ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS INFORMÁTICOS Y DE LA COMPUTACIÓN

DISEÑO DEL PLAN DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL SERVIDOR QUIPUX DE LA DIRECCIÓN DE GESTIÓN DE LA INFORMACIÓN Y PROCESOS DE LA ESCUELA POLITÉCNICA NACIONAL

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

EDGAR OMAR SÁNCHEZ RUIZ

edgar.sanchez@epn.edu.ec

OSCAR OMAR TENORIO BRAVO

oscar.tenorio@est.epn.edu.ec

DIRECTOR: Ing. MSc. DENYS ALBERTO FLORES ARMAS

denys.flores@epn.edu.ec

Quito, Junio 2015

DECLARACIÓN

Nosotros, Edgar Omar Sánchez Ruiz y Oscar Omar Tenorio Bravo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Edgar Omar Sánchez Ruiz

Oscar Omar Tenorio Bravo

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Edgar Omar Sánchez Ruiz y Oscar Omar Tenorio Bravo, bajo mi supervisión.

Ing. MSc. Denys Alberto Flores Armas

DIRECTOR

AGRADECIMIENTO

Quiero agradecer a todas las personas que de una u otra forma son parte de mi vida, en especial a mi padre Antonio Sánchez Carrión, que con gran esfuerzo y cariño siempre ha estado presente apoyándome en los momentos malos y buenos por los que he tenido que pasar. De igual forma quiero agradecerle a mi madre Silvana Magdalena Ruiz, que desde el cielo siempre ha estado conmigo y los pocos años que compartí contigo formaste las bases de la persona que soy ahora.

Omar Sánchez Ruiz

DEDICATORIA

Quiero dedicar este trabajo realizado con mucho esfuerzo, a mí querido y amado colegio “Mejía”, en el cual me formaron como un señor no solamente en el aspecto académico sino también en el aspecto personal, y que a través de su lema: “PER ÁSPERA AD ASTRA”, he podido sobrellevar los momentos más duros de mi vida, levantándome del suelo las veces que sean necesarias con el único objetivo de llegar hacia las estrellas.

Omar Sánchez Ruiz

AGRADECIMIENTO

Quiero dar en primer lugar, un agradecimiento especial a mi Dios Jehová, ya que es gracias a él que puedo disfrutar el don de la vida y es gracias a él que he podido seguir a lo largo de esta dura carrera estudiantil hasta terminarla.

Gracias a ti mamita por tu apoyo incondicional y por ayudarme constantemente a continuar con mis metas y sueños.

Gracias a ti papá por enseñarme con el ejemplo el valor del esfuerzo, por demostrarme que con perseverancia se puede conseguir cualquier cosa y por ser un ejemplo de arduo y duro trabajo.

A mis hermanas, Micaela y María Belén, por todo su amor y ayuda, le agradezco a Dios por tenerlas como parte de mi vida.

A mis amigos más allegados: Amparito, Iván, Isa, Edi y Evelyn porque al compartir momentos de diversión y esparcimiento me ayudaron a relajarme en momentos muy difíciles de la carrera.

Y a mi novia Helen, por ser una fuente interminable de amor, ánimo, apoyo y colaboración.

Oscar Omar Tenorio Bravo.

DEDICATORIA

Dedico este trabajo primeramente a Dios el cual se merece recibir todo el crédito por las cosas que tengo la posibilidad de hacer ya que mí objetivo en la vida para todas mis actividades es cumplir con lo que dice COLOSENSES 3:23:

"Cualquier cosa que estén haciendo, trabajen en ello de toda alma como para Jehová, y no para los hombres."

Además también lo dedico a mi familia y a mis amigos por confiar en mí… Esto es para ustedes.

Oscar Omar Tenorio Bravo.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación consta de cuatro capítulos, los que contienen las generalidades del proyecto, el análisis del estado actual de la seguridad de la información del servidor Quipux, la definición del plan de gestión de seguridad de la información y por último, las conclusiones y recomendaciones del proyecto.

El Capítulo I se constituye de cuatro secciones, en la primera sección se caracteriza la Dirección de Gestión de la Información y Procesos de la EPN, describiendo a la DGIP dentro de la EPN y su importancia en la misma, en la segunda sección se establece la situación actual de la seguridad de la información en la DGIP, la tercera sección se justifica la selección del caso de estudio definiendo la importancia del activo de información dentro de la organización y finalmente en su última sección se define el estándar NTE INEN-ISO/IEC 27001:2011, estableciendo una descripción del mismo y comparándolo con otros estándares.

El Capítulo II analiza el estado actual de la seguridad de la información del servidor Quipux, para lo cual está dividido en cuatro secciones. En la primera sección se establece el plan de acción para realizar el análisis de vulnerabilidades, en la segunda sección se encuentra las vulnerabilidades a nivel lógico del servidor, las cuales fueron encontradas al realizar pruebas con distintas herramientas, en la tercera sección se encuentran las vulnerabilidades a nivel físico, las cuales fueron encontradas con la utilización de checklist y finalmente en la última sección se enfoca en la evaluación de riesgos en base a los resultados obtenidos de la sección anterior, teniendo como resultado la matriz de evaluación de riesgos.

El Capítulo III está conformado de cuatro secciones para la definición del plan de gestión de seguridad de la información. En la primera sección se elabora el plan de gestión de seguridad de la información especificando los respectivos entregables, en la segunda sección se selecciona los controles en base al anexo A de la norma NTE INEN-ISO/IEC 27001:2011, elaborando la matriz de tratamiento de riesgos y la

matriz de aplicabilidad de los controles, en la tercera sección se desarrolla la factibilidad del proyecto en base a los controles seleccionados, y finalmente culmina el capítulo en la cuarta sección detallando los tipos de recursos necesarios para la implementación del plan.

El capítulo IV se presentan las conclusiones correspondientes al proyecto, las cuales destacan los aspectos más importantes a ser tomados en cuenta por los usuarios de este proyecto y también las recomendaciones respectivas para aquellos lectores que quieran realizar un trabajo similar para alguna otra organización.

CAPÍTULO 1 GENERALIDADES DEL PROYECTO

El presente proyecto tiene como objetivo general:

Diseñar el Plan de Gestión de la Seguridad de la Información para el servidor Quipux[1] de la Dirección de Gestión de la Información y Procesos de la Escuela Politécnica Nacional.

Y como objetivos específicos:

- Analizar la situación actual de la seguridad de la información del servidor Quipux de la Dirección de Gestión de la Información y Procesos, tomando en cuenta los objetivos de control de la norma NTE INEN- ISO/IEC 27001:2011
- Seleccionar los controles de los dominios de la norma NTE INEN-ISO/IEC 27001:2011 adecuados para la elaboración del Plan de Gestión de Seguridad de la Información, considerando las áreas más críticas del análisis anterior.
- Definir un Sistema de Gestión de Seguridad de la Información para el servidor Quipux que satisfaga las necesidades de seguridad identificadas.

Una vez establecido los objetivos enmarcados en este proyecto se aborda el análisis del entorno administrativo, mismo que comprende misión, visión, objetivos estratégicos, políticas, organigrama institucional, plan estratégico, mapa de procesos entre otros con lo que se tendrá un marco referencial para realizar el proyecto.

Además de esto se analizará la situación actual de la información del caso de estudio empezando de forma general con el análisis de la situación actual de la seguridad de la información en organizaciones estatales hasta llegar al caso de estudio, con lo cual se justificará la selección del caso de estudio y la importancia del proyecto.

Para terminar este capítulo se analizará el estándar NTE INEN-ISO/IEC 27001:2011 empezando desde sus antecedentes hasta la justificación del uso de dicho estándar en este proyecto.

[1] A lo largo de este proyecto se entiende como "servidor Quipux" al sistema que proporciona el servicio del software Quipux, es decir, al hardware, al software del sistema operativo y al software Quipux.

1.1 CARACATERIZACIÓN DE LA DIRECCIÓN DE GESTIÓN DE LA INFORMACIÓN Y PROCESOS DE LA ESCUELA POLITÉCNICA NACIONAL

Dado que la guía de implementación del SGSI NTE INEN-ISO/IEC 27003, estipula que para la realización de cualquier proyecto de este tipo es necesario que se tengan los fundamentos generales del lugar en donde se va a realizar el mismo, es necesario una caracterización que nos ayudará a tener un panorama general del lugar en donde se realizará este proyecto.

Una caracterización es una determinación de los atributos particulares de algo o de alguien, así que el objetivo de esta caracterización es determinar los atributos particulares de la Dirección de Gestión de la Información y Procesos para así tener un marco referencial de trabajo.

1.1.1 LA DIRECCIÓN DE GESTION DE LA INFORMACION Y PROCESOS DENTRO DE LA ESCUELA POLITÉCNICA NACIONAL

Para realizar la caracterización de la Dirección de Gestión de la Información y Procesos, se necesitó una autorización para el acceso a la información confidencial, misma que fue proporcionada por el director el Ingeniero Christian Villarroel. MSc. previo a la formalización respectiva (Anexo 1 y Anexo 2). A continuación se mostrará la información con la que dispone actualmente la DGIP.

Cabe destacar que muchos de los documentos solicitados aún están en etapa de desarrollo, por lo tanto la información proporcionada es la que ha sido únicamente la aprobada.

En este punto es importante mencionar que después de la caracterización de la organización la norma NTE INEN-ISO/IEC 27001 estipula que se debe realizar la gestión de activos para determinar cuáles son los activos de información críticos para la organización, sin embargo en este proyecto no se realiza esta gestión de activos ya que la Dirección de Gestión de la Información y Procesos de la Escuela

Politécnica Nacional a través de su director el Ing. Christian Villarroel. MSc y al oficial de seguridad la Ing. Liliana Córdova, requirió que se realizara el plan del SGSI específicamente para el sistema Quipux el cual está conformado por:

- Hardware: el cuál es el servidor físico que se encuentra en las instalaciones de la DGIP.
- Software: el cuál se aloja en el servidor físico y corresponde a 2 elementos:
    - Sistema operativo
    - Software Quipux.

Esta es la razón por la que se discrimina a los otros activos de información que son parte de la Dirección de Gestión de la Información y Procesos de la Escuela Politécnica Nacional.

1.1.1.1 Misión

La dirección de gestión de la información y procesos tiene la siguiente misión:

La Dirección de Gestión de la Información y Procesos tiene como misión administrar y centralizar los recursos informáticos y tecnológicos de la EPN, para fortalecer los ejes estratégicos de docencia, investigación y proyección social mediante la administración por procesos, innovación tecnológica, seguridad de la información y gestión del conocimiento, contribuyendo al desarrollo de la comunidad politécnica. [1]

1.1.1.2 Visión

La dirección de gestión de la información y procesos tiene la siguiente visión:

Ser un referente universitario en el apoyo a la gestión tecnológica y su vinculación con la comunidad, a través de la innovación tecnológica y la gestión del conocimiento [1]

1.1.1.3 Valores

- Respeto
- Solidaridad
- Honestidad

- Trabajo en equipo

1.1.1.4 Objetivos de la Dirección de Gestión de la Información y Procesos

- Gestionar la información Institucional, para la generación de datos duros que aporten a la toma de decisiones.
- Diseñar, implementar y administrar soluciones de innovación tecnológica, que permitan apoyar las actividades académicas, administrativas, de investigación y relación con el medio externo de la institución, a fin de cumplir los objetivos estratégicos institucionales.
- Generar una cultura de conocimiento y uso de las Tic´s en la comunidad politécnica.
- Establecer e implementar un modelo de gestión por procesos que asegure un cambio de cultura en la institución.
- Asegurar el perfeccionamiento profesional del personal de la DGIP a través de gestión del conocimiento. [2]

1.1.1.5 Organigrama institucional:

- NIVEL DIRECTIVO: El nivel directivo establecido en la estructura organizacional es ejercido por el Director, y es el que define políticas y lineamientos para la ejecución de las actividades que realiza el personal de la Dirección.

- NIVEL EJECUTIVO: El nivel ejecutivo establecido en la estructura organizacional es ejercido por los Líderes de Área, los mismos que implementarán las políticas y lineamientos establecidos por la Dirección, coordinarán y supervisarán el trabajo de su equipo.

- NIVEL OPERATIVO: El nivel operativo establecido en la estructura organizacional, es ejercido por los grupos de trabajo de cada área los mismos que ejecutarán el trabajo conforme a los lineamientos establecidos desde la dirección y las jefaturas. [2]

Figura 1-1 - Organigrama funcional de la DGIP [2]

1.1.1.6 Atribuciones y responsabilidades

- Planificar, organizar y coordinar las actividades relacionadas con la gestión de TIC's y Gestión por procesos.
- Establecer políticas, estrategias, procesos y procedimientos que regulen el uso de las TIC's y la Gestión por Procesos.
- Elaborar e implementar el Plan Informático de Tecnologías de la Información y Comunicaciones.
- Elaborar el plan de contingencia y recuperación de información de TIC´s.
- Generar proyectos informáticos y de procesos que apoyen a la consecución de los objetivos institucionales.
- Planificar, administrar, coordinar, desarrollar y mantener soluciones informáticas integradas para el apoyo de las operaciones y a la toma de decisiones institucionales.

- Planificar, administrar, coordinar y mantener la infraestructura tecnológica y servicios de red de la institución, con el fin de satisfacer el acceso a los servicios de TIC.
- Definir, justificar, implantar y actualizar la infraestructura informática de la institución; así como, mantener actualizado su inventario tecnológico.
- Definir y regular los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica institucional.
- Administrar la entrega y el soporte de los Servicios de TIC en la Institución.
- Administrar, mantener y custodiar los datos institucionales, dentro de la Base de Datos Corporativa; así como establecer los mecanismos que la protejan y salvaguarden.
- Cumplir con las normativas legales vigentes relacionadas al derecho a la inviolabilidad y al secreto de la correspondencia física y virtual, y al derecho a la intimidad personal y confidencialidad.
- Definir los requerimientos de seguridad informática en función de sus necesidades.
- Definir políticas de seguridad de la información basada en estándares internacionales.
- Promover proyectos de innovación, eficiencia, calidad y mejoramiento en la gestión Institucional con enfoque en la satisfacción de sus clientes internos y externos;
- Coordinar e Implementar la gestión por procesos en la institución;
- Planificar, promover, coordinar e implementar el proceso de restructuración Institucional en coordinación con la entidad rectora y las Direcciones de Talento Humano y Planificación.
- Realizar diagnósticos de situación actual para implementar mejores prácticas en la gestión por procesos institucionales;
- Administrar el catálogo de procesos institucionales;
- Gestionar la Cadena de valor de los Procesos Institucionales, así como verificar el cumplimiento de indicadores, en coordinación con las diferentes unidades de la Institución para alcanzar las metas de calidad de gestión.
- Realizar la gestión de monitoreo y control de procesos;

- Preparar, controlar e informar el cumplimiento del Plan Operativo de la Dirección;
- Ejercer las demás atribuciones, delegaciones y responsabilidades en el ámbito de su competencia, establecidas en la normativa vigente y las que fueren asignadas. [2]

1.1.1.7 Productos y servicios

Infraestructura y Redes

- Políticas, procesos y procedimientos que regulen el funcionamiento del Área;
- Portafolio de proyectos del Área;
- Matriz de seguimiento de los proyectos del Área;
- Plan anual de mantenimiento preventivo y correctivo de la infraestructura tecnológica del Centro de Datos y Equipos de Comunicación;
- Informe de ejecución del plan anual de mantenimiento preventivo y correctivo de la infraestructura tecnológica del Centro de Datos y Equipos de Comunicación;
- Informes de evaluación de infraestructura tecnológica del Centro de Datos y Equipos de Comunicación;
- Informes de Monitoreo de la red.
- Planes de contingencia de la infraestructura tecnológica del Centro de Datos y Equipos de Comunicación;
- Procedimientos de recuperación de desastres;
- Plan de gestión de configuraciones;
- Políticas de respaldo de los datos corporativos;
- Informes de monitoreo de los servicios de T.I.;
- Planes para obtención de respaldos;
- Planes de capacidad de los servicios de T.I.;
- Políticas de seguridad informática;
- Planes e informes de seguridad informática;
- Plan de renovación de Infraestructura tecnológica Institucional

- Plan Operativo Anual de la DGIP (Elaborado en coordinación de las áreas de: Desarrollo de Soluciones Informáticas y Base de Datos, Infraestructura y Redes, Operaciones y Servicios; y Procesos, bajo los lineamientos del Director de la DGIP) [2]

Desarrollo de Soluciones Informáticas y Base de Datos

- Políticas, procesos y procedimientos que regulen el funcionamiento del Área;
- Sistemas Informáticos integrados;
- Metodología y Arquitectura de desarrollo;
- Estudio de innovaciones tecnológicas aplicables a la Escuela Politécnica Nacional;
- Informes de análisis de factibilidad para la implementación de nuevas tecnologías y modelos de arquitectura tecnológica;
- Portafolio de Proyectos del Área;
- Matriz de seguimiento de los proyectos del Área;
- Actas o acuerdos con entidades públicas y /o privadas de servicios tecnológicos externos para el funcionamiento y mejoramiento del servicio institucional;
- Documentación de los proyectos y soluciones, conforme a la metodología definida;
- Plan de Gestión de Cambios;
- Plan de Gestión de Versiones;
- Informe de ejecución de planes, programas o proyectos del Área;
- BDD corporativa Institucional y su diccionario;
- Administración de la BDD;
- Plan Informático Estratégico de Tecnologías de la Información y Comunicaciones (Elaborado en coordinación de las áreas de: Desarrollo de Soluciones Informáticas y Base de Datos, Infraestructura y Redes y Operaciones y Servicios, bajo los lineamientos del Director de la DGIP). [2]

Operaciones y Servicios

- Políticas, procesos y procedimientos que regulen el uso y la entrega de los servicios de TI;
- Portafolio de proyectos del Área;
- Matriz de seguimiento de proyectos del área;
- Mesa de Servicios;
- Acuerdo de Niveles de Servicios;
- Proyecto de mejoramiento de los niveles de servicio en la institución;
- Indicadores de satisfacción y uso de los servicio;
- Términos de Referencias consolidados de equipos informáticos y software;
- Inventario de equipos informáticos y software Institucional;
- Base de datos del conocimiento y de errores conocidos;
- Procesos y procedimientos de atención a usuarios;
- Informes de atención a usuarios;
- Planes de renovación de equipos tecnológicos de la EPN;
- Catálogo de Servicios de T.I. de la DGIP;
- Plan anual de mantenimiento preventivo y correctivo de equipos informáticos de la institución;
- Informe de ejecución del plan anual de mantenimiento preventivo y correctivo de equipos informáticos de la institución;
- Plan de contingencia de equipos informáticos y software. [2]

Procesos

- Políticas y procedimientos que regulen la Gestión por Procesos;
- Metodología de trabajo;
- Informe de diagnóstico institucional sobre el modelo de gestión de procesos institucional;
- Portafolio de proyectos del Área;
- Matriz de seguimiento de proyectos del área;
- Catálogo de procesos, productos y servicios institucionales;
- Mapa de procesos institucional;

- Cadena de valor institucional
- Estatuto de Orgánico por Procesos Institucional;
- Matriz de selección de procesos;
- Ficha de procesos;
- Matriz de procesos críticos priorizados;
- Flujogramas de procesos institucionales en situación actual;
- Procesos optimizados y/o automatizados;
- Flujogramas de procesos institucionales mejorados;
- Matriz de indicadores de procesos;
- Documentos o instrumentos de implementación de procesos;
- Medición de la calidad de procesos;
- Planes de mejora continua;
- Plan anual de Capacitación Informática (Elaborado en coordinación de las áreas de: Desarrollo de Soluciones Informáticas y Base de Datos, Infraestructura y Redes y Operaciones y Servicios, bajo los lineamientos del Director de la DGIP);
- Informes de ejecución del Plan anual de Capacitación Informática. [2]

1.1.2 IMPORTANCIA DE LA DGIP EN LA ESCUELA POLITÉCNICA NACIONAL

Dentro de la Escuela Politécnica Nacional se maneja un gran caudal de información por lo que sería sumamente difícil manejarla de forma independiente; además en la mayoría de los casos la información que se genera dentro de la EPN es crítica, por lo que se debe garantizar la integridad, confiabilidad y disponibilidad de la información.

Dado el caso entonces la DGIP es sumamente importante en la Escuela Politécnica Nacional ya que es el eje central del manejo de dicha información la cual debe ser manejada de manera apropiada y siguiendo normas y estándares ya que del manejo correcto de la información depende el éxito o fracaso de la institución.

Por otro lado la DGIP no se encarga solamente del manejo de información sino que se le ha asignado el deber de panificar, diseñar, implementar, controlar y mantener procesos institucionales.

El objetivo de estos procesos es lograr resultados exitosos los cuales generan ganancia para la institución y se encargan de que los objetivos institucionales se los realice de una forma estandarizada, dicho esto entonces la DGIP cumple una función importante en el desarrollo de dichos procesos y la ejecución de los mismos, con lo cual se logra un avance significativo en el cumplimiento de los objetivos de la institución.

1.2 SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA DIRECCIÓN DE GESTIÓN DE LA INFORMACIÓN Y PROCESOS DE LA ESCUELA POLITÉCNICA NACIONAL

1.2.1 SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES ESTATALES

De acuerdo a la norma NTE INEN-ISO/IEC 27000:2012, dentro de las organizaciones privadas y estatales, uno de los activos más importantes e imprescindibles es la información. Partiendo de esto, es necesario conocer con qué tipo de controles cuentan las organizaciones estatales en el campo de la seguridad de la información.

Actualmente el gobierno nacional cuenta con la Subsecretaría de Gobierno Electrónico, la cual a su vez se compone de tres direcciones:

- Dirección de Gestión de Gobierno Electrónico,
- Dirección de Arquitectura Tecnológica y Seguridad de la Información
- Dirección de Servicios de Gobierno Electrónico.

La Dirección de Arquitectura Tecnológica y Seguridad de la Información tiene especial relevancia para las distintas organizaciones estatales, así como para los usuarios de las mismas, ya que su misión es “Planificar, diseñar, mantener y difundir la Arquitectura de Gobierno Electrónico y Seguridad de la Información; para

implementar servicios de Gobierno Electrónico que contribuyan a satisfacer los requerimientos de la ciudadanía y del gobierno nacional, garantizando la confidencialidad, integridad y disponibilidad de la información" [3]. Esta dirección es un eje fundamental en lo que se refiere a la seguridad de la información de las distintas entidades gubernamentales.

