UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSTGRADO

MAESTRIA EN INGENIERÍA DE SOFTWARE

TEMA:

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EMELNORTE

PROTOTIPO: PROCESO DE LEVANTAMIENTO DE UN NUEVO CLIENTE

Trabajo de Investigación previo a la obtención del Título de Magíster en Ingeniería de Software

TUTOR: Ing. Mauricio Rea Msc.

MAESTRANTE: Ing. Alexandra Catalina Gordillo Almeida

Ibarra – Ecuador

2017

MAESTRÍA EN INGENIERÍA DE SOFTWARE

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de grado denominado "**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EMELNORTE. PROTOTIPO: PROCESO DE LEVANTAMIENTO DE UN NUEVO CLIENTE**", realizado por la Ing. ALEXANDRA CATALINA GORDILLO ALMEIDA, para optar por el grado de Magister en Ingeniería de Software, ha sido guiado y revisado periódicamente, por lo que doy fe de que dicho trabajo reúne los requisitos y méritos suficientes cumpliendo con las normas estatutarias establecidas por la Universidad Técnica del Norte para ser sometido a presentación (pública o privada) y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra a los 10 días del mes de noviembre de 2017.

_____
ING. MAURICIO REA MSC.
TUTOR
C.C. 1002485744

MAESTRÍA EN INGENIERÍA DE SOFTWARE

APROBACIÓN DEL JURADO

"**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EMELNORTE. PROTOTIPO: PROCESO DE LEVANTAMIENTO DE UN NUEVO CLIENTE**"

Autor: Alexandra Catalina Gordillo Almeida

Trabajo de Grado de Maestría aprobado en nombre de la Universidad Técnica del Norte por el siguiente jurado, a los 10 días del mes de noviembre de 2017.

	Apellidos y Nombres	Firma
Miembro Tribunal 1:	M.Sc. Daniel Jaramillo	
Miembro Tribunal 2:	M.Sc. Cosme Ortega	
Miembro Tribunal 3:	M.Sc. Fausto Salazar	

MAESTRÍA EN INGENIERÍA DE SOFTWARE

DECLARACIÓN DE RESPONSABILIDAD

Ing. Alexandra Catalina Gordillo Almeida

DECLARO QUE:

El proyecto de grado denominado "**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EMELNORTE. PROTOTIPO: PROCESO DE LEVANTAMIENTO DE UN NUEVO CLIENTE**" y bajo juramento que el contenido e información que se encuentra en el presente trabajo de investigación, ha sido desarrollado con base a una investigación exhaustiva y de mi autoría, respetando derechos intelectuales de terceros conforme se menciona en la sección bibliográfica de éste trabajo.

_____

Ing. Alexandra Catalina Gordillo Almeida
C.I. 1003310008

MAESTRÍA EN INGENIERÍA DE SOFTWARE

AUTORIZACIÓN PARA EL USO PUBLICACIÓN
A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

(a) IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento deja sentada nuestra voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003310008		
APELLIDOS Y NOMBRES:	GORDILLO ALMEIDA ALEXANDRA CATALINA		
DIRECCIÓN:	CALLE TAHUANDO 2-128 Y JOSÉ DOMINGO ALBUJA IBARRA – IMBABURA - ECUADOR		
EMAIL:	alexc.gordillo@gmail.com		
TELÉFONO FIJO:		TELÉFONO MÓVIL:	0992010552

DATOS DE LA OBRA		
TITULO:	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EMELNORTE. PROTOTIPO: PROCESO DE LEVANTAMIENTO DE UN NUEVO CLIENTE	
AUTOR:	GORDILLO ALMEIDA ALEXANDRA CATALINA	
FECHA:	2017-11-10	
SOLO PARA TRABAJOS DE GRADO		
PROGRAMA	PREGRADO	POSGRADO ✓
TITULO POR EL QUE OPTA	MAGISTER EN INGENIERIA DE SOFTWARE	
ASESOR/DIRECTOR	ING. MSC. XAVIER MAURICIO REA PEÑAFIEL	

