **ISO/IEC 27000, cláusula 2.51**, define como "la intención y orientación general, tal como han sido expresadas formalmente por la Dirección"; es decir, es una declaración de intenciones que cubre la seguridad de la información, proporcionando las bases necesarias para definir y delimitar responsabilidades sean estas técnicas u organizativas.

La política en una empresa constituye una guía donde se define el comportamiento aceptable del personal dentro de la institución.

Dentro de una institución pueden existir varias políticas, de acuerdo a las áreas/departamentos de actividad importantes o críticos, además, las políticas están establecidas por un orden jerárquico y pueden ser independientes o dependientes entre sí.

Por lo general, las políticas se clasifican dentro de tres niveles de orden jerárquico, como se muestra en la **Figura N.- 2.5-1**.

Figura N.- 2.5-1 Tipos de políticas de seguridad de la información

Fuente: Anexo D ISO 27003 [25]

Niveles de políticas dentro de una organización:

- **Políticas generales de alto nivel**

Son una guía de trabajo general, donde se definen los objetivos de seguridad para garantizar la continuidad del negocio y limitar o evitar el daño en los activos.

- **Políticas de alto nivel relacionadas con un tema específico**

Son un subconjunto subordinado de las políticas generales de alto nivel, que están relacionadas un área específica.

- **Políticas detalladas**

Son políticas que apoyan a las políticas de alto nivel para temas específicos, permiten especificar los requisitos de la seguridad interior.