Además el Acuerdo Ministerial 166, emitido por la Secretaría Nacional de la Administración Pública (SNAP), establece que para la Gestión de la Seguridad de la Información se debe utilizar obligatoriamente la familia de normas NTE INEN ISO/IEC 27000 dentro de las entidades de la Administración Pública Central. Junto con este acuerdo se anexó el Esquema Gubernamental de Seguridad de la Información (EGSI), el cual se basa en la norma NTE INEN ISO/IEC 27002:2009 y recoge varias directrices para su cumplimiento. [4]

Con lo mencionado anteriormente se tiene una base para la adecuada gestión de la seguridad de la información dentro de las distintas organizaciones estatales, y su adopción se la realiza de acuerdo a la estructura de la organización y al nivel de madurez de la gestión de la seguridad de la información.

Cabe recalcar que la Escuela Politécnica Nacional al tratarse de una entidad pública autónoma, que no pertenece a ninguno de los poderes estatales, no tienen como obligación seguir las normativas de la Secretaría Nacional de la Administración Pública (SNAP) ya que dicha secretaría regula a las instituciones que se encuentran bajo el poder ejecutivo. Por lo tanto estas normas podrían ser una guía para tratar el tema de la seguridad de la información en organizaciones que no cuenten con una normativa respecto a este campo, como es el caso de la Escuela Politécnica Nacional.

1.2.2 IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se ha convertido en un tema recurrente en la actualidad debido al impacto que esta genera tanto de forma individual, como en las grandes empresas, esto ha llevado a que la información sea, en muchos de los casos, el activo de información más importante de las empresas.

Por tal razón la aplicación de técnicas y políticas de seguridad dentro de las empresas se ha convertido en un hito crítico con lo cual se garantiza la integridad, confidencialidad y disponibilidad de la información; de tal forma que toda la información de la empresa sea protegida, pero no de cualquier manera, sino más bien siguiendo normas y estándares.

Todo esto resultará en los siguientes beneficios para la empresa:

- Mejor posicionamiento en el mercado.
- Ventaja competitiva frente a sus pares.
- Mejora de la imagen de la empresa.
- Aumento de los niveles de confianza de los clientes.
- Mejora continua de la gestión de la seguridad de la información.
- Reducción de costos relacionados a los diversos incidentes de seguridad.
- Identificación y mitigación de riesgos.
- Garantiza la continuidad del negocio.

Con esto se concluye que la seguridad de la información juega un papel importante en el crecimiento total de la empresa y por lo cual es necesario que se aplique de forma correcta y responsable.

1.2.3 SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN EL CASO DE ESTUDIO

El establecer la situación actual de la seguridad de la información de la DGIP puede convertirse en un trabajo complejo, debido a las áreas que la componen (Desarrollo, Operaciones, Procesos, Redes e Infraestructura), y a la cantidad de activos de información que posee, así como también su personal. Por tal razón en este apartado se busca identificar en rasgos generales de la situación actual de la información en la DGIP lo cual es un punto de partida para después centrarse en el caso de estudio específico.

Para ello se ha elaborado Checklist que ayudan a definir la situación actual de la seguridad de la información, dichos Checklist contienen preguntas de acuerdo a los

activos de información más críticos para la DGIP y están divididos para las áreas más representativas.

Los Checklist están detallados en el Anexo 17, cada uno de estos está conformado con 105 y 220 preguntas respectivamente con respuestas de SI y NO.

Las preguntas en las que se marque un SI como respuesta indican que el activo de información del que se está tratando es seguro, caso contrario se asume que tiene fallas de seguridad.

De acuerdo al número de respuestas SI y NO se determina el grado de seguridad de la información que existe en cada área y posteriormente se calcula un promedio general entre las 3 áreas involucradas, con lo cual se tendrá un panorama general de la situación actual de la seguridad de la información en la DGIP.

Los resultados de los Checklist son los siguientes:

Para el área de operaciones:

ÁREA	TOTAL DE PREGUNTAS	CONFORMIDADES	OPORTUNIDADES DE MEJORA
OPERACIONES	105	71	34

Tabla 1-1 – Tabulación de Resultados del Área de Operaciones[2]

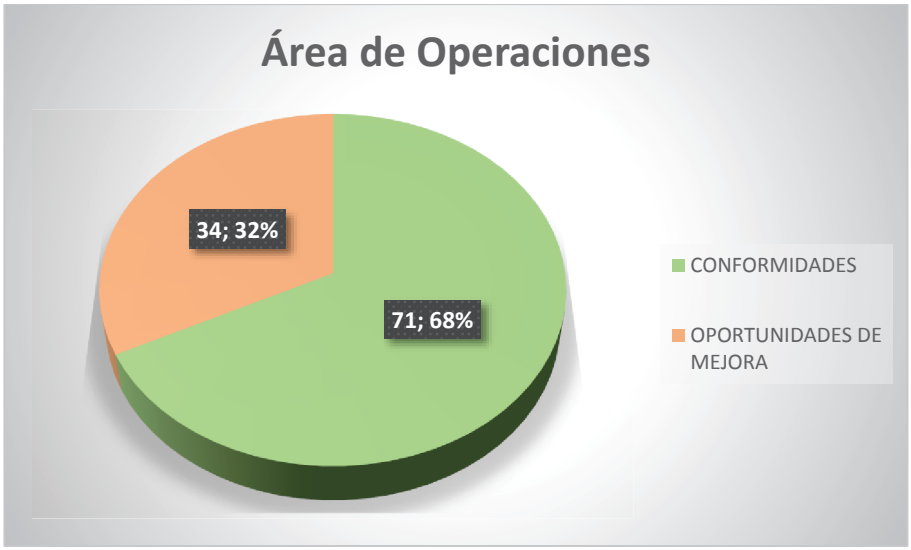

Figura 1-2 - Resultado de la Seguridad Física del Área de Operaciones[3]

[2] Tabla tabulada por los autores, como resultado de los checklist realizados dentro de la organización.

Para el área de redes e infraestructura:

ÁREA	TOTAL DE PREGUNTAS	CONFORMIDADES	OPORTUNIDADES DE MEJORA
REDES E INFRAESTRUCTURA	220	160	60

Tabla 1-2 - Tabulación de Resultados del Área de Redes e Infraestructura[4]

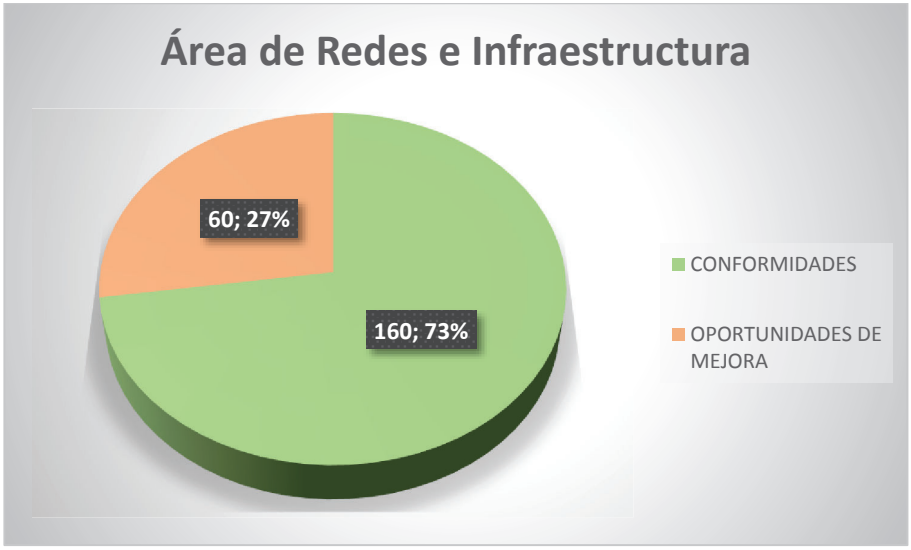

Figura 1-3 - Resultado de la Seguridad Física del Área de Redes e Infraestructura[5]

Para el área de desarrollo:

ÁREA	TOTAL DE PREGUNTAS	CONFORMIDADES	OPORTUNIDADES DE MEJORA
DESARROLLO	61	42	19

Tabla 1-3 - Tabulación de Resultados del Área de Desarrollo[6]

[3] Figura realizada por los autores en base a la Tabla 1-1
[4] Tabla realizada por los autores en base a los checklist realizados dentro de la organización.
[5] Figura realizada por los autores en base a la Tabla 1-2
[6] Tabla realizada por los autores en base a los checklist realizados dentro de la organización.

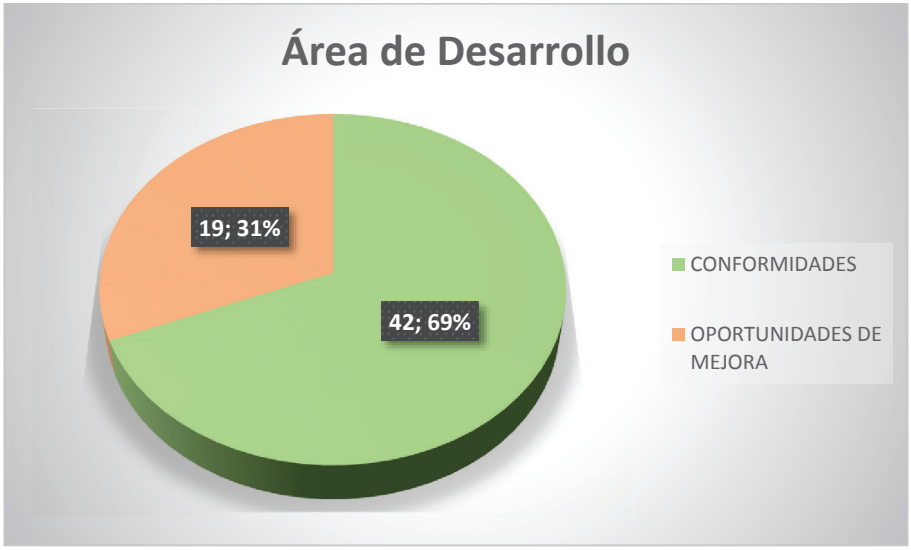

Figura 1-4 - Resultado de la Seguridad Física del Área de Desarrollo[7]

Dados estos resultados se procede a realizar un balance general de todas las áreas en las que se realizaron los checklist, teniendo así una idea general de cómo se está manejando la seguridad de la información dentro de la DGIP. Los resultados son los siguientes:

ÁREAS	CONFORMIDADES	OPORTUNIDADES DE MEJORA
DESARROLLO	69%	31%
OPERACIONES	73%	27%
REDES E INFRAESTRUCTURA	68%	32%
PROMEDIO	70%	30%

Tabla 1-4 - Tabulación del Resultado de todas las Áreas[8]

[7] Figura realizada por los autores en base a la Tabla 1-3

[8] Tabla elaborada por los autores, tabulando todos los checklist realizados dentro de la organización

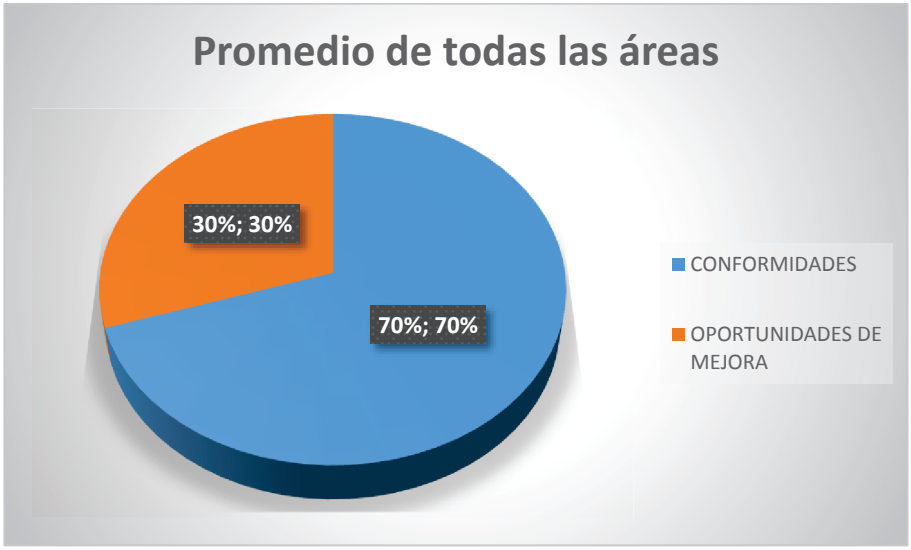

Tabla 1-5 - Resultado de la Seguridad Física de la DGIP[9]

1.3 JUSTIFICACIÓN DE LA SELECCIÓN DEL CASO DE ESTUDIO

1.3.1 CARACTERIZACIÓN DEL CASO DE ESTUDIO

El Sistema Quipux es un sistema de gestión documental que facilita la creación, manejo y transmisión de la información dentro de la Escuela Politécnica Nacional.

Cabe destacar que en este proyecto se realiza el plan para el Sistema de Gestión de Seguridad de la Información para este activo de información en específico, ya que fue un requerimiento hecho por la DGIP, por lo que no se realiza la gestión de activos estipulada en la norma NTE INEN-ISO/IEC 27001.

El sistema Quipux como activo de información está conformado por 2 partes:

- Hardware: el cuál es el servidor físico que se encuentra en las instalaciones de la DGIP.
- Software: el cuál se aloja en el servidor físico y corresponde a 2 elementos:
    - Sistema operativo
    - Software Quipux.

[9] Figura realizada por los autores en base a la Tabla 1-4

Para cada una de estas partes se debe especificar cuáles son las amenazas y vulnerabilidades que podrían incurrir en riesgos.

1.3.2 IMPORTANCIA DEL SERVIDOR QUIPUX EN LA ESCUELA POLITÉCNICA NACIONAL

Como se mencionó en puntos anteriores la Escuela Politécnica Nacional genera, recibe y procesa mucha información en la mayoría de los casos plasmada en documentos que son soporte de procesos que se desarrollan dentro de la institución, por tal razón era necesaria la correcta administración de dichos documentos.

Partiendo de esta necesidad se implanto el servidor Quipux dentro de la Escuela Politécnica Nacional; Quipux es un sistema de gestión documental modificado a partir de ORFEO el cual utiliza tecnologías y estándares abiertos, el responsable de hacer estas modificaciones fue la Subsecretaria de Gobierno Electrónico, adaptándolo a las necesidades de las entidades públicas del Ecuador.

Estos sistemas de gestión documental son herramientas básicas para el registro, control, circulación y organización de documentos digitales o impresos en las empresas, razón por la cual la Escuela Politécnica Nacional vio necesaria su implantación.

La importancia de este sistema de gestión documental radica en que proporciona las siguientes ventajas:

- Ahorro de espacio físico para almacenamiento de documentos.
- Disminución del riesgo de la perdidas por incendios, robos, inundaciones, otros.
- Conservación intacta de los documentos a lo largo del tiempo.
- Acceso inmediato a los documentos independientemente del lugar geográfico
- Búsqueda de documentos definiendo criterios de acceso de forma flexible y fácil.
- Consulta simultanea de varios lectores.
- Reproducción y envío de documentos obviando el traslado físico.

- Inviolabilidad de la información a través de mecanismos de seguridad digital.
- Minimización de tiempos de distribución y consulta.
- Ahorro de recursos físicos y económicos para gestionar los documentos.
- Disminución de impresión de documentos.
- "Apoyo a la conservación del ambiente [5]

1.4 DEFINICIÓN DEL ESTÁNDAR NTE INEN-ISO/IEC 27001:2011

1.4.1 ANTECEDENTES

El origen de la estandarización de controles para la seguridad de la información empieza en el año 1979 cuando un grupo de empresarios y especialistas en seguridad las más grandes empresas de Inglaterra se reunieron con el fin de acordar controles claves de seguridad para que todas las organizaciones las puedan cumplir.

Luego de esto el departamento de comercio e industria (The Department of Trade and Industry), decide desarrollar 10 controles en un código de buenas prácticas para la Administración de la Seguridad de la información.

El desarrollo formal de un estándar para la Administración de la Seguridad de la Información fue propuesta por el Instituto Estándar Británico (British Estándar Institute) el cual publico la norma 7799, en 1995, que era un código de buenas prácticas para la seguridad de la información fue la primera parte.

Posteriormente en el año 1998 el Instituto Estándar Británico genera la segunda parte del código de buenas prácticas, donde se detallan más de 100 controles como parte de un ISMS (Sistema de Administración de Seguridad de la Información), basado en una estrategia formal de Análisis de Riesgos.

El estándar tenía el nombre de BS 7799 y empresas europeas, asiáticas y norteamericanas adoptaron la norma por la necesidad de contar con un estándar que sea confiable en el manejo de internet y del e-bussiness.

Las dos partes del estándar se revisaron en 1999 y la primera parte fue adoptada por ISO la cual se denominó ISO 17799 en el año 2000.

La segunda parte de la norma BS 7799 se revisó y actualizo en el año 2002 con lo cual la ISO la publico con el nombre de ISO/IEC 27001, al mismo tiempo se revisó y actualizo la ISO 17799, la cual con el tiempo adoptaría el nombre de ISO 27002:2005.

En Marzo de 2006, posteriormente a la publicación de ISO/IEC 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

1.4.2 VERSIONES DEL ESTÁNDAR ISO/IEC 27001

La norma ISO/IEC 27001 ha tenido una serie de variaciones desde su publicación esta evolución se la puede resumir en el siguiente cuadro [6]:

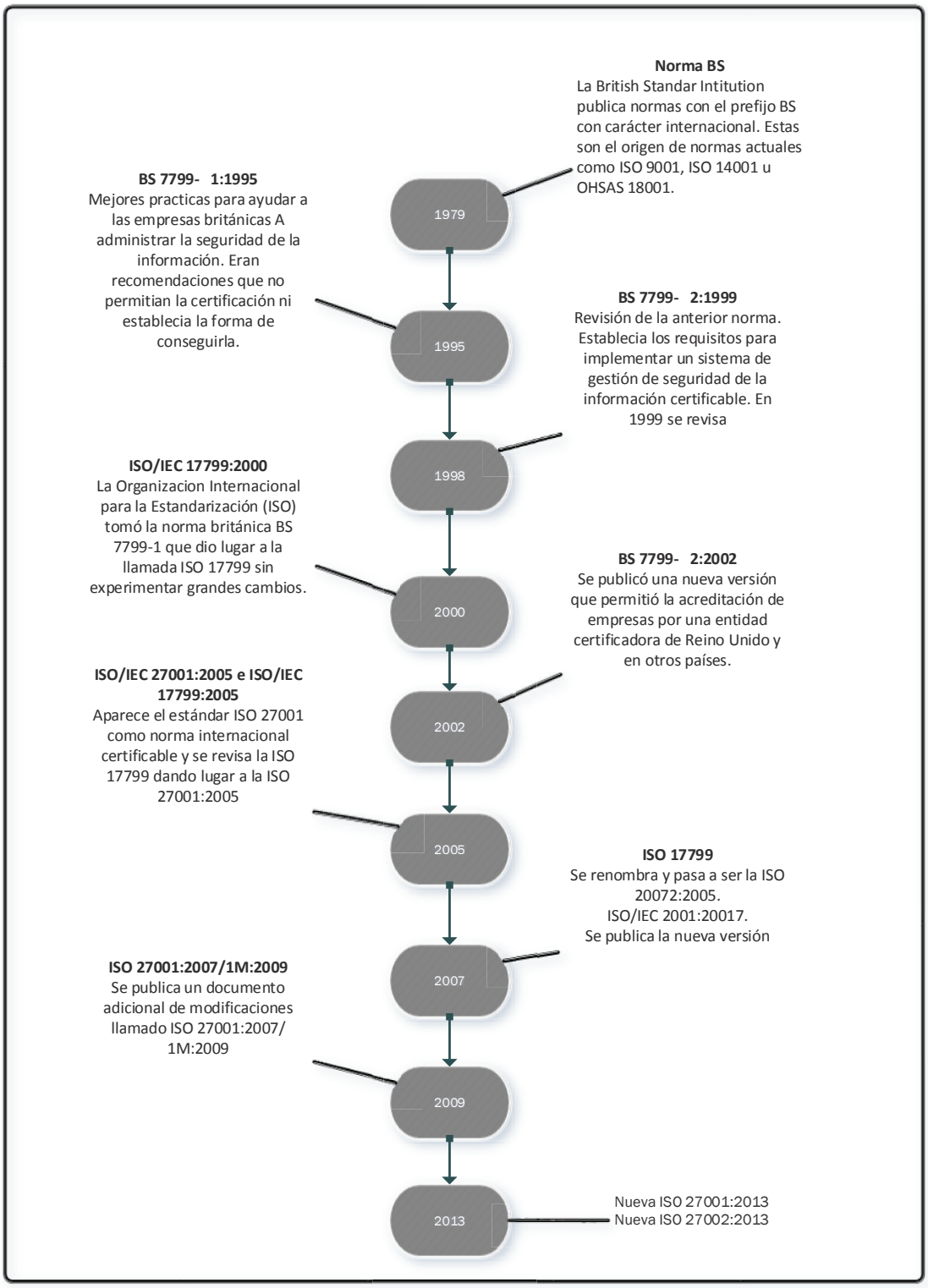

Figura 1-5- Versiones del estándar ISO/IEC 27001 [6]

1.4.3 DESCRIPCIÓN DEL ESTÁNDAR NTE INEN-ISO/IEC 27001:2011

La norma NTE INEN-ISO/IEC 27001:2011 es una adaptación idéntica de la norma ISO/IEC 27001 del 2005 y de la revisión realizada en el 2007, así que se trata de la norma principal de la familia de normas ISO/IEC 27000 ya que es la única susceptible de certificación.

Dicha norma contiene los requisitos necesarios para planificar, desarrollar, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) en cualquier tipo de organización, de acuerdo al ciclo PDCA (Plan-Do-Check-Act) y con un enfoque de gestión de riesgos hacia los activos de información más relevantes de las organizaciones.