(b) AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Alexandra Catalina Gordillo Almeida, con cédula de identidad número: 1003310008, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizamos a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la

disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

(c) CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 10 días del mes de noviembre de 2017

LA AUTORA

_____

Ing. Alexandra Catalina Gordillo Almeida

C.I. 1003310008

MAESTRÍA EN INGENIERÍA DE SOFTWARE

CESIÓN DE DERECHO DE LA AUTORA DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Alexandra Catalina Gordillo Almeida, con cédula de identidad número: 1003310008, manifiesto de forma libre y voluntaria ceder a la Universidad Técnica del Norte los derechos de autor basados según la Ley de Propiedad Intelectual del Ecuador en sus artículos 4, 5 y 6, en calidad de autora del trabajo de grado denominado "**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EMELNORTE. PROTOTIPO: PROCESO DE LEVANTAMIENTO DE UN NUEVO CLIENTE**", que ha sido desarrollado para optar por el título de Magister en Ingeniería de Software, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En la condición de autora me reservo los derechos morales de la obra antes citada. En cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Ibarra, a los 10 días del mes de noviembre del 2017.

_____

Ing. Alexandra Catalina Gordillo Almeida
C.I. 1003310008

Dedicatoria

A mi hijo Francisco,

Por ser mi compañero de lucha y aventura en el camino de la vida.

A mis padres,

Porque nunca han dejado de creer en mí.

Alexandra Catalina…

Agradecimiento

A la Universidad Técnica del Norte en especial al Instituto de Postgrado, quienes me dieron la oportunidad de obtener mi maestría en Ingeniería de Software, para así continuar caminando a lo largo varios proyectos y sueños que permiten seguir creciendo profesionalmente.

A mi director de trabajo de grado Msc. Mauricio Rea, quién por su orientación y conocimientos otorgados me permitieron llegar a culminar con éxito el presente proyecto de investigación.

Alexandra Catalina…

Índice de contenido

RESUMEN

Las instituciones procuran fortalecer sus procesos para afianzar la seguridad de la información y sus activos, desarrollando nuevos y mejores métodos para prevenir y minimizar los riesgos a los que se encuentran expuestas (Kosutic, 2013). En este contexto, la Organización Internacional de Normalización (ISO), en el año 2005, emitió la norma ISO 27001 que proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma tiene como fin proteger los activos de la información de cualquier organización.

El presente trabajo realiza un análisis del procedimiento de implantación del SGSI basado en la norma ISO 27001, aplicándolo a un proceso de negocio de Emelnorte. El procedimiento inicia con la identificación de los activos de información y su valoración, la identificación de amenazas y la determinación de riesgos sobre los cuales se deben seleccionar los controles a aplicarse.

Los resultados del estudio muestran que un gran porcentaje de los activos de información se ven afectados por riesgos no tolerables, para los cuales se han seleccionado una lista de controles de la norma ISO 27001 a ser aplicados a fin de minimizar dichos riesgos. La selección de los riesgos incluye la determinación de indicadores para medir su cumplimiento, las fórmulas de cálculo de los indicadores y las fechas en las que la empresa deberá implementar estos controles.

La implementación de esta norma es necesario el uso de un sistema informático para mantener, controlar y evaluar un SGSI de manera óptima, ya que la información manejada puede llegar a ser muy extensa dificultando su correcto tratamiento e interpretación, en estos casos, el uso de un software desarrollado a medida se convierte en una herramienta clave para la gestión.

Se ha desarrollado un software de apoyo en la implementación de la norma. Este software analiza la información ingresada sobre los activos y las amenazas para calcular los riesgos y su tolerancia. Además, permite llevar un registro de los controles

seleccionados de la norma y su ejecución para mantener un control adecuado de la implementación.