2.5.1 ESTRUCTURA DE UNA POLÍTICA

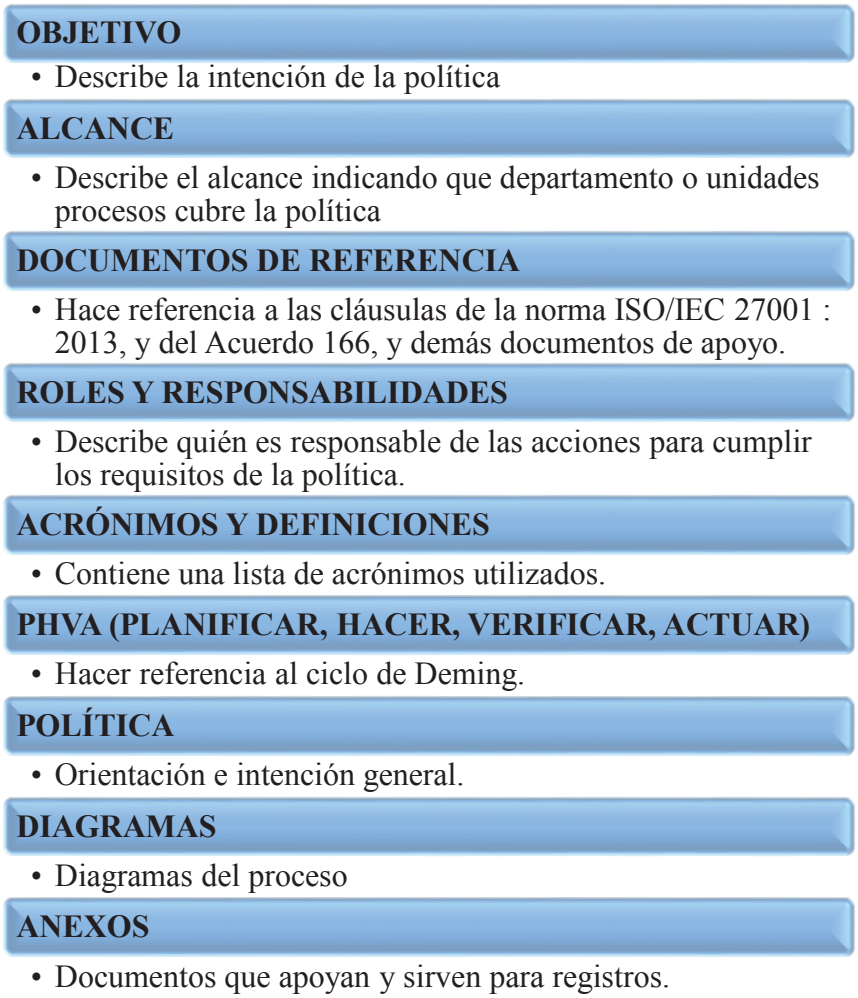


Figura N.- 2.5-2 Estructura de la Política de seguridad de la Información

Fuente: Autores

Las políticas de Seguridad de la Información deben ser específicas, aprobadas por la dirección y revisadas por el Comité de seguridad, es decir pasan por un proceso de aprobación para trabajar conjuntamente con el departamento de Talento Humano para

realizar planes educación concientización y formación apoyados con el departamento de Comunicación para la publicación y difusión por medio de boletines, videos, etc.

2.5.2 EJEMPLO DE POLÍTICA

La portada la política debe contener:

SNNA Sistema Nacional de Nivelación y Admisión	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSI-SNNA-PRRRI Versión: 01 Fecha última revisión: 19/12/2015

- Logo de la institución
- Título
- Formato de etiquetado.
- Tabla de Autores y aprobaciones.
- Nota de confidencialidad

POLÍTICA DE RESPALDO RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN

Realizado por:	Revisado por:	Autorizado por:	Aprobado por:
Fernando Gualotuña			

NOTA DE CONFIDENCIALIDAD

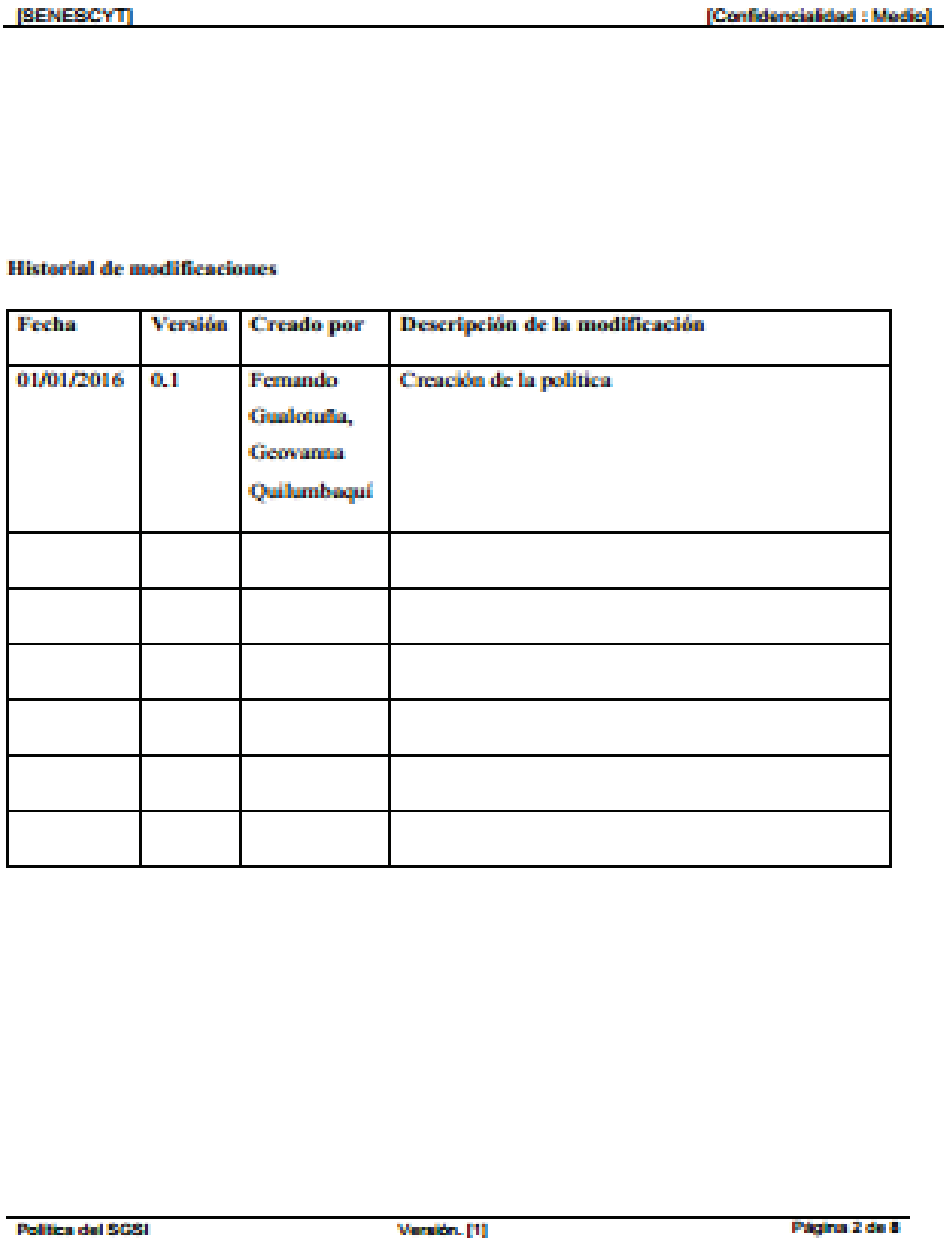
Este documento es propiedad exclusiva de la SENESCYT, queda prohibido la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte del Comité de Seguridad de la Información, su uso y distribución está autorizado para ser comunicado al interior de la Institución, y por parte del personal debidamente autorizado.