1.4.3.1 Estructura:

Está compuesto por los siguientes apartados:

a) Introducción
b) Objeto y campo de aplicación
c) Normas de Referencia
d) Términos y definiciones
e) Sistema de gestión de seguridad de la información
f) Responsabilidad de la dirección
g) Auditoría interna del SGSI
h) Revisión del SGSI por la dirección
i) Mejora del SGSI

Anexo A (Normativo) Objetivos de control y controles. [7]

1.4.3.2 Anexo A:

Describe de forma general 39 objetivos de control y sus respectivos controles.

a) Políticas de la seguridad

b) Organización de la seguridad de la información
c) Gestión de activos
d) Seguridad de los recursos humanos
e) Seguridad física y del entorno
f) Gestión de operaciones y comunicaciones
g) Control de acceso
h) Adquisición, desarrollo y mantenimiento de sistemas de información
i) Gestión de incidentes de la seguridad de la información
j) Conformidad [8]

1.4.4 COMPARACIÓN DEL ESTÁNDAR NTE INEN-ISO/IEC 27001:2011 CON OTROS MARCOS DE TRABAJO

1.4.4.1 ISM3

El Modelo de Madurez de Gestión de Seguridad de la Información es un estándar orientado a procesos que a través de la utilización de niveles de madurez pretende dar un enfoque diferente basado en modelos (Modelo de la gestión de seguridad de la información, Modelo organizacional, Modelo de sistemas de información y Modelo de la seguridad en contexto) para la especificación, implementación, operación y evaluación de los sistemas de gestión de seguridad de la información. [9]

Si bien es cierto que ISM3 permite construir un SGSI de acuerdo al tamaño de la organización, dicha norma más bien se la puede utilizar para establecer el nivel de madurez de SGSI existentes y también puede servir de ayuda a la implementación de la ISO/IEC 27001 puesto que en los cinco niveles de madurez que contempla el ISM3 hace referencia a estándares conocidos tales como ISO 9001 el cual es compatible con la ISO/IEC 27001.

1.4.4.2 SOGP:

El Estándar de las Buenas Prácticas para la Seguridad de la Información aborda a la seguridad de la información desde una perspectiva de negocios y

provee una base ideal para mejorar y asegurar la información de una organización. El estándar cubre el espectro completo de las medidas de seguridad que se deben tomar para mantener los riesgos asociados a los sistemas de información dentro de los límites aceptables y presenta buenas prácticas en declaraciones funcionales y claras, proporcionando a las organizaciones el soporte necesario para abordar la seguridad de la información a través de tres aspectos claves: intercambio del conocimiento, reportes e investigaciones, herramientas y métodos. [10]

El SOGP contempla un conjunto de buenas prácticas basadas en la experiencia de la ISF (Information Security Forum) y forma parte de su modelo de seguridad formado por distintas herramientas, a diferencia de la ISO/IEC 27001 la cual fue desarrollada por una organización internacional con credibilidad a nivel mundial; a partir de esto una de las diferencias más relevantes entre SOGP e ISO/IEC 27001 es que para el análisis del riesgo, SOGP utiliza su propia herramienta de análisis como lo es IRAM (Information Risk Analysis Methodology) mientras que en la ISO/IEC 27001 se puede hacer uso de distintas metodologías para el correcto análisis del riesgo dependiendo de los requerimientos de la organización.

1.4.4.3 *COBIT*

Los Objetivos de Control para Información y Tecnologías Relacionadas proveen un marco de trabajo para la correcta administración y gobernanza de la información de la empresa y la tecnología, y está dirigida al control y supervisión de las TI. [11]

COBIT 5 para la Seguridad de la Información: se trata de una guía específica para los profesionales de la Seguridad de la Información y otros interesados, la cual construye sobre el marco del COBIT 5, un enfoque robusto para el gobierno y la gestión de la seguridad de la información, sobre la base de los procesos de negocios de la organización. [12]

COBIT está orientado al negocio y al gobierno de TI en su totalidad, mientras que la ISO/IEC 27001 provee prácticas y metodologías para la gestión de seguridad de la información a través de la implementación de diversos controles de seguridad. La diferencia más relevante se puede considerar el

alcance de cada una, puesto que COBIT plantea un conjunto completo para el gobierno de TI en el cual se aborda de cierta manera un planificación de la seguridad dentro de la organización, mientras que la ISO/IEC 27001 se la puede considerar como una guía independiente para la seguridad de la información dentro de una organización.

1.4.4.4 ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información es un estándar para la gestión de servicios aceptado a nivel mundial, el cual proporciona un conjunto de conceptos y buenas prácticas para planificar, entregar y dar soporte a los servicios de TI. [13]

ITIL está compuesto por 5 libros (Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio) que contemplan el ciclo de vida del servicio, de los cuales en el segundo libro “Diseño del Servicio” que permite diseñar nuevos servicios así como mejorar y cambiar los existentes, se puede encontrar los procesos de Gestión del Riesgo y Gestión de la Seguridad de TI cuyo objetivo primordial es “asegurar la confidencialidad, la integridad y la disponibilidad de las informaciones, datos y servicios de TI de una organización” [14].

La seguridad de la información dentro de ITIL es abarcada en uno de sus libros a través del proceso de Gestión de la Seguridad, dicho proceso solo busca establecer políticas para mantener la confidencialidad, integridad y disponibilidad de la información, mientras que el estándar ISO/IEC 27001 contiene los requisitos para la implementación de un SGSI, también ITIL puede ser aplicado parcialmente sin la necesidad de justificar la no aplicabilidad, cosa contrario ocurre con la ISO/IEC 27001 la cual determina que la no aplicabilidad de algunos de sus controles tiene que ser justificada de forma adecuada.

1.4.4.5 Tabla Comparativa

	ORGANIZACIÓN	ORGANIZACIÓN RECONOCIDA INTERNACIONALMENTE	PROPIETARIA	LIBRE	COMPATIBLE CON OTRAS NORMAS	CERTIFICABLE	ENFOQUE ORIENTADO A PROCESOS	ENFOQUE ORIENTEADO A CONTROLES
SOGP	ISF (Information Security Forum)		X		X			X
ISM3	CONSORCIO ISM3			X	X		X	
COBIT	ISACA (Information Systems Audit and Control Association) e ITGI (IT Governance Institute)	X		X	X		X	
ITIL	OGC (Office of Government Commerce)	X	X			X	X	
ISO/IEC 27001	International Organization for Standardization	X	X		X	X		X

Tabla 1-6 - Comparación entre marcos de trabajo que contemplan SGSI[10]

[10] Tabla elaborada por los autores, en la cual se comparan distintos tipos de frameworks que contemplan SGSI

Del análisis anterior se selecciona el estándar ISO/IEC 27001 para el diseño de un Plan de Gestión de Seguridad de la Información dadas las siguientes razones:

- La norma original fue desarrollada por la ISO e IEC, instituciones las cuales son reconocidas a nivel mundial en el campo de la normalización.
- La mayor parte de los institutos de estandarización nacionales para el desarrollo de sus normas se basan parcial o totalmente en las normas ISO, las cuales son aceptadas internacionalmente.
- La ISO/IEC 27001 ofrece certificación externa y las organizaciones que la utilicen si lo hacen de forma adecuada pueden entrar en un proceso de certificación de la misma.

1.4.5 SGSI SEGÚN LA NTE INEN-ISO/IEC 27000:2012

La norma NTE INEN ISO/IEC 27000 define a un SGSI (Sistema de Gestión de la Seguridad de la Información) de la siguiente manera: “Un SGSI (Sistema de Gestión de la Seguridad de la Información) provee un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información de información, para alcanzar los objetivos del negocio basado en una evaluación del riesgo y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar efectivamente los riesgos”. [15]

Con esta definición se puede tener una base de lo que es un SGSI, es decir, conocer cuáles son los objetivos y que se espera tener a largo plazo, y aunque es verdad que este proyecto no tiene como alcance implementar un SGSI en la organización, esta definición es de utilidad porque al diseñar el plan del SGSI, el cual si está dentro del alcanza de este proyecto, se deben tener muy presente las metas que se espera conseguir, de tal forma que el diseño del plan para la implementación del SGSI constituya una base sólida sobre la cual se pueda implementar el SGSI.

Además de esto es importante desglosar los términos más importantes que contiene la definición previamente dada, y este sentido la norma también nos proporciona la definición de estos términos. A continuación están las definiciones más importantes

para tener un conocimiento concreto de lo que es un SGSI según la norma NTE ISO/IEC 27000.

- ***Información:*** La norma considera a la información como uno más de los activos de la empresa, pero lo considera como un activo esencial para el negocio de la organización por lo que debe ser protegida apropiadamente. Esta puede ser almacenada de distintas maneras, puede estar en formato digital o en forma material y puede ser transmitida por medios electrónicos o físicos.
- ***Seguridad de la Información:*** La norma describe a la seguridad de la información mediante tres dimensiones principales, las cuales son:
    1. Confidencialidad
    2. Disponibilidad
    3. Integridad

  Lo que se busca con la seguridad de la información es aplicar medidas y controles que aseguren el correcto funcionamiento de las tres dimensiones, lo que supone la consideración de una gran variedad de amenazas. Los controles seleccionados llegan a existir gracias a un análisis previo de riesgos y del estado de la seguridad de la información de la organización, esto corresponde a la identificación de controles los cuales después deben ser implementados, monitoreados, revisados y mejorados donde sea necesario.
- ***Gestión:*** El termino gestión puede tener diferentes enfoques dependiendo del ámbito en el que se desarrolle y según la norma y dentro del ámbito de un SGSI, gestión es todo lo que tiene relación con la supervisión y toma de decisiones necesarias para alcanzar los objetivos del negocio a través de la protección de los activos de información de la organización.
- ***Sistema de Gestión:*** Un sistema de gestión tiene una estructura organizacional, políticas, actividades de planificación, responsabilidades, practicas, procedimientos, procesos y recursos. Dentro del ámbito de la seguridad de la información un sistema de gestión permite:
    - Satisfacer los requerimientos de seguridad de los clientes y de las partes involucradas.
    - Mejorar los planes y actividades de la organización.

- Cumplir con los objetivos de la organización respecto a la seguridad de la información.
- Cumplir con regulaciones, legislación y mandatos de la industria.
- Gestionar los activos de información de una manera organizada que facilite la mejora continua y el ajuste de las metas actuales de la organización y al entorno. [15]

CAPÍTULO 2 ANÁLISIS DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL SERVIDOR QUIPUX

2.1 PLAN DE ACCIÓN PARA ANÁLISIS DE VULNERABILIDADES Y EVALUACIÓN DE RIESGOS EN EL SERVIDOR QUIPUX.

Para realizar el análisis de vulnerabilidades y la evaluación de riesgos en el servidor Quipux administrado por la DGIP de la Escuela Politécnica Nacional, es necesario definir un plan de acción, el cual consiste en un conjunto de pasos ordenados con la utilización de distintas herramientas y basados en los principios de ethical hacking fundamentado sobre un marco legal.

A continuación se describe dicho plan con los puntos correspondientes.

2.1.1 MARCO LEGAL

El marco legal planteado describe los términos legales que corresponden a este proyecto, marcando así el límite y el alcance del proyecto, dejando claro que si no se cumple dichos términos, se procederá a ejecutar las sanciones correspondientes por parte de las autoridades pertinentes.

El siguiente cuadro detalla la disposición, artículos y sanciones aplicables a este proyecto:

MARCO LEGAL		
DISPOSICIÓN	**ARTÍCULO**	**SANCIÓN**
CÓDIGO ORGÁNICO INTEGRAL PENAL	Artículo 204.- Daño a un bien ajeno	Pena privativa de libertad de 1 a 3 años
	Artículo 229.- Revelación ilegal de base de datos	Pena privativa de libertad de 1 a 3 años
	Artículo 230.- Interceptación ilegal de datos	Pena privativa de libertad de 3 a 5 años
	Artículo 232.- Ataque a la integridad de sistemas informáticos	Pena privativa de libertad de 3 a 5 años
LEY DE COMERCIO ELECTRONICO, FIRMAS	Artículo 5.- Confidencialidad y Reserva	Sanción conforme a normas que rigen la

ELECTRONICAS Y MENSAJES DE DATOS	Artículo 9.- Protección de datos	materia
	Artículo 61.- Daños Informáticos	Pena privativa de libertad de 3 a 5 años y multa de $200 a $600 dólares de los Estados Unidos de Norteamérica
ESCUELA POLITÉCNICA NACIONAL - RESOLUCIÓN ADMINISTRATIVA No. 218-2013	Artículo 1.- Esta política es aplicada a los empleados, trabajadores, personal académico y estudiantes de la EPN	La DGIP debe notificar el incumplimiento de lo establecido en la presente resolución, a la autoridad correspondiente para los fines legales respectivos
	Artículo 2.- Propiedad y uso de los activos de información institucional.	
	Artículo 7.- Uso de la web 2.0	
	Artículo 9.- Confidencialidad de la información y uso de credenciales de acceso a los activos de información institucionales	
	Artículo 10.- Seguridades de redes LAN internas, servidores y laboratorios	
LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA	Artículo 6.- Información confidencial	Acciones legales pertinentes conforme a normas que rigen la materia
NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS	300 Evaluación de riesgo (300-1 Identificación, 300-2Plan de mitigación, 300-3Valoración y 300-4 Respuesta al riesgo)	-
	410-10 Seguridad de tecnología de información	-
	410-11 Plan de contingencias	-

Tabla 2-1 - Marco Legal del Proyecto[11]

Antes de realizar el análisis de vulnerabilidades a nivel lógico se debe establecer los límites legales sobre los cuales se actuará, empezando en la "Resolución Administrativa No. 218—2013 de la Escuela Politécnica Nacional", la "Ley de

[11] Tabla elaborada por los autores, en la que se identifican distintos artículos de leyes y normas, así como sus respectivas sanciones, en caso de que se incurra en cierta falta en el momento de realizar el análisis físico y lógico de vulnerabilidades.

Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", "La Ley orgánica de transparencia y acceso a la información pública" y el "Código Orgánico Integral Penal" de los cuales se han seleccionado ciertos artículos que se consideran que guardan relación con el correcto tratamiento de la información así como de los sistemas que los manejan.

- La Resolución Administrativa No. 218—2013 es de ámbito local es decir su aplicación es dentro de la Escuela Politécnica Nacional, por ende afecta a estudiantes, trabajadores y personal académico así como el manejo de los activos de información pertenecientes a la EPN.
- La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, hace referencia al comercio a través del uso de sistemas de información y de redes electrónicas, pero existen ciertos artículos de esta ley que hace referencia a ciertas características de la seguridad de la información como son confidencialidad y la protección de los datos.
- La Ley orgánica de transparencia y acceso a la información pública, establece el acceso a la información pública generada por organismos del sector público, así como también su respectivo manejo, en este caso existen penalidades si se divulgan información pública personal y tomarían las acciones legales pertinentes.
- El Código Orgánico Integral Penal es la normativa más importante ya que fue discutido y aprobado por la Asamblea Nacional del Ecuador, y contiene las sanciones respectivas al infringir los artículos de dicho código. También las normativas nombradas anteriormente hacen referencia al COIP.
- De igual forma se hace referencia a las "Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos" ciertas de las cuales establecen que es necesario definir mecanismos de control de riesgo al que está expuesta la organización para el logro de sus objetivos.

2.1.2 PLAN DE ACCIÓN

El plan de acción para la realización del proyecto constará de dos partes, la primera de un análisis de ethical hacking de caja blanca, el cual se realizará al interior de la Escuela Politécnica Nacional y la cual será supervisada por la parte administraba de la misma, y la segunda un análisis externo de ethical hacking de caja gris, en el cual se buscará vulnerabilidades desde el exterior de la Escuela Politécnica Nacional con lo cual se tendrá un análisis completo del estado de la seguridad de la información del servidor Quipux.

- ***Hacking de caja blanca***: consiste en utilizar técnicas de hackeo no intrusivo dentro de la organización, con la aprobación y el consentimiento de los altos mandos de la organización, el hecho de que no sea intrusivo significa que no va provocar daños en los sistemas, ni en la infraestructura de la organización garantizando la continuidad del negocio. El hacker de sombrero blanco no tiene como objetivo hacer daño a la organización sino todo lo contrario, busca mediante el uso de herramientas de hacking descubrir vulnerabilidades para informar a la dirección y que se puedan tomar medidas preventivas o correctivas.
- ***Hacking de caja gris:*** *este* tipo de hackeo es una mezcla entre un hackeo de caja blanca y un hackeo de caja negra, es decir que puede aprovechar sistemas externos a la organización para tratar de vulnerar sus sistemas o infraestructura, puede contar con la autorización de la dirección de la organización, pero en algunos los casos no es así. Aunque el hacker de sombrero gris no tiene como objetivo hacer daño a la organización, podría provocarlo debido al uso de herramientas intrusivas.

2.1.2.1 Respecto a las herramientas

Las herramientas a ser utilizadas, tanto para el análisis dentro de la Escuela Politécnica Nacional como fuera de está, son las siguientes:

Nessus:

Es una herramienta para ethical hacking la cual realiza análisis de vulnerabilidades en distintos sistemas operativos, fue desarrollado por Tenable Network Security y es gratuito para uso en ambientes no empresariales.

Nessus puede instalarse en un servidor y puede ser utilizado desde una consola web de acceso remoto y existen versiones para GNU/Linux, Mac OS X, Solaris, FreeBSD y Windows, en el caso de este proyecto Nessus está instalado en un sistema operativo Windows y la versión es la 6.1.2. [16]

Para realizar el análisis con Nessus se necesita configurar directivas dentro de la herramienta, una directiva está compuesta por opciones de configuración que se relacionan con la realización de un análisis de vulnerabilidades, entre otras opciones incluyen:

- Parámetros que controlan aspectos técnicos del análisis, tales como tiempos de espera, cantidad de hosts, tipo de analizador de puertos, etc.
- Credenciales para análisis locales, análisis de bases de datos Oracle autenticados, autenticación basada en HTTP, FTP, POP, IMAP o Kerberos.
- Especificaciones de análisis en función de plugins o familias pormenorizadas.
- Comprobaciones de directivas de compatibilidad de bases de datos, nivel de detalle de los informes, configuración de los análisis para la detección de servicios, comprobaciones de compatibilidad de Unix, etc.

Las directivas para este proyecto son las que vienen en la versión gratuita de Nessus y son las siguientes:

Basic Network Scan: es una directiva para realizar un escaneo de los hosts que se conectan a una red y se debe especificar la dirección IP del host que del que se quiere identificar vulnerabilidades.

Host Discovery: esta directica escanea host activos y puestos abiertos que podrían ser una amenaza para el servidor.

Web Application Test: escanea vulnerabilidades a nivel de aplicación dando como resultado una lista de vulnerabilidades publicadas o desconocidas. [17]

Maltego:

Es una aplicación de código abierto de análisis forense que permite la minería de datos y cuya representación gráfica posibilita una interpretación sencilla de los resultados obtenidos.

Maltego es un programa que puede ser utilizado para determinar las relaciones y enlaces del mundo real entre:

- Personas
- Los grupos de personas (redes sociales)
- Empresas
- Organizaciones
- Sitios Web
- Infraestructura de Internet, tales como: Dominios, Nombres DNS, Netblocks (bloques de red), Direcciones IP, Frases, Documentos y archivos

Estas entidades están vinculadas utilizando inteligencia de datos de fuentes abiertas [18].

Foca:

Es una herramienta que proporciona acceso a metadatos de diversos tipos de documentos (Microsoft office, Open office, pdf, etc.), los cuales una vez obtenidos cruza esa información para obtener datos relevantes de una organización. Es decir que FOCA descarga los diversos archivos ofimáticos relacionados con un dominio en específico, extrae los metadatos y organiza los datos presentado información como:

- Nombres de usuarios del sistema
- Rutas de archivos
- Versión del Software utilizado
- Correos electrónicos encontrados
- Fechas de Creación, Modificación e Impresión de los documentos.
- Sistema operativo desde donde crearon el documento
- Nombre de las impresoras utilizadas

- Permite descubrir subdominios y mapear la red de la organización
- Nombres e IPs descubiertos en Metadatos, etc.

Nmap:

Se trata de una herramienta de código abierto que permite analizar redes completas y es de gran ayuda para la auditoría informática, también se puede analizar objetivos individuales. [19]

Luego de realizar el análisis Nmap presenta cierta información como los host analizados, la topología de los mismos, pero la información más relevante es la "tabla del objetivo" que contiene información tal como número de puerto, estado del puerto, el servicio y la versión del servicio de dicho puerto.

- Nmap clasifica a los puertos en 6 estados: abierto, cerrado, filtrado, no filtrado, abierto filtrado y cerrado filtrado.
- Filtrado: Nmap no puede determinar si el puerto está abierto debido a que un filtro de paquetes no le permite alcanzar el objetivo.
- No Filtrado: el puerto es accesible pero Nmap no puede determinar si el puerto se encuentra abierto o cerrado.
- Abierto Filtrado: Nmap no puede determinar si el puerto está abierto o filtrado, generalmente ocurre cuando los puertos abiertos no responden.
- Cerrado Filtrado: Nmap no puede determinar si el puerto está cerrado o filtrado.

Comandos:

- Análisis puertos abiertos
  nmap -sS -p 1-65535 X.X.X.X
- Identificar versiones de los servicios de los puertos abiertos
  nmap -sS -sV -p 1-65535 X.X.X.X
- Identificación del sistema operativo
  nmap -O X.X.X.X
- Identificación del perímetro de red
  nmap --traceroute X.X.X.X

Acunetix:

Es una herramienta que permite realizar análisis de la seguridad de aplicaciones web, escaneando el sitio en busca de fallos de seguridad. La aplicación ejecuta una serie de pruebas configurables por el usuario para identificar las vulnerabilidades tanto en la programación de la página como en la configuración del servidor. [20]

2.1.2.2 Respecto a los paso a seguir

1. Realizar el cronograma de actividades detallando las herramientas que se van a utilizar para las distintas pruebas, para este caso es recomendable realizar las pruebas dentro y fuera de la Escuela Politécnica Nacional, preferiblemente a partir de las 20:00 horas, garantizando así que no se interfiera en el desempeño del servidor.
2. Escoger los puntos en los que se va a realizar las pruebas, para ello se debe seleccionar al menos dos puntos dentro de la Escuela Politécnica Nacional preferiblemente en distintas facultades o departamentos, para el caso del análisis externo basta con que el punto de acceso no sea parte de la red de la Escuela Politécnica Nacional.
3. Utilizar las herramientas para el análisis de vulnerabilidades con el fin de explotar posibles vulnerabilidades en el funcionamiento del servidor Quipux.
4. Clasificar los resultados de acuerdo al tipo de prueba y al tipo de herramienta que se utilizó
5. Realizar el análisis de dichos resultados para encontrar posibles falsos positivos y para filtrar las verdaderas vulnerabilidades.
6. Presentar un informe ejecutivo con el resultado del análisis realizado y las posibles opciones de solución de problemas.