Palabras Clave: ISO 27001, seguridad se la información, SGSI, riesgos de la información

ABSTRACT

Institutions seek to strengthen their processes to strengthen the security of information and their assets, developing new and better methods to prevent and minimize the risks to which they are exposed (Kosutic, 2013). In this context, the International Organization for Standardization (ISO), in 2005, issued the ISO 27001 standard that provides a model for the creation, implementation, operation, supervision, revision, maintenance and improvement of a Safety Management System of Information (SGSI). This standard is intended to protect the assets of the information of any organization.

The present work carries out an analysis of the implementation procedure of the ISMS based on the ISO 27001 standard, applying it to an Emelnorte business process. The procedure begins with the identification of information assets and their assessment, the identification of threats and the determination of risks over which the controls to be applied must be selected.

The results of the study show that a large percentage of the information assets are affected by non-tolerable risks, for which a list of controls of the ISO 27001 standard has been selected to be applied in order to minimize said risks. The selection of risks includes the determination of indicators to measure compliance, the calculation formulas of the indicators and the dates on which the company must implement these controls.

The implementation of this norm is necessary the use of a computer system to maintain, control and evaluate an ISMS in an optimal way, since the information handled can become very extensive, making it difficult to correct their treatment and interpretation, in these cases, the use of customized software becomes a key tool for management.

Support software has been developed in the implementation of the standard. This software analyzes the information entered on assets and threats to calculate the risks and their tolerance. In addition, it allows keeping a record of the controls selected from the

standard and its execution in order to maintain an adequate control of the implementation.

Keywords: ISO 27001, information security, ISMS, information risks

CAPITULO I. PROBLEMA DE INVESTIGACIÓN

1.1. Antecedentes

La información es uno de los activos más importantes dentro de las empresas y en ese ámbito, las TIC han tomado la posta convirtiéndose en un factor clave para mejorar la productividad de cualquier actividad económica. Es por esto que, a pesar de que las herramientas tecnológicas se han desarrollado velozmente demostrando sobradamente su fiabilidad, es necesario observar algunos aspectos básicos de seguridad que nos dé la confianza de estar protegidos contra interrupciones de servicio, fallos de sistemas, pérdida de datos, etc. Cabe indicar que no existe la seguridad absoluta, el nivel de protección total es prácticamente imposible, sin embargo, es posible establecer medidas de seguridad en base a los posibles riesgos y amenazas que se detecten (López Rubio & Callejón Piicón, 2014).

Las instituciones procuran fortalecer sus procesos para afianzar la seguridad de la información y sus activos, desarrollando nuevos y mejores métodos para prevenir y minimizar los riesgos a los que se encuentran expuestas. En este contexto, la Organización Internacional de Normalización (ISO) emite la norma ISO 27001, la cual se ha convertido en un estándar para el tratamiento de la seguridad de la información. Muchas empresas han certificado el cumplimiento de esta norma (Kosutic, 2013). En ella se describe cómo gestionar la seguridad de la información dentro de una empresa.

La ISO 27001 proporciona toda una metodología para implementar y gestionar la seguridad de la información. La función principal de la ISO 27001 consiste en proteger los atributos de confidencialidad, integridad y disponibilidad de la información de una institución. Para ello investiga cuáles son los riesgos potenciales que pueden afectarla, mediante una evaluación de riesgos, para posteriormente definir las acciones necesarias para reducirlos, lo cual se conoce como mitigación del riesgo. Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente (Kosutic, 2013).

En el Ecuador, esta norma ha sido adoptada y traducida de forma idéntica por el Instituto Nacional de Normalización INEN, emitiendo la norma técnica ecuatoriana NTE INEN ISO/IEC 27001(*Tecnologías de la Información. Técnicas de Seguridad.*

Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.) Esta norma nacional se ha preparado para proporcionar los requisitos para establecer, implementar, y mantener el mejoramiento continuo en un sistema de gestión de seguridad de la información. La adopción de un SGSI es una decisión estratégica para una organización (Institucio Nacional de Tecnologías de a Comunicación, 2017), su establecimiento e implementación están influenciados por las necesidades y objetivos de las instituciones, los requisitos de seguridad, los procesos utilizados de la organización y el tamaño y estructura de la organización (INEN, 2011).