Figura N.- 2.5-3 Portada de una política de Seguridad de la Información.

Fuente: Autores

Encabezados y pie de página, en la que se especifica el nombre de la Institución y el nivel de confidencialidad

Historial de modificaciones, con fechas, versiones en orden creciente, el responsable y descripciones.



[SENESCYT] [Confidencialidad : Medio]

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
01/01/2016	0.1	Fernando Gualotuña, Geovanna Quilumbaquí	Creación de la política

Política del SGSI Versión. [1] Página 2 de 8

Figura N.- 2.5-4 Historial de modificaciones de la política

Fuente: Autores

Tabla de contenidos y su respectivo desarrollo se muestra en la **Figura N.-2.4.5**

CONTENIDO

Figura N.- 2.5-5 Desarrollo de la Política de acuerdo a la estructura

Fuente: Autores

Políticas se encuentran en el Anexo C.

La política de seguridad es un documento que debe ser actualizado, revisado y modificado cuando existan incidentes de seguridad, después de una auditoria o cuando existan cambios esenciales en el/los proceso.

2.6 CLAÚSULAS PRIORITARIOS SEGÚN EL ACUERDO 166

Clausulas marcadas * en el acuerdo 166, son consideradas como prioritarias, pero eso no significa que todas las instituciones públicas que deben cumplir con dicho acuerdo, lo hagan al 100% como lo se muestra en la **Figura N.-2.6-1**

1	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**
1.1	***Documento de la Política de la Seguridad de la Información***
a)	Disponer la implementación del EGSI en la institución por la máxima autoridad.
b)	Difundir la política de seguridad de la información de referencia o propia de la institución.
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
2.1	***Compromiso de la máxima autoridad de la institución con la seguridad de la información***
a)	Realizar el seguimiento de la puesta en marcha de las normas de este documento
b)	Disponer la difusión, capacitación y sensibilización del contenido de este documento
c)	Conformar oficialmente el Comité de Gestión de la Seguridad de la Información de la institución y designar a los integrantes.
2.2	Coordinación de la Gestión de la Seguridad de la Información
a)	La coordinación estará a cargo del Comité de Gestión de Seguridad de la Información el cual tendrá las siguientes funciones:
	Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del CSI.
	Designar formalmente al responsable de seguridad del área de Tecnologías de la Información.
2.5	***Acuerdos sobre Confidencialidad***
a)	Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI
b)	Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción

Figura N.- 2.6-1 Descripción de las Cláusulas Prioritarias separadas por dominios y objetivos de Control.