2.2 VULNERABILIDADES A NIVEL LÓGICO DEL SERVIDOR

Al seguir el plan de acción con las distintas herramientas, se obtuvieron los siguientes resultados; para obtener información más detallada respecto al proceso de pruebas revise el Anexo 17.

2.2.1 PRUEBAS DE FOOTPRINTING CON FOCA

Como resultado más importante tenemos las direcciones ip tanto internas como externas de este servidor, ya que a partir de esto se puede realizar otras pruebas en las cuales se puede poner como objetivo dichas direcciones ip.

Además el hecho de que se pueda acceder al directorio del servidor Quipux dentro de la Escuela Politécnica Nacional también se lo considera un resultado importante ya que podrían existir muchas formas de explotar esta vulnerabilidad.

La información recopilada puede ser utilizada de forma maliciosas si así se lo quisiera es por ello que se deben aplicar controles preventivos para que la información pública revelada por esta herramienta sea manejada de la forma correcta.

2.2.2 PRUEBAS DE FOOTPRINTING CON MALTEGO

Con esta herramienta se obtuvieron resultados más detallados y al igual que la herramienta anterior los datos más sensibles encontrados fueron las direcciones ip del servidor, tanto interna como externa, esto representa una vulnerabilidad ya que se podría usar dichas direcciones ip para causar fallos en el servicio que presta este servidor.

Además esta herramienta presento resultados nuevos relacionados con números telefónicos y cuentas de correo electrónico relacionados al servidor Quipux, esto se convierte en una vulnerabilidad ya que se podría realizar ingeniería social para descubrir a quien pertenecen estos datos y ver cuanta influencia o qué relación

tienen con el servidor, por ejemplo si uno de esos correos o números telefónicos fueran del administrador del servidor, esta persona pudiera ser objetivo de ataque.

2.2.3 PRUEBAS DE PENETRACIÓN CON NMAP

El servidor Quipux de la Escuela Politécnica Nacional tiene como sistema operativo base CentOS, y el servidor web es Apache/2.2.15, por ende los puertos TCP abiertos de este servidor tienen que ver con servicios web, los cuales tienen que ser administrados de forma correcta, tomando las precauciones del caso para así no tener incidentes relacionados con los mismos.

2.2.4 AUDITORÍA CON NESSUS

Los resultados que genero la herramienta fueron los siguientes:

Vulnerabilidad	Cantidad
Altas	1
Medias	7
Bajas	2
Informativas	31

Tabla 2-2 - Resultados de la Auditoría con Nessus[12]

Para ver el detalle de las vulnerabilidades referirse al Anexo 17.

2.2.5 PRUEBAS DE VULNERABILIDADES WEB CON ACUNETIX

La herramienta genero un informe de 1839 páginas en las que se encuentran detallados los siguientes resultados:

Vulnerabilidad	Cantidad
Altas	390
Medias	262
Bajas	29
Informativas	3962

Tabla 2-3 - Resultados de las Pruebas de Vulnerabilidades con Acunetix[13]

[12] Tabla realizada por los autores, en base a los resultados obtenidos con la herramienta Nessus

[13] Tabla realizada por los autores, en base a los resultados obtenidos con la herramienta Acunetix

De estos resultados solamente tomamos las vulnerabilidades altas, ya que pueden representar un alto grado de vulnerabilidad para el servicio web. Las demás vulnerabilidades, pueden ser utilizadas para un análisis posterior después de analizar las vulnerabilidades altas. Para ver el detalle de las vulnerabilidades altas referirse al Anexo 17.

2.2.6 PRUEBAS DE VULNERABILIDADES WEB CON MCAFEE

El informe que proporcionado por esta herramienta fue de 1654 páginas en las que se encuentran detallados los siguientes resultados:

Nivel de Vulnerabilidad	Cantidad
Altas	3
Medias	6
Bajas	11
Informativas	16

Tabla 2-4 - Resultado de las Pruebas con McAfee[14]

De estos resultados solamente tomamos las vulnerabilidades altas, ya que pueden representar un alto grado de vulnerabilidad para el servicio web. Las demás vulnerabilidades, pueden ser utilizadas para un análisis posterior después de analizar las vulnerabilidades altas.

Para ver el detalle de las vulnerabilidades referirse al Anexo 17.

2.2.7 DISCUSIÓN DE LOS RESULTADOS

Se utilizaron las siguientes herramientas para el análisis lógico de vulnerabilidades:

- FOCA
- Maltego
- Nmap
- Nessus
- Acunetix

Con FOCA se logró obtener acceso a una estructura de carpetas que contienen archivos php relacionados al dominio del servidor Quipux, muchos de los cuales

[14] Tabla realizada por los autores, en base a los resultados obtenidos con la herramienta McAfee

tienen información relacionada con el desarrollo (módulos, métodos, validaciones, notificaciones) de la página web del Quipux, también se pudo obtener la IP interna del servidor con lo que posteriormente se podrá realizar pruebas con Nmap.

Con Maltego a partir del nombre del dominio se pudo obtener varias transformaciones tales como, DNS, url del Quipux, dirección IP externa del servidor, bloques de red relacionados a la ip del servidor, correos electrónicos relacionados al dominio del servidor, sitios donde se encuentra registrado el dominio del servidor, números telefónicos, usuarios relacionados al servidor, etc., mucha información de la cual puede ser utilizada por ejemplo para analizar la red del servidor, o simplemente para realizar ingeniería social dentro de la organización.

Con Nmap se escaneó al servidor Quipux tanto desde la red interna como desde una red externa, al escanear el servidor se logró obtener información de los puertos TCP abiertos del Quipux, que en este caso fue de un número de 3 puertos abiertos, los cuales tienen servicios conocidos (https, http-proxy, ssh-hostkey)

Con Nessus se escaneó al servidor Quipux, esta herramienta aparte de la información de los puertos abiertos, entrega también información sobre posibles vulnerabilidades que afecten al host escaneado y su severidad en el mismo, en este caso se realizó dos tipos de análisis (Advanced Scan y Web Application Test) tanto desde la red interna de la institución como de una red externa a la misma. En el primer análisis desde la red externa se obtuvo 22 vulnerabilidades (1 alta, 1 media y 20 informativas) y desde la red interna se obtuvo 33 vulnerabilidades (5 medias, 1 baja y 27 informativas), mientras que en el segundo análisis tanto desde la red interna como desde la red externa se obtuvo el mismo resultado es decir 24 vulnerabilidades (4 medias, 2 bajas y 18 informativas). Cabe recalcar que en la mayoría de los casos los resultados eran los mismos por lo que en un análisis global tiene un total de 41 vulnerabilidades (1 alta, 7 medias, 2 bajas y 31 informativas). Para cada vulnerabilidad la herramienta brinda algún tipo de solución.

Con Acunetix se escaneó al servidor Quipux con el fin de encontrar vulnerabilidades en el servidor ya que el servicio que proporciona este servidor es un servicio Web y Acunetix se especializa en encontrar vulnerabilidades en aplicaciones web. Los resultados fueron variados teniendo en cada nivel de riesgos vulnerabilidades de distintos tipos, el resultado final fue 390 vulnerabilidades altas, 262 vulnerabilidades

medias, 29 vulnerabilidades bajas y 3962 informativas. Los resultados obtenidos muestran que es importante que se realice un análisis de estas vulnerabilidades ya que podrían presentar potenciales riesgos para el servicio que ofrece este servidor, para ellos se debe empezar por las vulnerabilidades altas, de tal forma que se pueda determinar qué porcentaje de las mismas son falsos positivos y cuales son en verdad una amenaza para el servicio. Al analizar las vulnerabilidades altas se podrá tener claras cuáles son las medidas que se deben aplicar para mitigar los riesgos a lo mínimo posible. Después de hacer el análisis de las vulnerabilidades altas es recomendable que se realice un nuevo escaneo con esta herramienta ya que muchas de las vulnerabilidades medias se pueden solucionar al momento de resolver las vulnerabilidades altas.

Con McAfee se escaneó al servidor Quipux, pero se lo hizo en un ambiente totalmente controlado por la DGIP y con la realización y la supervisión de el mismo personal de la DGIP, por lo que no se obtuvo detallas de la ejecución de la prueba, pero sí de los resultados. Esta herramienta puede obtener vulnerabilidades en distintos campos como por ejemplo a nivel de aplicaciones web, a nivel de dominio, a nivel de red, etc. Para este caso solamente son tomados los resultados de las vulnerabilidades encontradas a nivel de aplicación web, estos resultados fueron los siguientes: 3 altas, 6 medias, 11 bajas y 16 informativas. Al igual que en el caso de Acunetix es importante que se analicen en primer lugar las vulnerabilidades altas para determinar si son falsos positivos o si representan un riesgo para el servidor, la diferencia de esta herramienta con Acunetix es que esta herramienta aparte de buscar las vulnerabilidades que existen también las explota, es por eso que en este caso se encuentran menos vulnerabilidades, pero es más probable que sean más serias y que representen un riesgo más alto para el servidor, por lo que se debe dar prioridad a los resultados obtenidos por esta herramienta.

2.3 VULNERABILIDADES A NIVEL FÍSICO DEL SERVIDOR

El Checklist correspondiente a la seguridad física, debido a que son 11 preguntas, se han establecido los siguientes niveles de seguridad de acuerdo al número de preguntas que se han contestado afirmativamente:

Nivel de Seguridad	# de preguntas afirmativas
Bajo	0-4
Medio	5-8
Alto	9-11

Tabla 2-5 - Resultados de las Vulnerabilidades a Nivel Físico[15]

De acuerdo a las respuestas obtenidas por parte de la institución, se tienen 8 respuestas afirmativas, por lo que el servidor Quipux tiene un nivel medio de seguridad. Las principales vulnerabilidades que se han encontrado, se listan a continuación:

- No se cuenta con un servidor similar al original como respaldo.
- No se cuenta con un proveedor en caso de que se necesite renovar el quipo
- No se realiza actualizaciones periódicas del equipo

2.4 EVALUACIÓN DE RIESGOS EN BASE A LOS RESULTADOS OBTENIDOS.

La Evaluación de Riesgos se va a realizar de forma parcial en base a la Metodología de Evaluación de Riesgos NIST que contempla los siguientes pasos:

1. Caracterización del sistema
2. Identificación de Amenazas
3. Identificación de vulnerabilidades
4. Controles vigentes
5. Determinación de la Probabilidad
6. Análisis del Impacto
7. Determinación del Nivel de Riesgo
8. Recomendaciones de Controles
9. Documentación de Resultados

Nota: Los pasos 2, 3, 4 y 6 pueden ser conducidos en paralelo después de que el paso 1 haya sido completado.

[15] Tabla elaborada por los autores, en base al checklist realizado sobre el servidor Quipux

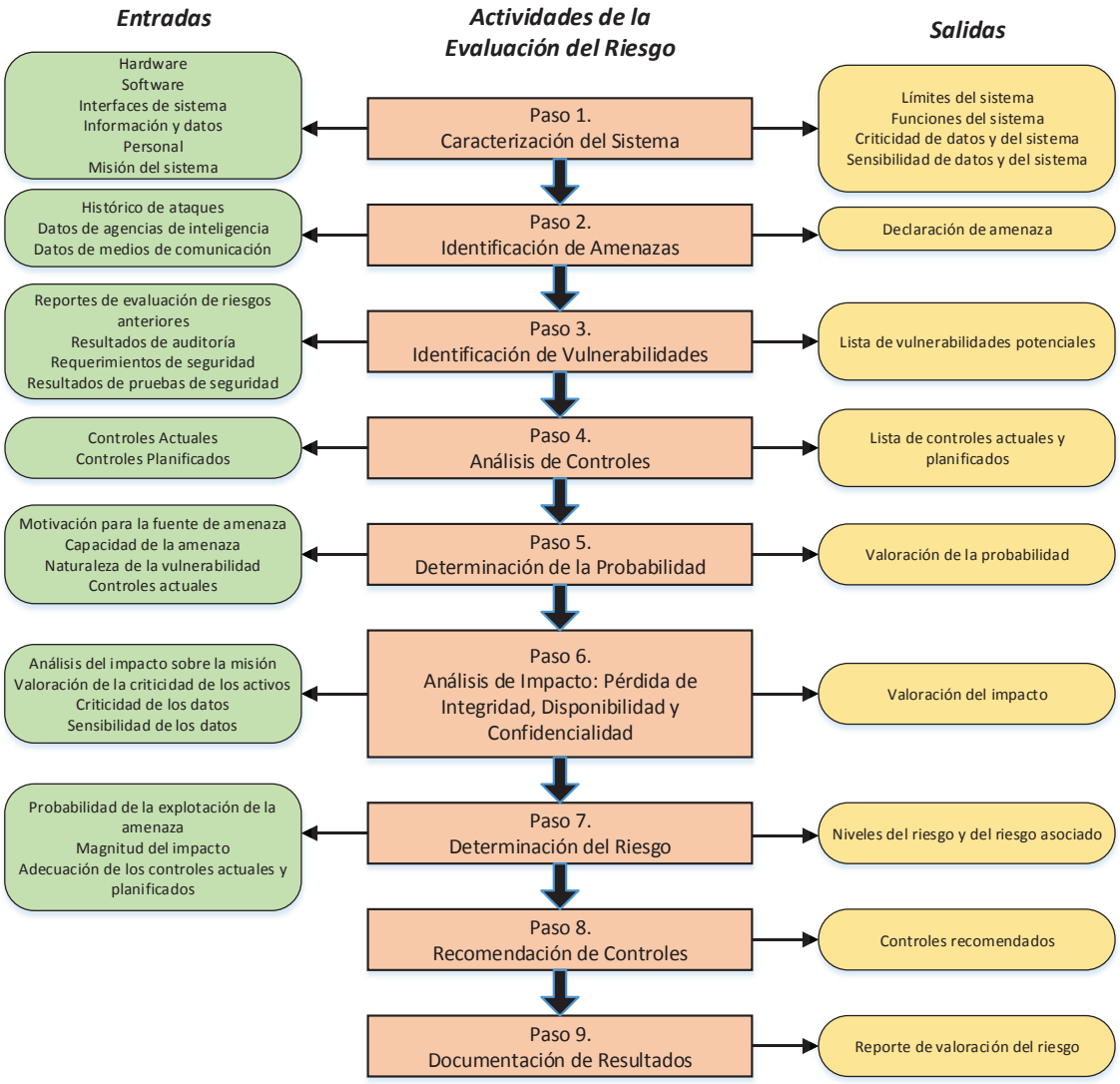

Figura 2-1 - Actividades de la Evaluación del Riesgo [21]

2.4.1 CARACTERIZACIÓN DEL SISTEMA

El activo de información seleccionado para la Evaluación de Riesgos se acordó en conjunto con la organización en una entrevista con el director de la DGIP y un oficial de seguridad de la organización, el activo de información seleccionado es el sistema Quipux, puesto que el mismo consiste en uno de los activos de información más crítico para la institución, tal como se lo indicó en el Capítulo I.

Se trata de un servidor con S.O Linux (CentOS), se encuentra ubicado en un lugar físico adecuado y cuenta con una alimentación de energía auxiliar. A dicho activo de

información solamente tiene acceso personal autorizado y cuenta con mantenimiento periódico.

2.4.2 IDENTIFICACIÓN DE AMENAZAS

2.4.2.1 Identificación de Riesgos

En base al análisis lógico y físico de la seguridad del servidor, se han identificado un total de 28 riesgos, el detalle de los mismos se encuentra en el Anexo 8

2.4.2.2 Identificación de Amenazas

En base a los riesgos que se identificaron en el paso anterior se han identificado amenazas por cada uno de estos riesgos, los cuales se listan en el Anexo 8.

2.4.3 IDENTIFICACIÓN DE VULNERABILIDADES

2.4.3.1 Identificación de Vulnerabilidades

En base a los riesgos y amenazas que se identificaron en el punto anterior se han identificado vulnerabilidades por cada uno de estos riesgos, los cuales se listan en el Anexo 8.

2.4.4 CONTROLES VIGENTES

Actualmente en la organización se manejan los controles que se muestran en la siguiente tabla con respecto a los riesgos identificados en el punto 2.4.2.1

#	Controles Vigentes
R1	Conocimiento técnico del administrador del servidor, Cuentan con un manual técnico del software
R2	Cuentan con un manual técnico del software
R3	Cuentan con un manual técnico del software
R4	No existen controles actuales
R5	Mantenimiento periódico del servidor
R6	Mantenimiento periódico del servidor
R7	Mantenimiento periódico del servidor

R8	Solo tiene acceso personal autorizado
R9	Mantenimiento periódico del servidor
R10	No existen controles actuales
R11	VPN, Firewall, IDS e IPS de la organización
R12	VPN, Firewall, IDS e IPS de la organización
R13	VPN, Firewall, IDS e IPS de la organización
R14	VPN, Firewall, IDS e IPS de la organización
R15	VPN, Firewall, IDS e IPS de la organización
R16	VPN, Firewall, IDS e IPS de la organización
R17	VPN, Firewall, IDS e IPS de la organización
R18	VPN, Firewall, IDS e IPS de la organización
R19	No cuenta con controles actuales
R20	No cuenta con controles actuales
R21	VPN, Firewall, IDS e IPS de la organización
R22	VPN, Firewall, IDS e IPS de la organización
R23	VPN, Firewall, IDS e IPS de la organización
R24	VPN, Firewall, IDS e IPS de la organización
R25	VPN, Firewall, IDS e IPS de la organización
R26	VPN, Firewall, IDS e IPS de la organización
R27	VPN, Firewall, IDS e IPS de la organización
R28	VPN, Firewall, IDS e IPS de la organización

Tabla 2-6 - Controles Vigentes para los Riesgos Encontrados[16]

Cabe destacar que los controles anteriores se identificaron a través de los checklist contestados por el personal de la organización así como también a los elementos identificados en su diagrama de red.

2.4.5 DETERMINACIÓN DE LA PROBABILIDAD

2.4.5.1 Consideraciones para evaluación de riesgos

a) Evaluación Cuantitativa del Riesgo:

Esta evaluación proporciona una medida aproximada de la magnitud del impacto, por lo general en términos financieros, así esta medida puede ser utilizada en el análisis costo beneficio de los controles recomendados. [21] La estimación del valor del riesgo está vinculado con la implementación de medidas

[16] Tabla elaborada por los autores, en base a los checklist y entrevistas realizadas dentro de la organización

numéricas, es decir que se realiza una evaluación numérica de la probabilidad, impacto y nivel de riesgo. Por lo general se lo hace después del análisis cualitativo. [22]

b) Evaluación Cualitativa del Riesgo:

Se trata de una evaluación de riesgos relativamente más fácil de realizar que la evaluación cuantitativa, además puede permitir la priorización de riesgos, y es útil en la identificación de áreas de vulnerabilidades que requieran atención inmediata; esta evaluación consiste en la clasificación relativa del riesgo, de forma que refleje desde el riesgo bajo hasta el riesgo alto, se basa en el juicio, la intuición y la experiencia en lugar de en los números y valores financieros. [21] Permite priorizar riesgos para un posterior análisis más profundo, además se enfoca en el establecimiento de contingencias para riesgos de alta amenaza de forma rápida y es efectiva en costos para establecer las contingencias adecuadas. [22]

Análisis de Riesgos	Métodos Cuantitativos	Métodos Cualitativos
Ventajas	Permiten la definición de las consecuencias de la ocurrencia de los incidentes en forma cuantitativa, lo que facilita la realización de un análisis de costos y beneficios durante la selección de las protecciones. Ofrecen una imagen más precisa del riesgo.	Permite colocar los riesgos encontrados según la prioridad. Permite la determinación de las áreas de mayor riesgo en corto tiempo y sin gastos mayores. El análisis es relativamente fácil y barato.
Desventajas	Las medidas cuantitativas dependen del alcance y precisión de la escala de medición. Los resultados del análisis pueden no ser precisos o incluso	Para la determinación de probabilidades y resultados no permite utilizar medidas numéricas. El análisis de costos y beneficios es más difícil durante la

	confusos. Los métodos normales deben ser enriquecidos en la descripción cualitativa (en la forma del comentario, la interpretación). El análisis llevado a cabo con la aplicación de esos métodos es generalmente más caro, exigiendo una mayor experiencia y herramientas avanzadas.	selección de las protecciones. La mayor parte de veces los resultados obtenidos tienen carácter general y aproximado.

Tabla 2-7 Ventajas y Desventajas Metodología Cuantitativa y Cualitativa [23]

Por ende para la Evaluación de los riesgos que han sido identificados se va a realizar en base a un enfoque cualitativo, el cual tiene como factores elementales la Probabilidad de que el riesgo se materialice y el Impacto que éste tendrá en la organización en este caso. [22]

Antes de iniciar con la evaluación de los riesgos se deben identificar las amenazas y vulnerabilidades de cada uno de ellos, lo cual se realizó en el punto 2.4.2.1 del presente documento.

2.4.5.2 Criterios para la valoración de la Probabilidad

Para la probabilidad se consideran los valores que se muestran en la siguiente tabla:

Probabilidad Baja	**1**	**Los controles vigentes son seguros y, hasta el momento, han proporcionado un nivel de protección adecuado. No se esperan incidentes nuevos en el futuro.**
Probabilidad Moderada	2	Los controles vigentes son moderados y, básicamente, han proporcionado un nivel suficiente de protección. Existe la posibilidad de que haya un incidente en el futuro.
Probabilidad Alta	3	Los controles vigentes son bajos o ineficaces. Existe una gran posibilidad de que haya incidentes así en el futuro.

Tabla 2-8 - Valoración de la Probabilidad [22]

2.4.6 ANÁLISIS DEL IMPACTO

2.4.6.1 Criterios para la valoración del Impacto

Por otro lado, el impacto se va a calcular de acuerdo a los valores que se muestran en la siguiente tabla:

Impacto Bajo	**1**	**La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la organización**
Impacto Medio	2	La pérdida de confidencialidad, disponibilidad o integridad causa gastos adicionales y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la organización.
Impacto Alto	3	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes e inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.

Tabla 2-9 - Valoración del Impacto [22]

2.4.7 DETERMINACIÓN DEL RIESGO

2.4.7.1 Criterios para el cálculo del nivel de riesgo

Para el cálculo del nivel de riesgo se multiplica el valor asignado al impacto y el asignado a la probabilidad.

2.4.7.2 Criterios para la aceptación de riesgos

De acuerdo a la metodología de Evaluación de riesgos antes mencionada, se definen como Riesgos Aceptables a aquellos riesgos que luego de ser evaluados tienen un nivel de riesgo con valores de 1, 2, 3 y 4. [22]

Por otro lado los Riesgos no aceptables son aquellos que luego de ser evaluados tienen un nivel de riesgo con valores de 6 y 9. Serán estos riesgos lo que serán tratados y para los cuales se establecerán controles. [22]

2.4.8 MATRIZ DE EVALUACIÓN DE RIESGOS

En la matriz que se muestra a continuación se determina la probabilidad de ocurrencia de cada una de las amenazas y vulnerabilidades identificadas en los puntos 2.4.2 y 2.4.3 respectivamente, y se analiza el impacto que cada una de ellas, esto se realiza en base a las consideraciones establecidas en los apartados 2.4.5 y 2.4.6.

A partir de los valores asignados tanto a la probabilidad como al impacto, se estableció el valor del nivel de riesgo en base al apartado 2.4.3.4. Además de que se han marcado en rojo los riesgos que no son aceptables y en naranja y amarillo los aceptables, de acuerdo al apartado anterior.

A continuación se muestra parte de la matriz de evaluación de riesgo, para ver la matriz completa ir al Anexo 11.

En la matriz se indica lo siguiente:

- Nombre del activo de información del que se está haciendo la evaluación del riesgo así como el nombre del propietario del activo de información.
- Amenaza y origen de la amenaza según el Anexo C de la norma NTE INEN-ISO/IEC 27005:2012, este origen puede ser:
    - Accidental: Se utiliza para todas las acciones humanas que pueden dañar accidentalmente los activos de información.
    - Deliberado: Se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de información.
    - Ambiental: Se utiliza para todos los incidentes que no se basa en las acciones humanas.
- Vulnerabilidad y tipo de vulnerabilidad según el Anexo D de la norma NTE INEN-ISO/IEC 27005:2012. Los tipos de vulnerabilidades puede ser:
    - Hardware: son todas las vulnerabilidades que pueden afectar al correcto funcionamiento del hardware del activo de información.

  - Software: vulnerabilidades enfocadas a los sistemas software que forman parte del activo de información.
  - Red: vulnerabilidades que afectan a la infraestructura de red en la que se encuentra el activo de información.
  - Personal: vulnerabilidades relacionadas con el personal cercano al activo de información que se está evaluando, principalmente las personas que están a cargo de la administración del mismo.
  - Lugar: este tipo de vulnerabilidades se relacionan con el lugar físico en el que se encuentra el activo de información.
  - Organización: vulnerabilidades de carácter organizativo y administrativo que afectan el correcto funcionamiento del activo de información.
- Los valores del impacto, probabilidad y nivel de riesgo antes del tratamiento.
- Los controles vigentes de la organización respecto a las vulnerabilidades.

Es importante acotar, que a continuación solo se presentan los riesgos calificados como bajos, dado que se firmó un acuerdo de confidencialidad con la institución, lo que nos impide mostrar los riesgos catalogados como medios y altos.

MATRIZ DE EVALUACIÓN DE RIESGOS										
#	**Nombre del activo de información**	**Propietario del activo de información**	**Origen de la Amenaza según la norma NTE INEN-ISO/IEC 27005:2012**	**Amenazas según la norma ISO 27005**	**Tipo de Vulnerabilidad según la norma NTE INEN-ISO/IEC 27005:2012**	**Vulnerabilidad**	**Impacto**	**Probabilidad**	**Riesgo**	**Controles Vigentes**
R1	Sistema Quipux	EPN-DGIP	Accidental	Mal funcionamiento del equipo. M al funcionamiento del software.	Software	No existe soporte técnico para el software utilizado	2	1	2	Conocimiento técnico del administrador del servidor, Cuentan con un manual técnico del software
R3	Sistema Quipux	EPN-DGIP	Accidental	Error en el uso	Software	Los mensajes de error del software del servidor no son claros	2	1	2	Cuentan con un manual técnico del software

R8	Sistema Quipux	EPN-DGIP	Accidental y deliberado	Abuso de derechos Procesamiento ilegal de datos Negación de acciones	Organización	No se lleva una bitácora con la información de las personas que acceden a los datos de los backups y las modificaciones que realizan	2	1	2	Solo tiene acceso personal autorizado

Tabla 2-10 - Modelo de la Matriz de Evaluación de Riesgos[17]

[17] Matriz de evaluación de riesgos elaborada por los autores, la cual para efectos de la tesis muestra solamente riesgos bajos y medios, para revisar la matriz completa, dirigirse al anexo correspondiente.

CAPÍTULO 3 DEFINICIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SERVIDOR QUIPUX DE LA DGIP

En esa sección se definirá el plan de gestión de seguridad de la información para el servidor Quipux de la DGIP, en primer lugar se definirá la organización de la documentación que será parte del SGSI en base a la norma NTE INEN-ISO/IEC 27001:2011, posteriormente se utilizará la información recopilada en las secciones anteriores, sobre el servidor Quipux, respecto a las vulnerabilidades físicas y lógicas encontradas, así como el análisis de riesgos, con lo que se procederá a hacer el tratamiento de riesgos y la selección de controles en base al anexo A de la norma NTE INEN-ISO/IEC 27001:2011.

Finalmente se realizará un análisis de restricciones y factibilidad para la aplicación del plan de gestión de la seguridad de la información.

3.1 ELABORACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SERVIDOR QUIPUX DE LA DGIP

Hasta este punto se tienen los requerimientos necesarios para el desarrollo del plan de gestión de seguridad de la información para el servidor Quipux de la DGIP, estos requerimientos han sido recogidos en base a la norma NTE INEN-ISO/IEC 27000:2012 la cual menciona en su sección 3.5 la teoría para el establecimiento monitoreo, mantenimiento y mejoramiento de un SGSI. A continuación se describe el enfoque del proceso para la gestión de seguridad de la información y la descripción de los entregables que conforman dicho plan.

3.1.1 ENFOQUE DEL PROCESO

El enfoque del proceso presentado en la familia de normas de la ISO 27000 se basa en el ciclo PDCA (por sus siglas en ingles Plan, Do, Check, Act) la siguiente figura muestra como un SGSI partiendo de los requisitos de seguridad establecidos por las

partes interesadas y a través de las acciones y procesos necesarios, producen los elementos de salida de seguridad de la información que responden a dichos requisitos y expectativas. [24]

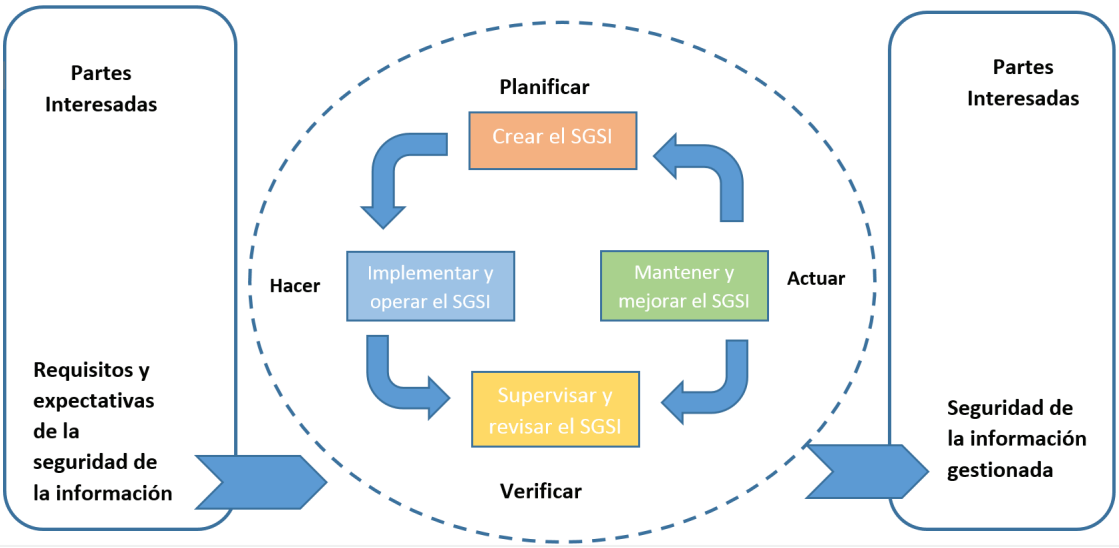

Figura 3-1 - Ciclo PDCA Relacionado con el SGSI [24]

- ***Planificar:*** Consiste en definir los objetivos, políticas, procesos y procedimientos del SGSI relevantes, para gestionar el riesgo y mejorar la seguridad de la información, en esta etapa de planificación se realiza el análisis de riesgos de seguridad de la información y la selección de controles adecuados para mitigar los riesgos que no son aceptados por la organización. Cabe destacar que hasta aquí llega el alcance de este proyecto la realización de las siguientes etapas del ciclo PDCA quedan a decisión de la organización, en este caso la DGIP.
- ***Hacer:*** Es la etapa de implantación y operación de los controles que fueron seleccionados en la etapa de planificación.
- ***Verificar:*** Es la etapa de evaluación del desempeño del SGSI e informar a los altos mandos de la organización.
- ***Actuar:*** En esta etapa se adopta medidas correctivas y preventivas en función del análisis realizado en la etapa de verificación con el objetivo de lograr el máximo rendimiento del SGSI y tener una mejora continua.

Debido a que este proyecto se enfoca solamente en el plan para un SGSI no se tomaron en cuenta las partes de implementación, supervisión y mantenimiento y mejoramiento de un SGSI, ya que esto se realiza cuando el SGSI está implementado en la organización.

Por lo tanto los puntos abarcados de la sección 3.5 de la norma INEN-ISO/IEC 27000:2012 y que se encuentran en las secciones anteriores de este documento son las siguientes:

- Descripción general.
- Identificación de requerimientos de seguridad de la información
- Evaluación de riesgos de la seguridad de la información
- Selección de controles de seguridad de la información

Estos son los puntos de partida para el desarrollo de un plan de gestión de seguridad de la información según la norma INEN-ISO/IEC 27003:2012, la cual es una guía de implementación para el SGSI.

Las secciones de la norma INEN-ISO/IEC 27003:2012 necesarias para la elaboración del plan del SGSI son las siguientes:

1. Obtención de la aprobación de la dirección para iniciar un proyecto de SGSI
2. Definir el alcance, límites y políticas del SGSI
3. Realizar el análisis de los requerimientos de la seguridad de la información
4. Realizar la evaluación del riesgo y la planificación del tratamiento del riesgo
5. Diseño del SGSI

La siguiente figura muestra las cinco fases de la planificación del proyecto del SGSI de acuerdo a las normas NTE INEN-ISO/IEC y a los principales documentos de salida: [25]

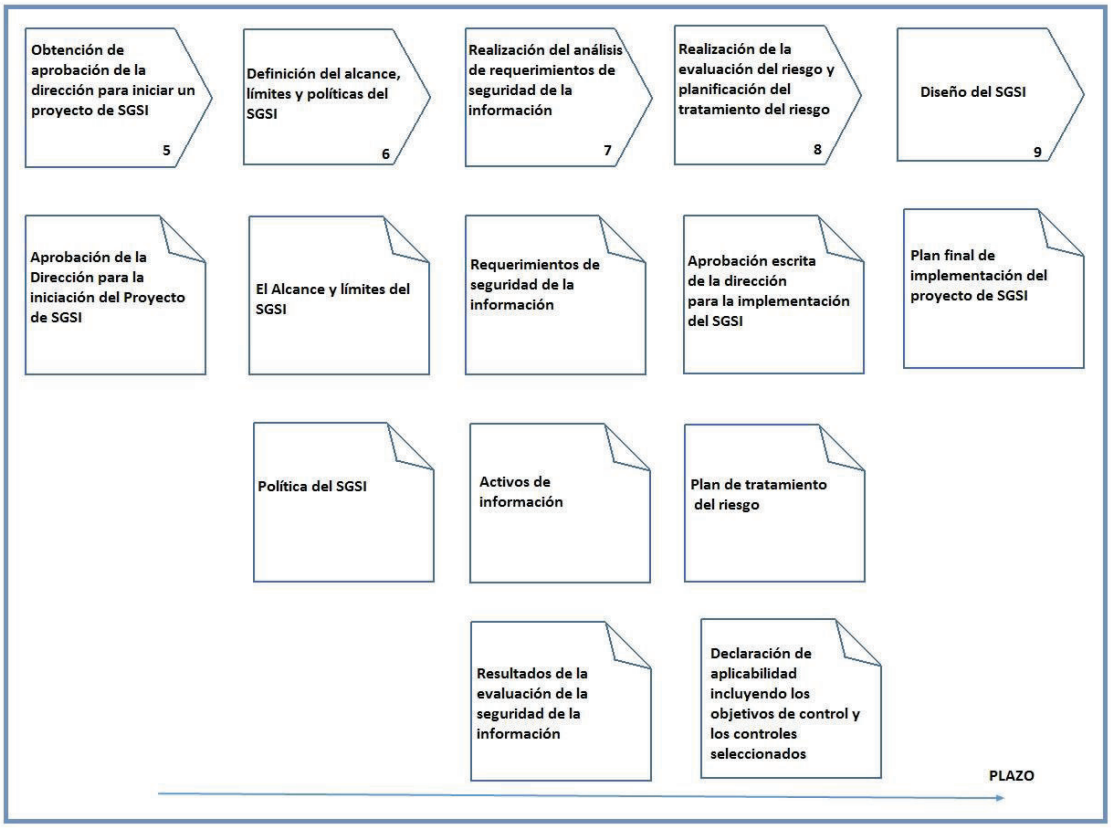

Figura 3-2 - Fases del Proyecto del SGSI [25]

3.1.2 ORGANIZACIÓN DE LA DOCUMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL SERVIDOR QUIPUX DE LA DGIP

Para manejar y procesar la información del SGSI del servidor Quipux de la DGIP se utilizará la siguiente organización:

SGSI Servidor Quipux – DGIP:

- Documentos Habilitantes
- Alcance del SGSI
    - Entradas
    - Salidas
- Plan de evaluación y tratamiento de riesgos
- Controles

- Plan del proyecto del SGSI

Cabe recalcar que los documentos que son parte del SGSI pueden ser físicos y/o digitales, por lo que sea cual sea el caso, se deberá dar el uso y mantenimiento apropiado de los mismos, por ejemplo si se los tiene de forma física, es necesario que cuenten con la protección y la organización necesaria, ubicándolos en un lugar apropiado y que solamente tengan acceso a ellos las personas con los permisos necesarios, por otro lado si se los mantiene en forma digital se puede hacer uso de gestores documentales como: Alfresco, Athento, Nuxeo, etc. Es necesario que se creen políticas de seguridad para la creación, mantenimiento y eliminación de los documentos pertenecientes al SGSI.

A continuación se muestra el mapeo de las secciones de la norma INEN-ISO/IEC 27003:2012 con la organización documental definida y los entregables.

1. Obtención de la aprobación de la dirección para iniciar un proyecto de SGSI
    a. Documentos habilitantes
        i. Carta de Solicitud.pdf
        ii. Carta de Compromiso de la Dirección.pdf
        iii. Documento de Caso del Negocio.docx
        iv. Documento de Propuesta del Proyecto.docx
    b. Alcance del SGSI
        i. Entradas
            1. Documento de Caracterización del Negocio.docx
            2. Documento de Objetivos y Metas con Respecto al SGSI.docx
            3. Requerimientos Contractuales, Legales y Regulatorios.docx
2. Definir el alcance, límites y políticas del SGSI
    a. Alcance del SGSI
        i. Salidas
            1. Documento de Alcance y Límites del SGSI.docx
3. Realizar el análisis de los requerimientos de la seguridad de la información
    a. Alcance del SGSI
        i. Salidas

1. Documento de Requisitos de Seguridad de la Información.docx

4. Realizar la evaluación del riesgo y la planificación del tratamiento del riesgo
    a. Plan de evaluación y tratamiento de riesgos
        i. Documento de Evaluación y Tratamiento de Riesgos.docx
        ii. Formato de Matriz de Evaluación de Riesgos.xlsx
        iii. Formato de Matriz de Tratamiento de Riesgos.xlsx
        iv. Matriz de Evaluación de Riesgos.xlsx
        v. Matriz de Tratamiento de Riesgos.xlsx
    b. Controles
        i. A.5 Políticas de Seguridad
            1. Políticas de Seguridad de la Información
                a. Documento de Política del SGSI.docx
        ii. A.6 Aspectos Organizativos
            1. A.6.1 Aspectos Organizativos
                a. Documento de Roles y Responsabilidades.docx
        iii. A.7 Gestión de Activos
            1. A.7.2 Clasificación de la Información
                a. Política para el Manejo de Información Clasificada.docx
                b. Política para control de Documentos y Registros.docx
        iv. A.12 Adquisición, Desarrollo y Mantenimiento de los SI
            1. A.12.6 Gestión de la Vulnerabilidad Técnica
                a. Estado Actual
                    i. Informe Técnico.docx
                    ii. Resumen Ejecutivo.docx
                    iii. Presentación.pptx
                b. Tratamiento del Riesgo
                    i. Plan de Tratamiento del Riesgo.docx
        v. A.13 Gestión de Incidentes de Seguridad de la Información
            1. Procedimiento para Gestión de Incidentes.docx
5. Diseño del SGSI
    a. Plan del proyecto del SGSI

3.1.3 ESPECIFICACIÓN DE LOS ENTREGABLES

Cada uno de los documentos generados en el proceso de elaboración del plan de gestión de la seguridad de la información, tienen una finalidad y a continuación se detalla cada documento junto con su descripción y el anexo al que debe referirse para poder ver el documento.

3.1.3.1 Carta de solicitud

Este documento empieza el proceso de la elaboración del plan del SGSI y es de suma importancia debido a que no se puede empezar con el desarrollo del plan sin el consentimiento de la organización, este documento debe contener la especificación de lo que se quiere realizar y como se lo va a realizar y debe ser dirigido preferiblemente a la persona que tenga el más alto rango en la organización, pudiendo ser el gerente general o el director; en todo caso se puede dirigir a personas de menor rango siempre y cuando el gerente o director tenga conocimiento de lo que se va a realizar.

El formato de esta carga depende de cada empresa pero los datos principales que debe tener son los siguientes:

- De: Nombre y cargo de la o las personas que redactan la solicitud.
- Para: Nombre y cargo de la o las personas que reciben la solicitud.
- Asunto: Es el tema que se trata en la solicitud, en este caso el desarrollo del plan de un SGSI
- Fecha: Fecha en la que se redacta la solicitud.
- Cuerpo de la solicitud: Contiene todo el mensaje de solicitud, especificando que es lo que se quiere hacer y como se lo va a hacer
- Firma: Firma de la o las personas que redactan la solicitud.

La carta de solicitud de este proyecto se encuentra en el Anexo 1.

3.1.3.2 Carta de Compromiso de la Dirección.

La carta de Compromiso de la Dirección se genera a partir de la Carta de Solicitud y básicamente contiene la aprobación, por escrito, para la ejecución de lo solicitado, esta Carta de Compromiso de la Dirección puede contener limitaciones expuestas por la dirección de la organización, con lo cual los solicitantes decidirán si continuar o no con la ejecución del desarrollo del plan del SGSI.

Es importante que en la carta de compromiso se especifique claramente el apoyo y la participación que va a tener la organización con el desarrollo del proyecto, además debe estar firmada necesariamente por alguien con un cargo alto en la organización.

La carta de compromiso de la dirección para este proyecto se encuentra en el Anexo 2.

3.1.3.3 Documento de Caracterización del Negocio.

El objetivo de este documento es caracterizar a la organización o negocio en el que se va a realizar el plan del SGSI, esta caracterización consiste en detallar la estructura interna de la organización con lo que se tendrá un marco de acción para el desarrollo del plan.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Sección 5.2 de la norma NTE-ISO-IEC 27003:2012
- Misión, Visión y objetivos del negocio de la Dirección de Gestión de la Información y Procesos de la Escuela Politécnica Nacional
- Objetivos estratégicos de la organización
- Diagrama lógico y físico de la Red

Las secciones que debe contener este documento son las siguientes:

- Caracterización de la organización.

- Misión: es la misión que está activa actualmente en la organización esta debe ser obtenida directamente de la organización, en caso de que no exista dejar esta sección vacía
- Visión: es la visión que está activa actualmente en la organización esta debe ser obtenida directamente de la organización, en caso de que no exista dejar esta sección vacía.
- Objetivos de la dirección: se debe especificar cuáles son los objetivos generales y específicos de la empresa.
- Orgánico Funcional: se debe incluir el diagrama del orgánico funcional actualmente activo en la organización.
- Infraestructura de la organización
    - Ubicación física de la organización: en esta parte definir la ubicación geográfica de la organización en donde se va a realizar el proyecto, si es posible incluir un croquis.
    - Diagrama lógico de red: presentar el diagrama lógico de red de la organización, esto dependerá de los permisos que haya otorgado la empresa para el acceso a esta información, en caso de no contar con los permisos necesarios dejar esta sección vacía.
    - Análisis de la infraestructura: se debe realizar un análisis de la infraestructura de la organización en función de la seguridad de la información.
- Lista de activos de la organización: esta sección debe contener la lista de activos tanto de software como hardware que tiene la organización.

El documento de caracterización del negocio para este proyecto se encuentra en el Anexo 3.