El documento completo se encuentra en el Anexo D.

2.7 REQUISITOS DOCUMENTALES DE ACUERDO A LA NORMA ISO/IEC 27001:2013 CONJUNTAMENTE CON EL ACUERDO MINISTERIAL 166

Para el desarrollo del SGSI los documentos mínimos requeridos son los que se muestran en la tabla N.-2.7-1, donde se especifica el documento y las cláusulas del Acuerdo 166 correspondiente, para verificación y constatación de hechos se define el anexo correspondiente al documento.

TABLA N.- 2.7-1 DOCUMENTOS REQUERIDOS POR LA NORMA TÉCNICA ISO Y ENTREGABLES.

FUENTE: AUTORES.

Documentos Obligatorios	**ENTREGABLES Y JUSTIFICACIONES**
Alcance del SGSI (cláusula 4.3)	Se define en el los objetivos y alcance del proyecto de titulación
Información de la política y objetivos de seguridad (cláusulas 5.2 y 6.2)	NO APLICA
La evaluación de riesgos y la metodología de tratamiento de riesgos (cláusula 6.1.2)	Se especifica en la metodología escogida por los autores "MAGERIT" y anexo A 27001 y el EGSI
Declaración de aplicabilidad (cláusula 6.1.3 d)	No se aplica dentro del periodo de desarrollo porque no se implementa
Plan de tratamiento de riesgos (cláusulas 6.1.3 y 6.2 e)	Se especifica en la metodología escogida por los autores "MAGERIT" y anexo A 27001 y el EGSI
Informe de evaluación de riesgos (cláusula 8.2)	Se entrega la matriz de evaluación del riesgo

Definición de roles y responsabilidades de seguridad (cláusulas A.7.1.2 y A.13.2.4)	Se encuentra detallada en cada política de seguridad.
Inventario de activos (A.8.1.1 cláusula) EGSI cláusula 3.1 j),k),l),m),n),o),p),q),r),s),t),u),v),w),x),y)	Aplica y se encuentra en los anexo "Tratamiento-Gestión de activos"
El uso aceptable de los activos (A.8.1.3 cláusula) EGSI cláusula 3.3 d) 3.3.2, 3.3.3	PSI-SNNA-PURISR
Política de control de acceso (A.9.1.1 cláusula) EGSI cláusula	PSI-SNNA-PPEL
Los procedimientos operativos para la gestión de TI (A.12.1.1 cláusula)	NO APLICA
Principios de ingeniería de sistemas seguros (A.14.2.5 cláusula)	NO APLICA
La política de seguridad del proveedor (A.15.1.1 cláusula)	PSI-SNNA-PMDS
Procedimiento de gestión de Incidentes (A.16.1.5 cláusula) EGSI cláusulas 6 , 6.1, e),6.6, b), c) d) 9.1 a),c)	PSI-SNNA-PGIS
Procedimientos de continuidad de negocios (A.17.1.2 cláusula) EGSI cláusula 6.27, a), b), c),d)	PSI-SNNA-PMDS
Los requisitos legales, reglamentarios y contractuales (A.18.1.1 cláusula)	1.6 MARCO LEGAL Y JURÍDICO
Los registros de capacitación, habilidades, experiencia y cualificaciones (cláusula 7.2)	NO EXISTE REGISTRO, PERO SE LAS SUGIERE EN LAS POLÍTICAS
Programa de auditoría interna (cláusula 9.2)	NO APLICA
Los resultados de las auditorías internas (cláusula 9.2)	NO APLICA

Los resultados de la revisión por la dirección (cláusula 9.3)	NO APLICA
Los resultados de las acciones correctivas (cláusula 10.1)	NO APLICA
Registros de las actividades del usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3) EGSI cláusula 6.26 h), i) ,j) ,k)	PSI-SNNA-PGIS
DE ACUERDO AL ANEXO A NO INDISPENSABLES PERO CON MAYOR FRECUENCIA DE USO.	
Procedimiento de control de documentos (cláusula 7.5)	NO APLICA
Los controles para la gestión de documentos (cláusula 7.5)	NO APLICA
Procedimiento de auditoría interna (cláusula 9.2)	NO APLICA
Procedimiento para la acción correctiva (cláusula 10.1)	PSI-SNNA-PGIS
Traiga su propio dispositivo (BYOD) Política (A.6.2.1 cláusula)	PSI-SNNA-PURISR
Dispositivo móvil y la política de teletrabajo (A.6.2.1 cláusula)	PSI-SNNA-PURISR
Información de la política de clasificación (cláusulas A.8.2.1, A.8.2.2 y A.8.2.3)	PSI-SNNA-PCEI
Política de contraseñas (cláusulas A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 y A.9.4.3)	PSI-SNNA-PGUC
Eliminación y política de destrucción (cláusulas A.8.3.2 y A.11.2.7)	
Procedimientos para trabajar en áreas seguras (A.11.1.5 cláusula) EGSI cláusula : 5 , 5.1, b), 5.2, a) ,c),5.3,b),d),5.4, d),e) 5.5, d), 5.6 a), 5.7, c) 5.8, c) 5.9 e)	PSI-SNNA-PCAF

Política de escritorio y pantalla limpia (A.11.2.9 cláusula)	PSI-SNNA-PPEL
La política de gestión del cambio (cláusulas A.12.1.2 y A.14.2.4)	NO APLICA
La política de copia de seguridad (A.12.3.1 cláusula) EGSI cláusula 6.12 a), b) , c)	PSI-SNNA-PRRRI
Política de transferencia de la información (cláusulas A.13.2.1, A.13.2.2 y A.13.2.3)	NO APLICA
Análisis de impacto empresarial (A.17.1.1 cláusula)	NO APLICA SE DEJA A CARGO DE LA INSTITUCIÓN
Hacer ejercicio y probar el plan (A.17.1.3 cláusula)	NO APLICA SE DEJA A CARGO DE LA INSTITUCIÓN
Mantenimiento y plan de revisión (A.17.1.3 cláusula)	NO APLICA SE DEJA A CARGO DE LA INSTITUCIÓN
Estrategia de continuidad del negocio (A.17.2.1 cláusula)	NO APLICA SE DEJA A CARGO DE LA INSTITUCIÓN

2.8 ANÁLISIS DE COSTOS DE IMPLEMENTACIÓN

Para la implementación el análisis se toma en cuenta los Costes de Formación o Capacitación.

Costes por Ayuda externa (Consultora Externa).

Tecnología, Tiempo.

Equipo de Expertos.

			TIEMPO DE IMPLEMENTACIÓN		VALOR DE ADQUISICIÓN
CARGO	**GRUPO**	**REMUNERACIÓN MENSUAL UNIFICADA**	**6 meses**	**18 meses**	
Analista de Seguridad	SP6	$ 14.200,00	$ 85.200,00	$ 255.600,00	
Analista de Seguridad (Oficial de Seguridad)	SP5	$ 1.212,00	$ 7.272,00	$ 21.816,00	
Jefe de Unidad de TICS	SP9	$ 1.900,00	$ 11.400,00	$ 34.200,00	
Consultora	Asesor	$ 2.783,00	$ 16.698,00	$ 50.094,00	
Herramientas para pruebas de vulnerabilidades técnicas rapid 7					$ 5.000,00
Capacitaciones para realizar pruebas de pent test					$ 650,00
Curso de Implementador LIDER, por persona. PECB					$ 2.500,00
		SUBTOTAL	$120.570,00	$ 361.710,00	$ 8.150,00
		TOTAL	**$128.720,00**	**$ 369.860,00**	

CONCLUSIONES Y RECOMENDACIONES

3.1. CONCLUSIONES

- De acuerdo a los requerimientos dispuesto por el SNNA, el alcance del proyecto abarcó hasta el proceso de Análisis y Gestión del Riesgo, el mismo que servirá de base para que la SENESCYT continúe con el proceso del SGSI en una segunda fase se implementará los controles, se difundirá las políticas, se dará capacitaciones a todos los funcionarios.