3.1.3.4 Documento de Objetivos y Metas con Respecto al SGSI.

El objetivo de este documento es el de especificar los objetivos y metas del negocio en función de la seguridad de la información para realizar el plan de implementación

de un SGSI utilizando el estándar NTE INEN-ISO/IEC 27001:2011 y estándares de apoyo a esta norma.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Sección 5.2 de la norma NTE-ISO-IEC 27003:2012
- Misión, Visión y objetivos del negocio de la Dirección de Gestión de la Información y Procesos de la Escuela Politécnica Nacional.
- Objetivos estratégicos de la organización
- Lista de requerimientos legales, regulatorios y contractuales.
- Diagrama lógico y físico de la Red

Las secciones que debe tener este documento son las siguientes:

- Objetivos y metas del negocio con respecto al SGSI.
    - Objetivos: se debe especificar los objetivos que tiene el negocio con respecto al SGSI.
    - Metas: se debe especificar cuáles son las metas que se quiere lograr después de terminado el proyecto.

El documento de objetivos y metas con respecto al SGSI para este proyecto se encuentra en el Anexo 4.

3.1.3.5 Requerimientos Contractuales, Legales y Regulatorios.

El documento de Requerimientos Contractuales, Legales y Regulatorios, contiene la información relacionada con las leyes y requerimientos legales que se requiere para la implementación del SGSI en la organización, es importante porque en base a este se realizara los límites y el alcance del SGSI y está presente en todo el proceso del plan del SGSI.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Sección 5.2 de la norma NTE-ISO-IEC 27003:2012

- Lista de requerimientos legales, regulatorios y contractuales.

Las secciones que debe contener este documento son las siguientes:

- Requerimientos regulatorios y su impacto en el SGSI
    - Requerimientos regulatorios externos
        - Impacto de las regulaciones externas en el SGSI
    - Requerimientos regulatorios internos
        - Impacto de las regulaciones internas en el SGSI

El documento de los requerimientos contractuales, legales y regulatorios para este proyecto se encuentra en el Anexo 5.

3.1.3.6 Documento de Alcance y Límites del SGSI.

El objetivo de este documento es el de definir el alcance y los límites del SGSI desde el punto de vista organizacional, tecnológico, de información y comunicación y físico.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Guía de implementación del sistema de gestión de la seguridad de información NTE-ISO-IEC 27003:2012 cl. 6.2, 6.3 y 6.4.
- Plan de proyecto del SGSI (Caso del Negocio y Plan Inicial del proyecto del SGSI)

Las secciones que debe tener este documento son las siguientes:

- Alcance organizacional del SGSI
    - Limites organizacionales para el SGSI
    - Funciones de las áreas incluidas dentro del alcance del SGSI
    - Estructura de las áreas incluidas dentro del alcance del SGSI
    - Procesos y responsabilidades organizacionales
    - Información intercambiada dentro del alcance
    - Información intercambiada a través de los límites
    - Jerarquía para la toma de decisiones

- Alcance tecnológico, de información y comunicación del SGSI
    - Descripción de infraestructura de comunicaciones, hardware y software que maneja la organización
        - Infraestructura de las comunicaciones
        - Software dentro de los límites organizacionales
        - Hardware de las TIC requerido por las redes, aplicaciones o sistemas de producción
        - Roles y responsabilidades relativas al SGSI y al uso de las TIC
    - Límites y alcance de las TIC para el SGSI
        - Límites de las TIC para el SGSI
        - Justificación de la exclusión de las TIC bajo el control de la organización
    - Información intercambiada dentro del alcance
    - Información intercambiada a través de los límites
- Alcance físico y ubicación del SGSI
    - Descripción de las funciones o procesos considerando su ubicación física y la medida en que la organización los controla.
    - Instalaciones especiales que contienen o almacena hardware de las TIC o datos dentro del alcance

El documento de alcance y límites del SGSI para este proyecto se encuentra en el Anexo 6.

3.1.3.7 Documento de Requisitos de Seguridad de la Información.

El objetivo de este documento es el de definir los requisitos de seguridad de la información utilizando para ello la lista de activos de información y la clasificación de procesos/servicios identificados dentro del Alcance del SGSI. Este documento se aplica a todo el proceso de planeación del SGSI, puesto que contiene los requisitos de seguridad de la información sobre las que se debe diseñar el SGSI para su posterior implementación.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Guía de implementación del sistema de gestión de la seguridad de información NTE-ISO-IEC 27003:2012 cl. 7.2.
- Documento de Alcance y Límites del SGSI
- Plan de proyecto del SGSI (Caso del Negocio y Plan Inicial del proyecto del SGSI)

Las secciones que debe tener este documento son las siguientes:

- Requisitos de seguridad de la información para el SGSI
    - Procesos, funciones, ubicaciones, sistemas de información y redes de comunicación principales
        - Procesos Principales
        - Funciones Principales
        - Ubicaciones Principales
        - Sistemas de información Principales
        - Redes de comunicación Principales
    - Activos de información de la organización
    - Clasificación de los procesos/activos críticos
        - Procesos Críticos
        - Activos Críticos
    - Requerimientos de seguridad de la información derivados de los requerimientos legales, regulatorios, y contractuales de la organización
        - Requerimientos Regulatorios
        - Impacto de las Regulaciones en el SGSI
        - Requerimientos de Seguridad de la información
    - Lista de vulnerabilidades públicamente conocidas
    - Requerimientos de capacitación y educación sobre seguridad de la información

El documento de requisitos de seguridad de la información para este proyecto se encuentra en el Anexo 7.

3.1.3.8 Documento de Evaluación y Tratamiento de Riesgos.

El objetivo de este documento es el de explicar la metodología seleccionada para la realización de la evaluación de riesgos así como del tratamiento de los riesgos identificados.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Anexo A de la norma NTE INEN-ISO/IEC 27001:2011
- Anexo C de la norma NTE INEN-ISO/IEC 27005
- Anexo D de la norma NTE INEN-ISO/IEC 27005
- CISM Review Manual 2013. Secciones de la 2.10 a la 2.17

Las secciones que debe tener este documento son las siguientes:

- Evaluación de Riesgos
    - Caracterización del Sistema
    - Identificación de Amenazas
        - Identificación de Riesgos
        - Identificación de Amenazas
    - Identificación de Vulnerabilidades
    - Controles Vigentes
    - Determinación de la Probabilidad
        - Consideraciones para evaluación de riesgos
        - Criterios para la valoración de la Probabilidad
    - Análisis del Impacto
        - Criterios para la valoración del Impacto
    - Determinación del Riesgo
        - Criterios para el cálculo del nivel de riesgo
        - Criterios para la aceptación de riesgos
        - Matriz de Evaluación de Riesgos
    - Recomendaciones de Controles
- Tratamiento de Riesgos
    - Opciones de Tratamiento de Riesgos

- Opción de Tratamiento Seleccionado
- Matriz de Tratamiento de Riesgos

El documento de evaluación y tratamiento de riesgos para este proyecto se encuentra en el Anexo 8.

3.1.3.9 Formato de Matriz de Evaluación de Riesgos.

Este formato es una herramienta para la evaluación de riesgos, debe estar vacía para que en cualquier momento se pueda hacer una copia y empezar un nuevo proceso de evaluación de riesgos.

El formato de esta matriz se encuentra en el Anexo 9.

3.1.3.10 Formato de Matriz de Tratamiento de Riesgos.

Este formato es una herramienta para el tratamiento de los riesgos encontrados, debe estar vacía para que en cualquier momento se pueda hacer una copia y empezar un nuevo proceso de tratamiento de riesgos.

El formato de esta matriz se encuentra en el Anexo 10.

3.1.3.11 Matriz de Evaluación de Riesgos.

La Matriz de Evaluación de Riesgos muestra todos los riesgos identificados en un análisis previo y muestra la amenaza, la vulnerabilidad y la calificación del riesgo de acuerdo a la metodología de evaluación de riesgo seleccionada, este documento sirve como base para realizar el tratamiento de riesgos.

El formato de esta matriz se encuentra en el Anexo 11.

3.1.3.12 Matriz de Tratamiento de Riesgos.

Esta Matriz es parecida a la matriz de evaluación de riesgos agregando el campo de controles para realizar el tratamiento de riesgos y una comparación para saber el estado del riesgo antes y después del tratamiento del riesgo.

El formato de esta matriz se encuentra en el Anexo 12.

3.1.3.13 Documento de Caso del Negocio.

El objetivo de este documento es el de definir el Caso del Negocio, es decir ayuda a determinar si vale la pena o no implementar el plan del SGSI en base a la factibilidad tecnológica, humana y operativa utilizando el estándar NTE-ISO-IEC 27003:2012.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Guía de implementación del sistema de gestión de la seguridad de información NTE-ISO-IEC 27003:2012 cl. 5.4
- Documento de roles y responsabilidades.
- Documento de Caracterización del Negocio en función de los Objetivos de Seguridad de la Información (Alcance Preliminar)

Las secciones que debe tener este documento son las siguientes:

- Caso del negocio
    - Metas y objetivos específicos del SGSI
        - Objetivos Específicos
        - Metas específicas
    - Beneficio para la organización con la implementación del SGSI
    - Alcance preliminar del SGSI
        - Roles involucrados en el SGSI
        - Activos Críticos
        - Procesos Críticos

        - Ubicación
        - Interacción entre roles involucrados
    - Visión del proyecto SGSI
    - Plan inicial de implementación
        - WBS (Work Breakdown Structure) del proyecto
        - Recursos requeridos
        - Recursos Humanos
        - Recursos Operativos
        - Recursos Tecnológicos
        - Recursos Totales
        - Cronograma con hitos clave
    - Roles y responsabilidades definidas
    - Consideraciones de implementación
    - Factores críticos de éxito
    - Beneficios cuantificados

El documento de caso del negocio para este proyecto se encuentra en el Anexo 13.

3.1.3.14 Documento de Propuesta del Proyecto.

El objetivo de este documento es el de definir la Propuesta de Proyecto del SGSI utilizando el estándar NTE-ISO-IEC 27003:2012.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Guía de implementación del sistema de gestión de la seguridad de información NTE-ISO-IEC 27003:2012 cl. 5.4
- Documento de roles y responsabilidades.
- Documento de Caracterización del Negocio en función de los Objetivos de Seguridad de la Información (Alcance Preliminar)

Las secciones que debe tener este documento son las siguientes:

- Propuesta del SGSI

- Hitos
- Importancia de cada hito clave
- Lineamientos generales de cada hito
    - Evaluación de riesgos y Planificación del Tratamiento de Riesgos
    - Implementación del SGSI
    - Ejecución de Auditorías internas
    - Revisión por parte de la dirección

El documento de propuesta des proyecto para este proyecto se encuentra en el Anexo 14.

3.2 SELECCIÓN DE CONTROLES EN BASE AL ANEXO A DE LA NORMA NTE INEN-ISO/IEC 27001:2011

La selección de controles se realiza en base a los riesgos encontrados después del análisis físico y lógico del activo de información seleccionado, en este caso todos los controles deben ser aplicables al servidor Quipux de la DGIP en base al análisis de riesgos realizado en la sección 2.4.

A continuación se realiza el tratamiento de riesgos junto con la selección de controles.

3.2.1 TRATAMIENTO DE RIESGOS

El tratamiento de los riesgos consiste en establecer los controles necesarios con el objetivo de mitigar los riesgos descritos en la sección anterior. Para realizar el tratamiento de riesgos se pueden usar las siguientes opciones:

1. Elección de control o controles de seguridad del Anexo A de la norma NTE INEN-ISO/IEC 27001:2011 u otros controles de seguridad.
2. Transferencia de los riesgos a terceros.

3. Evitar el riesgo interrumpiendo una actividad comercial si la ganancia que se obtiene de dicha actividad es menor que el mismo riesgo, transferir ese tipo de actividades a terceros.
4. Aceptación del riesgo: esta opción solamente está permitida si la aplicación de otros tratamientos supera los costos producidos por el impacto en el caso de que se materializara el riesgo.

En este caso para el tratamiento de los riesgos no aceptables, se seleccionó la primera opción ya que ésta nos permite realizar una nueva evaluación de los riesgos después de haber aplicado los controles adecuados para el tratamiento de los mismos, es decir que nos permite verificar la efectividad de los controles al tratar de hacer el riesgo aceptable para la organización.

3.2.2 MATRIZ DE TRATAMIENTO DEL RIESGO Y SELECCIÓN DE LOS CONTROLES DE SEGURIDAD ADECUADOS DE ACUERDO A LA NORMA NTE INEN-ISO/IEC 27001:2011

En base a los resultados obtenidos en la Matriz de Evaluación de Riesgos que es muestra en el punto 2.4.8, se han seleccionado ciertos controles que permitirán disminuir el valor de la probabilidad y del impacto de los riesgos que han sido considerados no aceptables, es decir los riesgos cuyo riesgo es igual a 3.

En la matriz se indica lo siguiente:

- Los valores del impacto, probabilidad y nivel de riesgo antes del tratamiento.
- Los controles seleccionados para el tratamiento.
- Los valores del impacto, probabilidad y nivel de riesgo después del tratamiento.
- Con la implementación de los controles seleccionados, lo que se busca es hacer a los riesgos aceptables para la organización.

A continuación se muestra parte de la matriz de tratamiento de riesgo, para ver la matriz completa dirigirse al Anexo 12.

#	Nombre del activo de información	Propietario del activo de información	Amenaza	Vulnerabilidad	Antes del Tratamiento				Tratamiento	Después del Tratamiento		
					Impacto	Probabilidad	Riesgo	Opción (1,2,3,4)	Control (si opción =1)	Impacto	Probabilidad	Riesgo
R2	Sistema Quipux	EPN-DGIP	Mal funcionamiento del software. Incumplimiento en el mantenimiento del software. Abuso de los derechos	No se realizan revisiones periódicas para evaluar el funcionamiento del software	3	2	6	1	A.7.1.1 Propiedad de los activos A.7.1.3 Uso aceptable de los activos A.8.1.1 Funciones y responsabilidades A.8.1.2 Investigación de antecedentes A.8.1.3 Términos y condiciones de contratación A.8.2.1 Responsabilidad de la dirección A.8.3.1 Responsabilidad del cese o cambio A.8.3.3 Devolución de activos A.8.3.3 Retirada de los derechos de acceso A.9.2.1 Emplazamiento y protección de equipos A.9.2.4 Mantenimiento de los equipos A.10.2.1 Provisión de servicios A.12.4.1 Control del software en explotación A.13.1.2 Notificación de los puntos débiles de seguridad A.13.2.3 Recopilación de evidencias A.15.2.1 Cumplimiento de las políticas y normas de seguridad	2	1	2

Tabla 3-1 - Modelo de la Matriz de Tratamiento del Riesgo[18]

[18] Matriz de tratamiento del riesgo, elaborada por los autores en base a los resultados obtenidos en la matriz de evaluación del riesgo.

3.2.3 MATRIZ DE APLICABILIDAD DE LOS CONTROLES

La aplicabilidad o exclusión de los distintos controles del Anexo A de la norma NTE INEN-ISO/IEC 27001:2011 debe ser respectivamente justificada. A continuación se presenta la justificación de los controles de los dos primeros objetivos de control (A.5 Política de seguridad y A.6 Aspectos organizativos de la seguridad de la información), para observar la matriz completa dirigirse al Anexo 23 la cual contiene la respectiva justificación de la aplicabilidad o no aplicabilidad de todos los controles.

En esta matriz la primera columna pertenece al Numeral “A.5.1.1” del control, la segunda describe el enunciado del control “Documento de política de seguridad de la información”, en la tercera se coloca “A” si el control aplica o “NA” si el control no aplica.

Matriz de Aplicabilidad de los Controles del Anexo A de la ISO NTE INEN-ISO/IEC 27001:2011			
Numeral	**Requisito NTE INEN-ISO/IEC 27001:2011**	**A/NA**	**Razones para la selección**
A.5	**Política de seguridad**		
A.5.1	**Política de seguridad de la información**		
A.5.1.1	Documento de política de seguridad de la información	A	Se aplica dado que es el documento que contiene la política general de seguridad de información, así como el compromiso de la dirección con la misma, dicho documento tiene que ser socializado tanto con partes externas como con las partes internas.
A.5.1.2	Revisión de la política de seguridad de la información	A	Se aplica puesto que permitiría examinar la política de seguridad de la información en caso de que ocurran cambios significativos dentro de la organización, con el fin de que la política esté acorde con los objetivos del negocio.
A.6	**Aspectos organizativos de la seguridad de la información**		
A.6.1	**Organización interna**		

A.6.1.1	Compromiso de la Dirección con la seguridad de la información	A	Se aplica ya que sin el apoyo de la dirección cualquier intención de mantener la seguridad de la información solo quedaría en eso, sin el apoyo de las autoridades es muy difícil lograr que las distintas políticas de seguridad cumplan con su objetivo dentro de la organización.
A.6.1.2	Coordinación de la seguridad de la información	A	Se aplica a causa de que la coordinación de la seguridad de la información permite involucrar tanto a mandos altos, medios y operacionales en las distintas actividades que conlleva la seguridad de la información, apoyando así al cumplimiento de la política de la información.
A.6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	A	Se aplica debido a que permitiría establecer distintos responsables de la seguridad de la información, logrando de cierta forma la protección de activos de información, pues son quienes responderán en caso de que ocurra algún tipo de incidente de seguridad de información.
A.6.1.4	Proceso de autorización de recursos para el tratamiento de la información	A	Se aplica porque para ciertos casos para mantener la seguridad de la información se utilizan nuevos recursos para tratar la información, dichos recursos deberían ser utilizados de forma adecuada y ser autorizados por parte de la dirección.
A.6.1.5	Acuerdos de confidencialidad	A	Si bien es cierto la organización cuenta con acuerdos de confidencialidad para la utilización de la información, este control se aplica porque dichos acuerdos deberían ser revisados regularmente procurando que estén de acuerdo con los objetivos y metas del negocio.
A.6.1.6	Contacto con las autoridades	A	Se aplica pues en caso de que exista algún tipo de incidente de seguridad dentro de la organización, la misma debería ponerse en contacto con las autoridades pertinentes para que se establezcan sanciones en caso de que se haya incumplido la ley.
A.6.1.7	Contacto con grupos de especial interés	A	Se aplica puesto que permitiría mantener contacto con grupos de interés especializados en seguridad de la información, consiguiendo intercambiar distinta información respecto a nuevas tecnologías así como amenazas, vulnerabilidades, etc.

A.6.1.8	Revisión independiente de la seguridad de la información	A	Es importante que se revise las distintas políticas y mecanismos de seguridad de la información y más aún si es realizada por una parte independiente, esto posibilitaría que se evalúe la idoneidad de las mismas así como que se encuentren funcionando de forma adecuada.
A.6.2	**A Terceros**		
A.6.2.1	Identificación de los riesgos derivados del acceso de terceros	NA	Este control no es aplicable puesto que ninguno de los riesgos identificados está relacionado con procesos de negocio que requieran de terceros.
A.6.2.2	Tratamiento de la seguridad en la relación con los clientes	NA	Este control no es aplicable puesto que ninguno de los riesgos identificados está relacionado con el acceso de los clientes de la organización a los activos o a la información de la misma.
A.6.2.3	Tratamiento de la seguridad en contratos con terceros	NA	Si bien es importante, manejar con cuidado los contratos que se firmen con terceros con respecto al acceso, procesamiento, comunicación o gestión de la información de la organización, en este caso este tipo de contratos no influyen en los riesgos identificados.

Tabla 3-2 - Matriz de Aplicabilidad de los Controles del Anexo A de la norma NTE INEN-ISO/IEC 27001:2011[19]

3.2.4 ESPECIFICACIÓN DE LAS POLÍTICAS A SER DESARROLLADAS PARA ESTE PROYECTO

Después de realizar la aplicabilidad de los controles se puede empezar a realizar políticas que permitan solventar los controles que son aplicables en este caso. A continuación se presenta la especificación de las políticas que servirán como base para empezar con la implementación del SGSI en la organización, cabe recalcar que estas son solamente las políticas iniciales que se pueden usar antes de la implementación del SGSI después se puede generar todas las políticas que atenderán a todos los controles aplicables seleccionados.

[19] Matriz elaborada por los autores, la cual contiene la aplicabilidad o no de cada control del anexo A de la NTE INEN-ISO/IEC 27001:2011.

3.2.4.1 Documento de Política del SGSI.

El objetivo de este documento es el de desarrollar la política del SGSI y obtener la aprobación de la dirección de la organización utilizando el estándar NTE INEN-ISO/IEC 27001:2011 y estándares de apoyo a esta norma.

Este documento es parte del control A.5 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Sección 6.6 de la norma NTE INEN-ISO/IEC 27003:2012
- Sección 7 de la norma NTE INEN-ISO/IEC 27005:2012
- Documento de Alcance y límites del SGSI
- Documento de Plan de Proyecto del SGSI (Caso del Negocio y Propuesta de Proyecto del SGSI)

Las secciones que debe tener este documento son las siguientes:

- Objetivos del SGSI
    - Enfoque general
    - Guía de acción para lograr los objetivos del SGSI
- Requerimientos regulatorios relacionados con el SGSI
    - Requerimientos regulatorios externos
    - Requerimientos regulatorios internos
- Contexto de la gestión de riesgos dentro de la organización
    - Consideraciones generales
    - Criterios de la evaluación de riesgos
    - Alcance y límites de la gestión de riesgos
    - Organización para la gestión de riesgo de la seguridad de la información
        - Partes interesadas
        - Relaciones entre la organización y las partes interesadas:
        - Rutas para escalar decisiones

    - Registros que deben ser conservados
- Responsabilidades de la alta dirección en relación al SGSI

El documento de política del SGSI para este proyecto se encuentra en el Anexo 15.

3.2.4.2 Documento de Roles y Responsabilidades.

El objetivo de este documento es el de especificar los roles y responsabilidades que tiene el SGSI utilizando el estándar NTE INEN-ISO/IEC 27001:2011 y estándares de apoyo a esta norma.

Este documento es parte del control A.6.1 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Guía de implementación del sistema de gestión de la seguridad de información NTE INEN-ISO/IEC 27003:2012 cl. 5.3.2
- Documento de Caracterización del Negocio en función de los Objetivos de Seguridad de la Información

En este documento se debe definir funciones y responsabilidades para el alcance preliminar del SGSI.

El documento de política del SGSI para este proyecto se encuentra en el Anexo 16.

3.2.4.3 Política para el Manejo de Información Clasificada.

El objetivo de este documento es el de especificar las directrices de clasificación, etiquetado y manejo de la información para de esta forma asegurar que la información recibe un nivel adecuado de protección, utilizando el estándar NTE INEN-ISO/IEC 27001:2011 y estándares de apoyo a esta norma.

Este documento es parte del control A.7.2 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Control A.7.2 del Anexo A de la norma NTE INEN-ISO/IEC 27001:2011 y a su respectiva descripción en la norma NTE INEN-ISO/IEC 27002:2009.
- Misión, Visión y objetivos del negocio de la DGIP

Las secciones que debe tener este documento son las siguientes:

- Política para el manejo de información clasificada
    - Pasos y responsabilidades
    - Clasificación de la información
        - Consideraciones generales
        - Criterios de clasificación
        - Niveles de confidencialidad
    - Etiquetado de la información
    - Manejo de información clasificada
    - Importancia de la clasificación, etiquetado y manejo de la información
        - Información interna
        - Información externa

El documento de política para el manejo de información clasificada para este proyecto se encuentra en el Anexo 17.

3.2.4.4 Política para control de Documentos y Registros.

El objetivo de este documento es el de Establecer criterios para la elaboración y control de documentos y registros relacionados con el SGSI, así como su aprobación, publicación, actualización y retiro, utilizando el estándar NTE INEN-ISO/IEC 27001:2011 y estándares de apoyo a esta norma.

Este documento es parte del control A.7.2 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Sección 4.3 de la norma NTE INEN-ISO/IEC 27001:2011.
- Organigrama y Políticas Interna de la institución.

Las secciones que tiene este documento son las siguientes:

- Procedimiento para control de documentos y registros
    - Control de documentos internos
        - Formato
        - Flujo de aprobación
        - Flujo de revisión
        - Publicación y retiro de circulación (para todos los niveles de confidencialidad)
        - Actualización de documentos
        - Control de registros
- Control de documentos externos
    - Control para recepción de documentos externos

El documento de política para el manejo de información clasificada para este proyecto se encuentra en el Anexo 18.

3.2.4.5 Informe Técnico.

Presenta un informe detallado de las vulnerabilidades a nivel lógico y a nivel físico encontradas en el análisis de riesgos realizado previamente, este documento es importante porque sirve para la toma de decisiones en cuanto a la mitigación de riesgos y la selección de controles de seguridad.

Este documento es parte del control A.12.6 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Las secciones que debe contener este documento son:

- Vulnerabilidades a nivel lógico
- Vulnerabilidades a nivel físico

El informe técnico para este proyecto se encuentra en el Anexo 19.

3.2.4.6 Resumen Ejecutivo.

Presenta información resumida del Informe Técnico, el objetivo de este documento es transmitir la información del Informe Técnico a personas que no están familiarizadas con términos técnicos por lo que este documento debe ser lo más sencillo y entendible posible.

Este documento es parte del control A.12.6 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Para realizar este documento se debe utilizar como referencia el informe técnico

Las secciones que son parte de este documento son las siguientes:

- Introducción
- Metodología
- Herramientas
- Hallazgos
- Conclusiones

El resumen ejecutivo para este proyecto se encuentra en el Anexo 20.

3.2.4.7 Plan de Tratamiento del Riesgo.

El objetivo de este documento es el de desarrollar el Plan para el tratamiento de riesgos dentro de la organización utilizando el estándar NTE INEN-ISO/IEC 27001:2011 y estándares de apoyo a esta norma.

Este documento es parte del control A.12.6 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Sección 8.3 de la norma NTE INEN-ISO/IEC 27003:2012.

- Documento de Evaluación y Tratamiento de Riesgos.
- Resumen del estado Actual de Seguridad de la Información.
- NTE INEN-ISO/IEC 27002:2009.
- NTE INEN-ISO/IEC 27005:2012.

Las secciones que debe tener este documento son las siguientes:

- Análisis de resultados de la evaluación de riesgos
- Análisis de resultados del estado actual de la seguridad de información
    - Análisis de resultados desde el punto de vista de la seguridad lógica
    - Análisis de resultados desde el punto de vista de la seguridad física
- Controles seleccionados para mitigar riesgos identificados
- Declaración de aplicabilidad
    - Matriz de aplicabilidad

El plan de tratamiento del riesgo para este proyecto se encuentra en el Anexo 21.

3.2.4.8 Procedimiento para Gestión de Incidentes.

El objetivo del presente documento es garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta ante incidentes de seguridad.

Este documento es parte del control A.13 del Anexo A de la NTE INEN-ISO/IEC 27001:2011.

Para realizar este documento se puede utilizar los siguientes documentos como referencia:

- Norma NTE INEN-ISO/IEC 27001, puntos 4.2.2 h) y A.8.2.3, capítulo A.13.
- Política del sistema de gestión de seguridad de la información.
- Legislación que regula la gestión de incidentes.
- Obligaciones contractuales que definen la gestión de incidentes.

Las secciones que debe tener este documento son las siguientes:

- Gestión de incidentes

- Definición del CSIRT
  - Definición de roles y responsabilidades del CSIRT
  - Posicionamiento del CSIRT en la organización
- Canales de comunicación principales y alternos
- Criterios de clasificación de incidentes
- Procedimiento de recepción y clasificación de incidentes, debilidades y eventos
- Procedimiento para definición de controles preventivos y correctivos
- Procedimiento para actualización de políticas internas
- Actividades de cierre y análisis del incidente
- Recolección de evidencia
- Formato de presentación del informe de investigación del incidente
- Medidas disciplinarias

El documento de procedimiento para gestión de incidentes para este proyecto se encuentra en el Anexo 21.

3.3 IDENTIFICACIÓN DE RESTRICCIONES PARA IMPLEMENTAR EL PLAN

En el proceso de implementación del plan del SGSI pudieran presentarse restricciones que impedirían que el plan se implemente correctamente, estas pueden ser las siguientes:

- Falta de responsabilidad de la dirección con la seguridad de la información.
- Discordancia de los objetivos del negocio con los objetivos de seguridad de la información.
- Carencia de recursos humanos, tecnológicos y financieros.
- Poco interés de los miembros de la organización en la ejecución del plan.
- Poco conocimiento técnico y científico del equipo de implementación del plan.
- Incumplimiento de requisitos legales y contractuales de la organización o del equipo de implementación.
- Incumplimiento en el cronograma de implementación del plan.

Por lo tanto de la implementación del plan del SGSI en la organización, se deben tomar en cuenta las siguientes consideraciones:

- El plan debe abarcar los activos de información más críticos de la organización, en este caso como se fue establecido por la dirección de la DGIP, solamente abarcará el servidor Quipux.
- Se deben establecer los controles y objetivos de control acorde con el activo de información a proteger.
- Establecer la viabilidad del proyecto en base a los recursos humanos y tecnológicos con los que cuenta la organización, rentabilidad y necesidades de protección de la información de la organización.
- Asegurar que los integrantes del equipo de implementación del SGSI y personal responsable de la organización estén comprometidos con el desarrollo del proyecto y que cuenten con las competencias necesarias para llevar a cabo una implementación exitosa del SGSI.
- Cumplir a cabalidad el plan de implementación del plan del SGSI.

3.4 ANÁLISIS DE FACTIBILIDAD PARA IMPLEMENTAR EL PLAN EN LA SITUACION ACTUAL DE LA ORGANIZACIÓN

El análisis de factibilidad del plan del SGSI, busca determinar los recursos necesarios para la implementación del mismo; los recursos son tecnológicos, humanos y operativos, dependiendo de la disponibilidad de estos recursos se determinará cuan factible es la implementación del plan.

A continuación se presenta una lista de los recursos humanos, tecnológicos y operativos que se necesitan para la implementación del SGSI de acuerdo a los controles seleccionados del anexo A de la norma NTE INEN-ISO/IEC 27001:2011.

	Recursos		
Controles	Humanos	Tecnológicos	Operativos
A.5.1.1	Comité de dirección del SGSI.	No aplica.	Equipo, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC

			27000.
A.5.1.2	Líder del equipo del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.6.1.1	Equipo directivo de la organización.	No aplica.	Equipos y Suministros de oficina.
A.6.1.2	Equipo directivo de la organización. Comité de dirección del SGSI. Líder del equipo del SGSI. Equipo de implementación.	No aplica.	Capacitaciones.
A.6.1.3	Comité de dirección del SGSI. Equipo directivo de la organización. Líder del equipo del SGSI.	No aplica.	Equipos y Suministros de oficina.
A.6.1.4	Comité de dirección del SGSI. Equipo directivo de la organización.	Software para modelar procesos. (Bonita, Bizagi, etc.)	Equipos y Suministros de oficina.
A.6.1.5	Comité de dirección del SGSI.	No aplica.	Equipos y Suministros de oficina.
A.6.1.6	Comité de dirección del SGSI. Equipo directivo de la organización.	Software para comunicación (Correo electrónico, Skype, Redes sociales, etc.)	Equipos y Suministros de oficina.
A.6.1.7	Comité de dirección del SGSI. Equipo directivo de la organización.	Software para comunicación (Correo electrónico, Skype, Redes sociales, etc.)	Equipos y Suministros de oficina.
A.6.1.8	Comité de dirección del SGSI. Líder del equipo del SGSI. Equipo de implementación.	Software para planificación de proyectos (Project, Open Project, etc.)	Equipos y Suministros de oficina.

A.7.1.2	Equipo de implementación del SGSI	No aplica.	Equipos y Suministros de oficina.
A.7.1.3	Comité de dirección del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.8.1.1	Equipo directivo de la organización.	No aplica.	Equipos, Suministros de oficina. Capacitaciones y Familia de normas NTE INEN-ISO/IEC 27000.
A.8.1.2	Equipo directivo de la organización.	No aplica.	Equipos y Suministros de oficina.
A.8.1.3	Equipo directivo de la organización.	No aplica.	Equipos y Suministros de oficina.
A.9.2.1	Equipo de implementación. Personal de seguridad.	No aplica.	Controles físicos de seguridad como candados, cerraduras, cámaras de vigilancia, rack con llaves, aire acondicionado, sistema de alarma y monitoreo para problemas ambientales, extintores, etc.
A.9.2.4	Soporte de primera línea, Especialista de Infraestructura en Respaldos y mantenimiento del Centro de Datos	No aplica.	Herramientas para el mantenimiento de equipos computacionales (Liquido limpia pantallas, Espuma limpiadora para exteriores, Liquido limpiador de contactos, Tela

			antiestática, Franela, Cepillo, Pulsera antiestática, Brocha pequeña, Destornilladores, etc.).
A.9.2.6	Especialista de Infraestructura en Respaldos y mantenimiento del Centro de Datos	Software para realizar formateo de discos a bajo nivel, disco externo para sacar respaldos.	No aplica.
A.10.1.1	Líder del equipo del SGSI. Equipo de implementación.	Software gestor documental.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.10.1.2	Líder del equipo del SGSI. Equipo de implementación.	Software gestor documental.	Equipos y Suministros de oficina.
A.10.1.3	Líder del equipo del SGSI. Equipo de implementación.	Software gestor documental.	Equipos y Suministros de oficina.
A.10.2.1	Equipo directivo de la organización.	No aplica.	Equipos y Suministros de oficina.
A.10.4.1	Líder del equipo del SGSI. Equipo de implementación.	Antivirus, Antispyware, Firewall, IDS, IPS.	Equipos, Capacitaciones y Familia de normas NTE INEN-ISO/IEC 27000.
A.10.4.2	Líder del equipo del SGSI. Equipo de implementación.	Antivirus, Antispyware, Antimalware, Firewall, IDS, IPS.	No aplica.
A.10.5.1	Líder del equipo del SGSI. Equipo de implementación. Especialista de Infraestructura en Respaldos y mantenimiento del Centro de Datos.	Software para realizar copias de seguridad.	Equipos y Suministros de oficina.

A.10.6.1	Especialista de Redes de Información en Gestión de equipos de seguridad.	Firewall, IDS, IPS.	No aplica.
A.10.6.2	Oficial de seguridades	Antimalware, Antispyware, Antispam, Antivirus, Antibot.	No aplica.
A.10.7.1	Comité de dirección del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.10.10.1	Líder del equipo del SGSI. Equipo de implementación.	Software de auditoría (Kali Linux, WinAudit, etc.)	Equipos y Suministros de oficina.
A.10.10.2	Líder del equipo del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.10.10.5	Líder del equipo del SGSI.	No aplica.	Equipos y Suministros de oficina.
A.11.1.1	Comité de dirección del SGSI. Líder del equipo del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.11.2.1	Comité de dirección del SGSI. Líder del equipo del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.11.2.2	Comité de dirección del SGSI. Líder del equipo del SGSI.	No aplica.	Equipos y Suministros de oficina.
A.11.2.3	Comité de dirección del SGSI. Líder del equipo del SGSI.	No aplica.	Equipos y Suministros de oficina.
A.11.2.4	Comité de dirección del SGSI.	No aplica.	Equipos y Suministros de

	Líder del equipo del SGSI.		oficina.
A.11.3.1	Equipo directivo de la organización.	No aplica.	Capacitaciones.
A.11.3.2	Equipo directivo de la organización.	No aplica.	Capacitaciones.
A.11.4.1	Comité de dirección del SGSI. Especialista de Redes de Información en Gestión de equipos de seguridad.	Firewall.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.11.4.2	Comité de dirección del SGSI. Especialista de Redes de Información en Gestión de equipos de seguridad.	No aplica.	Equipo y Suministros de oficina.
A.11.4.3	Líder del equipo del SGSI. Equipo de implementación. Especialista de Redes de Información en Gestión. Oficial de Seguridad.	Firewall, IDS, IPS, VPN, Router, Switch.	No aplica.
A.11.4.4	Líder del equipo del SGSI. Equipo de implementación. Especialista de Redes de Información en Gestión. Oficial de Seguridad.	Firewall, IDS, IPS, VPN, Router, Switch.	No aplica.
A.11.4.5	Líder del equipo del SGSI. Equipo de implementación. Especialista de Redes de Información en Gestión. Oficial de Seguridad.	Firewall, IDS, IPS, VPN, Router, Switch.	No aplica.

A.11.4.6	Líder del equipo del SGSI. Equipo de implementación. Especialista de Redes de Información en Gestión. Oficial de Seguridad.	Firewall, IDS, IPS, VPN, Router, Switch.	No aplica.
A.11.4.7	Líder del equipo del SGSI. Equipo de implementación. Especialista de Redes de Información en Gestión. Oficial de Seguridad.	Firewall, IDS, IPS, VPN, Router, Switch.	No aplica.
A.11.5.1	Comité de dirección del SGSI. Líder del equipo del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.11.5.3	Equipo de implementación. Oficial de Seguridad.	Software de gestión de contraseñas (Random Password Generator, KeePass Password Safe, etc.)	Equipos.
A.11.5.5	Equipo de implementación. Oficial de Seguridad. Administrador de ambientes / servicios	Herramientas del S.O.	Equipos.
A.11.5.6	Equipo de implementación. Oficial de Seguridad. Administrador de ambientes / servicios	No aplica.	Equipos.
A.11.6.1	Equipo de	Herramientas del	Equipos.

	implementación. Oficial de Seguridad. Administrador de ambientes / servicios	S.O y de las aplicaciones.	
A.11.6.2	Equipo de implementación. Administrador de ambientes / servicios	Servidor dedicado.	Equipos.
A.12.1.1	Equipo de implementación. Administrador de ambientes / servicios. Desarrollador. Tester.	No aplica.	Equipos.
A.12.2.1	Equipo de implementación. Administrador de ambientes / servicios. Desarrollador. Tester.	No aplica.	Equipos.
A.12.2.2	Equipo de implementación. Administrador de ambientes / servicios. Desarrollador. Tester.	No aplica.	Equipos
A.12.2.3	Equipo de implementación. Administrador de ambientes / servicios. Desarrollador. Tester.	No aplica.	Equipos
A.12.2.4	Equipo de implementación. Administrador de ambientes / servicios. Desarrollador. Tester.	No aplica.	Equipos
A.12.4.1	Comité de dirección del SGSI. Líder del equipo del SGSI.	No aplica.	Equipos y Suministros de oficina.

	Diseñador de sistemas.		
A.12.5.1	Comité de dirección del SGSI. Líder del equipo del SGSI. Gestor de cambios.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.12.5.2	Líder del equipo del SGSI. Gestor de cambios. Tester. Administrador de ambientes / servicios.	No aplica.	Equipos.
A.12.5.3	Líder del equipo del SGSI. Gestor de cambios.	No aplica.	Equipos.
A.12.5.4	Líder del equipo del SGSI. Equipo de implementación del SGSI.	Software de auditoría (Kali Linux, WinAudit, etc.)	Equipos.
A.12.5.5	Líder del equipo del SGSI. Administrador de ambientes / servicios. Gestor de cambios.	No aplica.	Equipos.
A.12.6.1	Líder del equipo del SGSI. Equipo de implementación del SGSI. Administrador de ambientes / servicios. Oficial de seguridad.	Nmap, Nessus, Maltego, FOCA, Kali Linux, Acunetix, MCafee, etc.	Equipos y Suministros de oficina.
A.13.1.1	Líder del equipo del SGSI. Equipo de implementación del SGSI. Oficial de seguridad.	Correo electrónico, Skype, telefonía IP, telefonía móvil.	Equipos y Suministros de oficina.
A.13.1.2	Líder del equipo del SGSI. Equipo de implementación del	Correo electrónico, Skype, telefonía IP, telefonía móvil.	Equipos y Suministros de oficina.

	SGSI. Oficial de seguridad.		
A.13.2.1	Comité de dirección del SGSI. Líder del equipo del SGSI.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.13.2.3	Comité de dirección del SGSI.	Correo electrónico, Skype, telefonía IP, telefonía móvil.	Equipos y Suministros de oficina.
A.14.1.2	Líder del equipo del SGSI. Equipo de implementación del SGSI. Oficial de seguridad.	No aplica.	Equipos, Suministros de oficina y Familia de normas NTE INEN-ISO/IEC 27000.
A.15.1.1	Equipo directivo de la organización. Comité de dirección del SGSI.	No aplica.	Equipos y Suministros de oficina.
A.15.1.4	Equipo directivo de la organización. Comité de dirección del SGSI.	No aplica.	Equipos y Suministros de oficina.
A.15.2.1	Equipo directivo de la organización. Comité de dirección del SGSI.	No aplica.	Equipos y Suministros de oficina.

Tabla 3-3 - Recursos Necesarios en Base a los Controles Seleccionados[20]

De lo expuesto anteriormente se puede distribuir la lista de recursos necesarios según su tipo.

3.4.1 RECURSOS HUMANOS

Las tareas no tienen que ser llevadas a cabo necesariamente por varias personas. El personal necesario de seguridad de la información dependerá del tamaño de la

[20] Tabla elaborada por los autores, en la cual se describen los recursos necesarios para la implementación del SGSI dentro de la organización.

organización y de sus requisitos de seguridad. La administración también debe garantizar que el personal involucrado en diversos aspectos del programa tiene las habilidades y conocimientos que necesitan para llevar a cabo eficazmente sus tareas.

Entonces en base de los roles y responsabilidades definidas para el SGSI tenemos la siguiente tabla de recursos humanos:

Cargo	Cantidad	Tipo de personal
Equipo directivo	2	Interno
Comité de dirección del SGSI	4	Interno y externo
Líder del equipo del SGSI	1	Externo
Equipo de implementación del SGSI	2	Externo

Tabla 3-4 - Recursos Humanos Necesarios para la Implementación del SGSI[21]

Para la implementación del SGSI se va a calcular el costo del personal externo necesario para cumplir con los procesos de implementación pero antes de ello es necesario calcular cual será el tiempo necesario para la implementación por lo que se hace uso de una herramienta online para el cálculo del tiempo de implementación para ISO/IEC 27001. Esta herramienta es parte de un paquete de herramientas pertenecientes a al sitio web 27001 Academy [26]. Las preguntas que se realizan para calcular el tiempo de implementación se presentan en el Anexo 24. El resultado que fue proporcionado por la herramienta para este proyecto fue de 6 meses, ese es el tiempo mínimo por el que se debe contratar a los recursos humanos que van a ser parte de la implementación.

En este proyecto la mayoría de los recursos humanos ya son empleados de la DGIP por lo que en el siguiente cuadro se muestra la lista de recursos humanos externos que deberían ser contratados para la ejecución del proyecto ya que, aunque existen cargos similares realizan también otras actividades en la organización:

RECURSOS HUMANOS						
Cargo	**Cantidad**	**Sueldo mensual**	**Tiempo (meses)**	**Costo**	**¿Recurso existente?**	**Costo real**
Auditor Líder	1	$ 1.676,00	6	$ 10.056,00	NO	$ 10.056,00

[21] Tabla elaborada por los autores, que describe los recursos humanos necesarios para la implantación del SGSI dentro de la organización.

Auditor Junior	2	$ 1.080,00	6	$ 12.960,00	NO	$ 12.960,00
			Subtotal estimado	$ 23.016,00	**Subtotal real**	$ 23.016,00

Tabla 3-5 - Costo de los recursos Humanos[22]

En este caso, como se necesita personal experto en la implementación de un SGSI y necesariamente tendrán que ser contratados, así que el ahorro en este punto es del 0%.

Figura 3-3 - Costo de los Recursos Humanos[23]

3.4.2 RECURSOS OPERATIVOS

Los recursos operativos son todos aquellos que sirven para administrar día a día el proceso de implementación, estos pueden ser físicos como los equipos y suministros de oficina o intelectuales como capacitaciones o seminarios. A continuación se presenta la lista de recursos operativos necesarios para este proyecto.

[22] Tabla elaborada por los autores, que describe los costos del recurso humano para la implantación del SGSI dentro de la organización.
[23] Figura elaborada por los autores, en base a la Tabla 3-22.