- En base a una comparación de metodologías se escogió Magerit, para el análisis y gestión del riesgo, debido a que; ésta se enfoca en la seguridad de la información, la misma que relaciona procesos, personas y TIC´s; además nos muestra su proceso por etapas y actividades generalizadas en 5 pasos para su implementación.

- Para conocer la situación actual de la Institución; se utilizó preguntas de auditoria, estas fueron realizadas a los funcionarios del proceso de Nivelación y Admisión (dueños del proceso); al evaluar la seguridad se determinó que el nivel de cumplimiento conforme a la Norma ISO/IEC 27002 fue bajo, se evidenció buenas prácticas, y los procedimientos e incidentes de seguridad no ha sido documentados.

- Para realizar el levantamiento de activos, se utilizó lenguaje común durante las entrevistas realizadas a los funcionarios dueños del proceso; no sobrepasando los 25 minutos por reunión, en equipos de grupo de trabajo que intervienen en cada tarea del proceso del SNNA, en el cual en su relato expresaban incidentes de seguridad, y las buenas prácticas que suelen hacer, en algunos casos no tenía conocimiento sobre los riesgos que poseen al manejar, crear, transportar o difundir la información institucional sin autorización.

- La SENESCYT es una institución pública y los sistemas de información / aplicaciones se encuentran en producción; por lo tanto, no se pudo realizar pruebas de penetración y testeo para identificar las vulnerabilidades técnicas.

3.2. RECOMENDACIONES

- Al momento de realizar las entrevistas; puede hacer uso del lenguaje común e ingeniería social, manteniendo una interacción mutua entre entrevistado e entrevistador, con el fin de obtener mayor información.

- Se sugiere que el consolidado de activos de información sean los más relevantes e importantes que intervienen en el proceso; agrupándolos como un todo y no por partes, establecer un enfoque global; Ejemplo: El sistema ABC; con el fin de reducir el tamaño de la matriz de riesgos, de tal manera que ésta sea entendible y facilite la valoración del riesgo.

- Para tener una mejor gestión de la seguridad de la información, se sugiere que los controles y políticas; sean aprobadas y revisadas periódicamente por el oficial de seguridad y el comité, especialmente cuando existe cambios significativos, con el fin de establecer acciones para asegurar la continuidad y misión del proceso.

- Las políticas de seguridad definidas y aprobadas se sugieren socializarlas a todos los funcionarios de la institución, para que sean conscientes de sus sanciones, deberes y al mismo tiempo contribuyan con la seguridad de la información y tengan conocimiento de la amenazas las cuales estén expuestos.

- Se sugiere contratar una empresa consultora especializa en seguridad informática para que realice pruebas de penetración y testeo; con el fin de detectar las vulnerabilidades técnicas de los sistemas y/o aplicaciones.

- Conformar un grupo de auditoria interna, con el fin de medir cuan efectivos son los controles implementados, estableciendo métricas medibles, documentar los cambios durante todo el proceso de implementación del SGSI.

REFERENCIA BIBLIOGRÁFICAS

[1] SNIESE, «educacionsuperior,» 2015. [En línea]. Available: https://infoeducacionsuperior.gob.ec/#/que-es-sniese. [Último acceso: 03 07 2015].

[2] S. SENESCYT, «snna.gob.ec,» [En línea]. Available: http://www.snna.gob.ec/wp-content/themes/institucion/snna_menu.php. [Último acceso: 08 07 2015].

[3] C. T. e. I. Secretaría de Educación Superior, «Biblioteca: Reglamento,» 05 Febrero 2014. [En línea]. Available: http://www.snna.gob.ec/dw-pages/Descargas/NUEVO_REGLAMENTO_SNNA.pdf. [Último acceso: 05 07 2015].