RECURSOS OPERATIVOS					
Insumo	**Cantidad**	**Costo Unitario**	**Costo total**	**¿Recurso existente?**	**Costo Real**
EQUIPOS DE OFICINA					
Computador personal	3	$ 440,00	$ 1.320,00	NO	$ 1.320,00
Impresora Láser Color	1	$ 320,00	$ 320,00	SI	$ 0,00
SUMINISTROS DE OFICINA					
Resma Papel Bond 75gr	10	$ 3,10	$ 31,00	NO	$ 31,00
Toner	5	$ 39,60	$ 198,00	SI	$ 0,00
Archivador metálico de 3 gavetas	1	$ 84,00	$ 84,00	NO	$ 84,00
Carpeta Folders Oficio (240x340mm) Manila Azul Ideal	50	$ 0,40	$ 20,00	NO	$ 20,00
Caja de Esferográficos	3	$ 2,50	$ 7,50	NO	$ 7,50
Grapadora	2	$ 16,10	$ 32,20	NO	$ 32,20
Dvd Imprimible, 4.7 Gb, Paquete De 50 Discos	1	$ 13,44	$ 13,44	NO	$ 13,44
Memoria Flash 16gb	3	$ 12,00	$ 36,00	NO	$ 36,00
HERRAMIENTAS DE MANTENIMIENTO DE EQUIPOS					
Kit De Herramientas 56 Piezas Para Mantenimiento De Pc	1	$ 40,00	$ 40,00	SI	$ 0,00
Kit De Limpieza Para	1	$ 12,00	$ 12,00	SI	$ 0,00

Computador					
Aspiradora Para Mantenimiento De Computadoras Pc	1	$ 23,00	$ 23,00	SI	$ 0,00
CONTROLES FÍSICOS DE SEGURIDAD					
Cerradura eléctrica (Cerradura Eléctrica De 12 Voltios C. Alterna)	1	$ 125,00	$ 125,00	SI	$ 0,00
Sistema de cámaras de vigilancia (Kit Video Vigilancia Seguridad 16 Cámaras)	1	$ 1.495,95	$ 1.495,95	SI	$ 0,00
Rack (Rack De Metal Para Equipos De Telecomunicaciones)	1	$ 550,00	$ 550,00	SI	$ 0,00
Sistema Biométrico	1	$ 1.829,00	$ 1.829,00	NO	$ 1.829,00
Sistema contra incendios (alarma, detectores, extintores)	1	$ 240,00	$ 240,00	SI	$ 0,00
Sistema suministro eléctrico (Ups Apc 1500va 1.5kva 865w)	1	$ 640,00	$ 640,00	SI	$ 0,00

Sistema de alarma y monitoreo para problemas ambientales(Termohigrometro Medidor De Temperatura Y Humedad Ambiental)	1	$ 38,00	$ 38,00	SI	$ 0,00
Sistema de aire acondicionado	1	$ 1.330,00	$ 1.330,00	SI	$ 0,00
NORMAS NTE INEN ISO/IEC					
NTE INEN ISO/IEC 27000:2012	1	$ 11,88	$ 11,88	NO	$ 11,88
NTE INEN ISO/IEC 27001	1	$ 18,48	$ 18,48	NO	$ 18,48
ISO/IEC 27001 (inglés)	1	$ 125,00	$ 125,00	NO	$ 125,00
NTE INEN ISO/IEC 27002:2009	1	$ 52,36	$ 52,36	NO	$ 52,36
ISO/IEC 27002:2009 (inglés)	1	$ 226,00	$ 226,00	NO	$ 226,00
NTE INEN ISO/IEC 27003:2012	1	$ 33,00	$ 33,00	NO	$ 33,00
NTE INEN ISO/IEC 27004:2012	1	$ 30,80	$ 30,80	NO	$ 30,80
NTE INEN ISO/IEC 27005:2012	1	$ 28,60	$ 28,60	NO	$ 28,60
CAPACITACIONES					
Capacitaciones SGSI por persona.	3	$ 500,00	$ 1.500,00	NO	$ 1.500,00

	Subtotal Estimado	$ 4.088,26	**Subtotal Real**	$ 5.399,26

Tabla 3-6 - Recursos Operativos Necesarios para la Implementación del SGSI[24]

Los recursos operativos se pueden adquirir en la mayoría de los casos de las propias instalaciones de la DGIP, uno de los gastos adicionales que se tiene que hacer es la compra de computadores personales para el personal que forma parte del equipo de implementación del SGSI los cuales son personas externas a la organización. A pesar de esto se logra tener un ahorro del 48.14% en este tipo de recursos.

Figura 3-4 - Costo de los Recursos Operativos[25]

3.4.3 RECURSOS TECNOLÓGICOS

Los recursos tecnológicos apoyan el proceso de implementación del SGSI y son necesarios para la correcta ejecución de los controles seleccionados. A continuación se presentan la lista de recursos tecnológicos necesarios para este proyecto.

[24] Tabla elaborada por los autores, que describe los costos operativos para la implantación del SGSI dentro de la organización.
[25] Figura elaborada por los autores, en base a la Tabla 3-23.

RECURSOS TECNOLÓGICOS			
Insumo	**Costo**	**¿Recurso existente?**	**Costo Real**
SOFTWARE			
IDS (licencia GPL)	$ 0,00	SI	$ 0,00
Antivirus, Antispyware, Antispam	$ 131,03	SI	$ 0,00
Antimalware	$ 31,54	SI	$ 0,00
Software para modelar procesos (Bonita - libre)	$ 0,00	SI	$ 0,00
Software para comunicación (skype, correo electrónico institucional, servicios streaming)	$ 0,00	SI	$ 0,00
Software para planificación de proyectos (Open Project - libre)	$ 0,00	SI	$ 0,00
Software para realizar formateo de discos a bajo nivel (HDD Low Level Format Tool - freeware)	$ 0,00	SI	$ 0,00
Software para realizar copias de seguridad. (TeraCopy Pro)	$ 19,95	SI	$ 0,00
Software de gestión de contraseñas (KeePassX - open source)	$ 0,00	SI	$ 0,00

Software para análisis de vulnerabilidades (Nmap, FOCA, Kali Linux - libres) (Nessus, Maltego Acunetix - trisl version)	$ 0,00	SI	$ 0,00
HARDWARE			
Servidor	$ 2.500,00	NO	$ 2.500,00
Firewall	$ 2.099,00	SI	$ 0,00
IPS	$ 6.089,22	SI	$ 0,00
Disco Duro Externo Anti-golpes	$ 126,00	SI	$ 0,00
Subtotal estimado	$ 10.996,74	**Subtotal real**	$ 2.500,00

Tabla 3-7 - Recursos Tecnológicos Necesarios para la Implementación del SGSI[26]

En el caso de los recursos tecnológicos se ve una gran ventaja ya que la mayoría de estos recursos ya están disponibles en la DGIP por lo que resulta sencillo comenzar con la implementación del plan, en este tipo de se puede tener un ahorro del % 77.27%

[26] Tabla elaborada por los autores, que describe los costos del recurso tecnológico para la implantación del SGSI dentro de la organización.

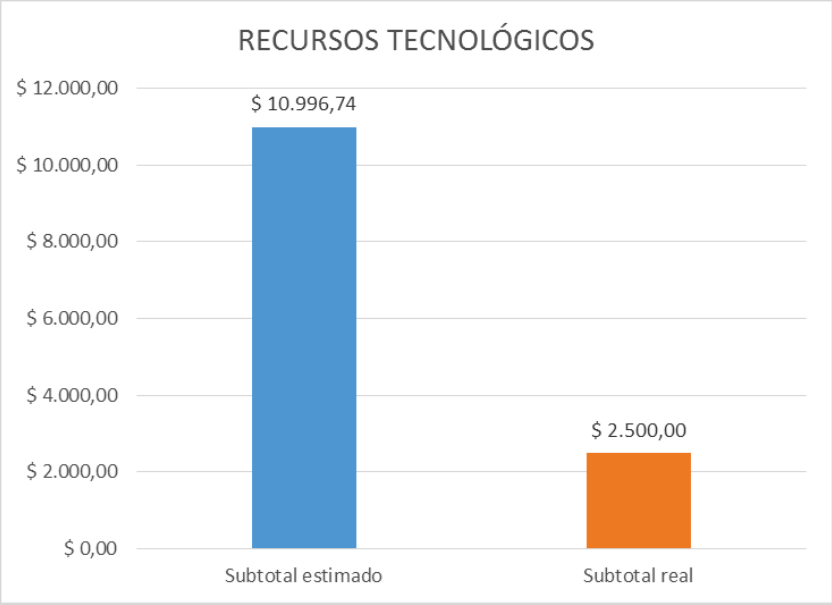

Figura 3-5 - Costo de los Recursos Tecnológicos[27]

3.4.4 CONCLUSIONES DEL ANÁLISIS DE FACTIBILIDAD

De lo expuesto en los puntos anteriores queda claro que la implementación del SGSI para el servidor es factible principalmente porque se cuenta con los recursos tecnológicos y operativos necesarios. En cuanto a los recursos humanos, la DGIP cuenta con la mayoría del personal necesario para ejecutar los controles de seguridad que se proponen en el plan, por lo que hace falta solamente que se contrate un líder auditor en seguridad de la información el cual sea experto en el tema de implementación de un SGSI y además debe estar acompañado de un equipo de implementación conformado por personas de menos experiencia que el líder, se asume que esto no debe ser complicado para el personal de talento humano de EPN ya que pueden contratar a exestudiantes que se hayan especializado en seguridad de la información de tal forma que el costo esperado para este proyecto sea igual o menor que el propuesto en este plan.

Otro factor que indica que es factible implementar el SGSI en el servidor Quipux, es que debido al uso, cada vez mayor, que se está dando a este servidor, es de suma importancia que se aplique de inmediato para así ofrecer mejores servicios y de mayor calidad garantizando la seguridad de la información.

[27] Figura elaborada por los autores, en base a la Tabla 3-24.

Las siguientes figuras muestran la factibilidad económica del proyecto por tipo de recuso y en general de todo el proyecto.

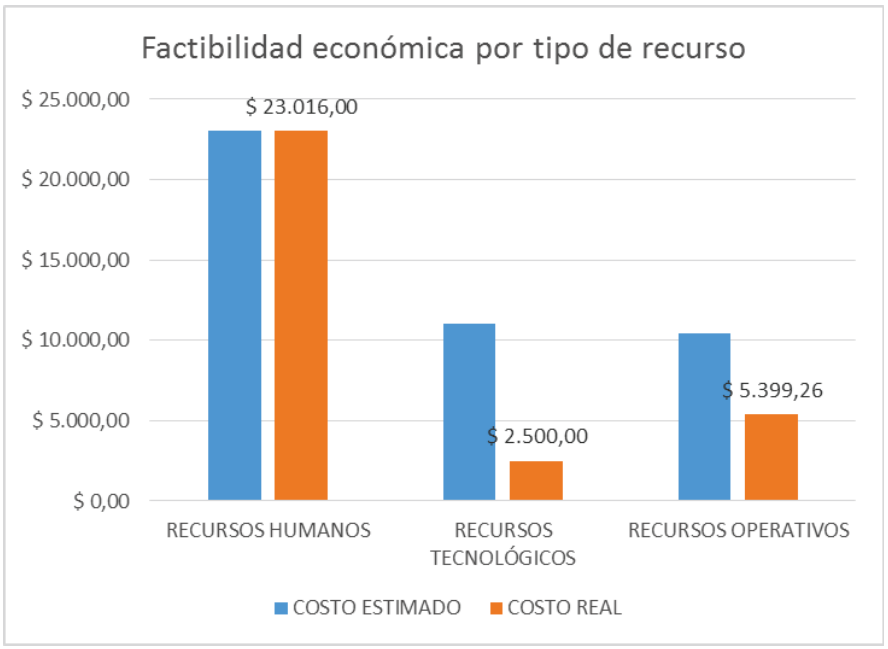

Figura 3-6 - Factibilidad Económica por Tipo de Recurso[28]

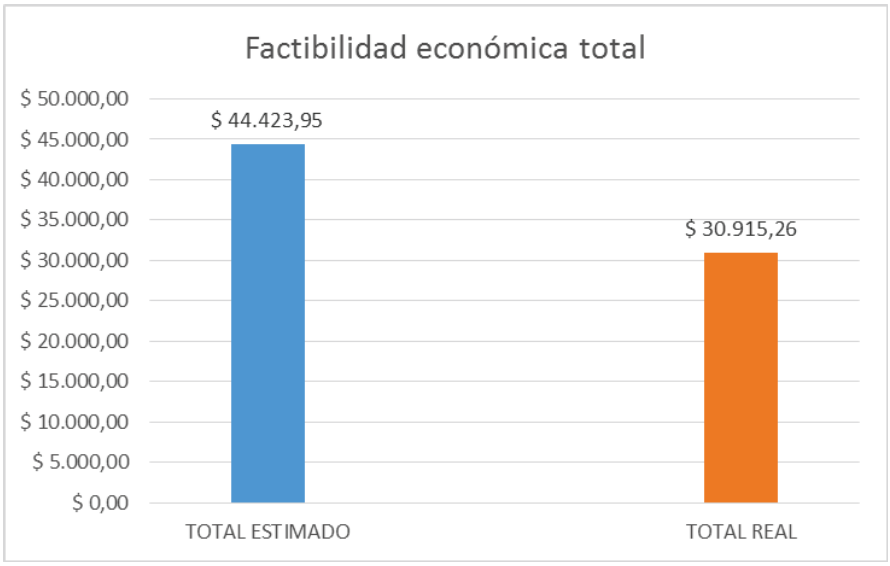

Figura 3-7 - Factibilidad Económica Total[29]

[28] Figura elaborada por los autores, en base a los costos humanos, operativos y tecnológicos.
[29] Figura elaborada por los autores, en base al total de costos estimado y real.

CAPÍTULO 4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONLUSIONES

- Con este proyecto se logró diseñar el plan del SGSI para el servidor Quipux de la EPN, permitiendo así, establecer un punto de partida para la posterior implementación, garantizando el cumplimiento de sus principios básicos (integridad, confidencialidad y disponibilidad).

- Se determinó que los niveles de seguridad implementados por la DGIP son aceptables de acuerdo a los resultados obtenidos en desarrollo del proyecto, cabe destacar que los mismos nacen de la adaptación de buenas prácticas de seguridad, motivo por el cual se considera viable que pase a etapa de implementación.

- A través de la elaboración del plan se crearon varios documentos, los cuales son componentes necesarios para la implementación del SGSI, dichos documentos permitieron definir el Sistema de Gestión de la Seguridad de la Información para el servidor Quipux de la EPN.

- En base a la norma NTE INEN-ISO/IEC 27002:2009, la cual contiene 133 controles, se seleccionaron 78 controles aplicables que permiten el tratamiento del riesgo, dado que la organización ya previamente implementó controles en aspectos físicos y otros, se descartó el resto de controles.

- Para la creación del plan fue necesario tomar como referencia secciones de otras normas de la familia NTE INEN-ISO/IEC 27000 como: NTE INEN-ISO/IEC 27002:2009 (selección de controles), NTE INEN-ISO/IEC 27003:2012 (guía de implementación), NTE INEN-ISO/IEC 27005:2012 (tratamiento de riesgos), por ende se puede concluir que la norma NTE INEN-ISO/IEC 27001:2011 no fue suficiente para la realización del plan del SGSI.

4.2 RECOMENDACIONES

- Antes de realizar el hackeo ético es recomendable crear un ambiente controlado de similares características al ambiente en producción, evitando posibles inconvenientes que afecten a la continuidad del negocio.

- Para proyectos de seguridad de la información en instituciones públicas, se recomienda tomar como referencia normativas establecidas por organismos de control, ya que no existe normativas de manera específica que traten el tema de la seguridad de la información para instituciones superiores públicas, como es el caso de le Escuela Politécnica Nacional.

- Se recomienda que la política de seguridad de la información sea socializada en todos los niveles dentro de la organización (mandos altos, medios y operacionales), para que todos los empleados estén conscientes de la importancia de la seguridad de la información.

- En proyectos de este tipo en los que el tiempo es un factor crítico, es recomendable que para la evaluación de riesgos se utilice una metodología cualitativa, dado que se basa en el juicio, la intuición y la experiencia en lugar de números, permitiendo así realizarla en menor tiempo.

- Se sugiere seleccionar herramientas apropiadas, específicas y actuales para procedimientos de hackeo ético de manera independiente, para que a la hora de probarlas en conjunto se pueda aislar errores que impidan un análisis correcto de la información.

- Si se va a implementar el SGSI, es recomendable que la documentación generada, se mantenga almacenada en un repositorio digital, utilizando herramientas como Alfresco, Quipux, entre otros, para que la documentación sea gestionada y de fácil acceso.

REFERENCIAS

[1] Dirección de Gestión de la Información y Procesos - DGIP, «www.epn.edu.ec,» 2015. [En línea]. Available: http://wweb.epn.edu.ec/ugi/index.php?option=com_content&view=article&id=19&Itemid=28. [Último acceso: 11 2014].

[2] DIRECCIÓN DE GESTIÓN DE LA INFORMACIÓN Y PROCESOS, «ESTRUCTURA ORGANIZACIONAL POR PROCESOS,» Quito, 2014.

[3] Secretaría Nacional de Administración Pública, «Secretaría Nacional de Administración Pública,» 2014. [En línea]. Available: http://www.administracionpublica.gob.ec/. [Último acceso: 12 10 2014].

[4] Secretaría Nacional de la Administración Pública, «Secretaría Nacional de la Administración Pública,» 16 9 2013. [En línea]. Available: http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2013/11/Acuerdo-No.-166.pdf. [Último acceso: 11 10 2013].

[5] S. N. d. l. A. Publica, «gobiernoelectronico.gob.ec,» [En línea]. Available: http://www1.gobiernoelectronico.gob.ec/gobierno-eficiente/accordion-b.

[6] PMG-SSI, «SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información,» ISOTools Excellence, Diciembre 2015. [En línea]. Available: http://www.pmg-ssi.com/2013/12/iso27001-origen/. [Último acceso: Septiembre 2014].

[7] INEN-ISO/IEC, «NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27001:2011,» Instituto Ecuatoriano de Normalización, Quito, 2011.

[8] INSTITUO ECUATORIANO DE NORMALIZACIÓN, «NORMS TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27002,» INEN, Quito, 2009.

[9] V. A. Canal, «ISECOM,» 2004. [En línea]. Available: WWW.ISECOM.ORG. [Último acceso: 20 10 2014].

[10] ISF, «The 2011 Standard of Good Practice for Information Security,» Information Security Forum, 2011.

[11] ISACA, «CISM Review Manual 2013,» 2012.

[12] R. S. Patricia Prandini, «ISACA,» 2012. [En línea]. Available: www.isaca.org/. [Último acceso: 14 10 2014].

[13] G. AG, «ITIL.org,» [En línea]. Available: http://www.itil.org/en/vomkennen/itil/ueberblick/index.php. [Último acceso: 20 10 2014].

[14] A. K. Stefan Kempter, «IT Process Maps,» 4 8 2013. [En línea]. Available: http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_la_Seguridad_de_TI. [Último acceso: 20 10 2014].

[15] I. E. d. Normalización, *Norma Técnica Ecuatoriana NTE-ISO/IEC 27000:2012,* Quito: INEN, 2012.

[16] Nessus, «Nessus : A security vulnerability scanning tool,» [En línea]. Available: http://www.cs.cmu.edu/~dwendlan/personal/nessus.html.

[17] T. n. security, «Guía del usuario de Nessus 5.2 HTML 5,» 2014.

[18] Paterva, «Maltego version 3 User guide,» 2011.

[19] «NMAP,» [En línea]. Available: https://nmap.org/.

[20] Acunetix, «Acunetix,» 2015. [En línea]. Available: https://www.acunetix.com/vulnerability-scanner/.

[21] ISACA, «CISM Review Manual 2013,» 2012.

[22] D. Flores, «Monitoreo del riesgo,» Quito, 2014.

[23] A. Rot, «IT Risk Assessment: Quantitative and Qualitative Approach,» San Francisco, 2008.

[24] I. E. d. Normalización, *Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001:2011,* Quito: INEN, 2011.

[25] I. E. d. Normalización, *Norma Técnica NTE INEN-ISO/IEC 27003:2012,* Quito: INEN, 2012.

[26] 2. Academy, «27001 Academy,» 2015. [En línea]. Available: 27001 Academy.

[27] Dirección de Gestión de la Información y Procesos, «Dirección de Gestión de la Información y Procesos - DGIP,» 2014. [En línea]. Available: ww.epn.edu.ec/ugi/index.php?option=com_content&view=article&id=19&Itemid=28. [Último

acceso: 13 10 2014].

[28] The Open Group, «The Open Group,» 2014. [En línea]. Available: https://www2.opengroup.org/. [Último acceso: 13 10 2014].

[29] J. Cano, «http://www.derechotecnologico.com,» 2004. [En línea]. Available: http://www.derechotecnologico.com/estrado/estrado003.html. [Último acceso: 5 Mayo 2014].

[30] A. S. Tanenbaum, Redes de Computadoras, Cuarta ed., México: Pearson Prentice Hall, 2003.

[31] Nessus, «http://www.nessus.com,» [En línea]. Available: http://www.nessus.com/. [Último acceso: 6 Mayo 2014].

ANEXOS

1. Carta de Solicitud.
2. Carta de Compromiso de la Dirección.
3. Documento de Caracterización del Negocio.
4. Documento de Objetivos y Metas con Respecto al SGSI.
5. Requerimientos Contractuales, Legales y Regulatorios.
6. Documento de Alcance y Límites del SGSI.
7. Documento de Requisitos de Seguridad de la Información.
8. Documento de Evaluación y Tratamiento de Riesgos.
9. Formato de Matriz de Evaluación de Riesgos.
10. Formato de Matriz de Tratamiento de Riesgos.
11. Matriz de Evaluación de Riesgos.
12. Matriz de Tratamiento de Riesgos.
13. Documento de Caso del Negocio.
14. Documento de Propuesta del Proyecto.
15. Documento de Política del SGSI.
16. Documento de Roles y Responsabilidades.
17. Política para el Manejo de Información Clasificada.
18. Política para control de Documentos y Registros.
19. Informe Técnico.
20. Resumen Ejecutivo.
21. Plan de Tratamiento del Riesgo.
22. Procedimiento para Gestión de Incidentes.
23. Matriz de Aplicabilidad de los Controles
24. Calculador gratuito del tiempo de implementación para ISO 27001/ISO 22301