[4] A. López Neira y J. Ruiz Spohr, «El portal de ISO 27001 en Español,» [En línea]. Available: http://www.iso27000.es/iso27000.html. [Último acceso: 05 07 2015].

[5] ISO/IEC, *Norma Internacional ISO/IEC 27000,* Tercera ed., 2014, p. 38.

[6] SNAP, *Acuerdo 166,* Quito, Pichincha, 2013, pp. 3-50.

[7] SNAP, «Curso : Gestíon de la Seguridad de la Información Fase II,» Quito, 2015.

[8] PECB, ISO 27001 Lead Implementer Official Course, E. Lanchapelle, Ed., Quito, Pichincha, 2015.

[9] B. f. Sicherheit, «BSI-Standar 100-1,» Godesberger Allee, 2008.

[10] ISO/IEC, «Consolidated ISO Supplement-Procedure specific to ISO,» 2015.

[11] A. Richard, S. James, Y. Lisa y W. Wiliam, Introducing OCTAVE Allegro: Improving the Information Security Risk, EEUU: Carnegie Mellow University, Mayo 2007.

[12] R. Caralli, J. Stevens, L. Young y W. Wilson, *Introducing OCTAVE Allegro,* Carnegie Mellon University ed., 2007, p. 154.

[13] G. Stoneburner, A. Goguen y A. Feringa, «csrc.nist.gov,» Natl. Inst. Stand. Technol. Spec. Publ. 800-30, 54 pages (July 2002), Julio 2002. [En línea]. Available:

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. [Último acceso: 05 Julio 2015].

[14] M. Amutio, «MAGERIT libro 1 versión3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» de *MAGERIT libro 1 versión3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I-Método*, G. B. Jesús, Ed., Madrid, Ministerio de Hacienda y Administraciones Públicas, Octubre,2012, p. 127.

[15] ENISA, «European Union Agency for Network and Information Security,» [En línea]. Available: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/comparison/comparison.html. [Último acceso: 6 Febrero 2016].

[16] K. Dejan y L. Rhand, «advisera.com,» 2016. [En línea]. Available: http://advisera.com/27001academy/es/que-es-iso-27001/ . [Último acceso: 20 Enero 2016].

[17] PAe, «Magerit Libro III Metodología de Análisis y gestión de Riesgos de los Sistemas de Información;,» Madrid, 2012.

[18] Halkyn,Consulting, Ltd;, «Specialist Security & Risk Management Consultants,» 2013.

[19] ISECT, «iso27001security,» 2016. [En línea]. Available: www.iso27001security.com/ISO27k. [Último acceso: 2015].

[20] INCOTEC, «Norma Técnica Colombiana NTC 5254 Gestión del Riesgo,» Bogotá, 2004.

[21] G. Amutio, J. Candau y J. Mañas, *Libro I - Método,* J. G. Barroso, Ed., Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012, p. 127.

[22] S. Harris, CISSP Examen Guide, Mc Graw Hill, 2013, p. 26.

[23] C. Gobierno, «Objetivo Gubernamental de Auditoría Años 2011 a 2014. Proceso de Gestión de Riesgos,» 2011.

[24] ISO/IEC, *Norma Técnica Colombiana NTC-ISO/IEC 27005,* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación, 2009, p. 74.

[25] 2. ISO/IEC, «Information Technology -Security techniques-Information security management system imolementation guidance,» Switzerland, 2010.

[26] K. Gaona, «Aplicación de la Metodología Magerit para el análisis y gestión de Riesgos de la Seguridad de la Información aplicado a la empresa pesquera Bravito S.A.,» Octubre 2013. [En línea]. Available: http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

[27] G. Stoneburner, A. Goguen y A. Feringa, «nist.gov,» Julio 2002. [En línea]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. [Último acceso: 05 Julio 2015].