En el año 2013, la Secretaría General de Administración Pública emitió el Acuerdo No. 166 en el cual se dispone a todas las entidades del sector público el uso obligatorio de la norma NTE INEN ISO/IEC 27001 para la gestión de la seguridad de la información.

El proceso de implementación de un SGSI puede convertirse en un proceso muy extenso dependiendo del tamaño de la organización, por lo cual para su implementación se utiliza el ciclo continuo PDCA ("Plan-Do-Check-Act"), tradicional en los sistemas de gestión de calidad, en el cual se trabaja con cada proceso de negocio dentro de la institución. En el caso de Emelnorte, el core del negocio corresponden a los procesos del área comercial.

1.2. Planteamiento del problema

Las entidades públicas son entes generadores de gran cantidad de información, por lo que requieren garantizar su seguridad, integridad y disponibilidad, de tal forma que les permita cumplir con los procesos administrativos y operativos con total eficiencia. El acceso a la información de las instituciones, a través de su red, es relativamente fácil con las herramientas disponibles y de libre obtención en internet. La ausencia de un nivel de seguridad de información efectivo provoca que las Tecnologías de la Información y Comunicación (TIC’s) que utiliza no sean confiables.

La gestión de la seguridad dentro de una institución debe realizarse mediante un proceso sistemático, estructurado y documentado que permita garantizar que los riesgos identificados en la gestión de la seguridad de la información sean correctamente tratados

para minimizar su impacto. Este proceso es el que constituye un SGSI (Sistema de Gestión de Seguridad de la Información).

La norma ISO 27001 plantea un cuadro de mando para la gestión de la seguridad de las tecnologías de información. Esta herramienta de gestión facilita la toma de decisiones mediante un conjunto de indicadores que proporcionan una visión comprensible del estado de la seguridad de la institución.

En la actualidad, Emelnorte no cuenta con un SGSI que permita garantizar el manejo, control y medición de la seguridad de la información. La seguridad se ejerce de forma empírica y no existen procedimientos establecidos para ello.

La implementación del SGSI debe iniciarse por los procesos principales del negocio de la empresa, los cuales corresponden a los procesos del Área Comercial, que básicamente comienza con el levantamiento de un nuevo cliente.

1.3.Formulación del problema

¿Cómo incide el diseño y la automatización de un Sistema de Gestión de la Seguridad de la Información(SGSI) en el manejo, control y medición de la seguridad de la información de la Empresa Eléctrica Regional Norte?

1.4. Justificación de la Investigación

La información es considerada uno de los activos más importantes de las instituciones (Najar Pacheco & Suárez Suárez, 2015), el disponer de la información de forma adecuada y oportuna puede generar claras ventajas competitivas. La mayor parte de la información reside en equipos informáticos, sistemas de almacenamiento, redes de datos, todos ellos englobados dentro de lo que se conoce como Sistemas de Información (Institucio Nacional de Tecnologías de a Comunicación, 2017), los cuales se encuentran sujetos a amenazas y riesgos generados dentro y fuera de la institución.

Cual sea la forma en que se almacene la información debe estar protegida y administrada, lo cual es realizable mediante la aplicación de un cuadro de mando de seguridad bien elaborado que permita al SGSI evaluar la eficacia y calidad de las políticas planteadas, así como el estado de la seguridad para la tomar de decisiones.

Adicionalmente, la Secretaria Nacional de Administración Pública ha emitido el Acuerdo 166, art 1 que dice "Disponer a las entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva el uso obligatorio de las normas técnicas ecuatorianas INEN ISO/IEC 27000, para la gestión de la seguridad de la información".

Por lo anteriormente expuesto se genera la necesidad de Diseñar el SGSI para la Empresa Eléctrica Regional Norte, definiendo un cuadro de mando que brinde un soporte en la toma de decisiones en lo concerniente a la seguridad de la información.

1.5. Objetivos de la investigación

1.5.1. Objetivo general

Desarrollar el Sistema de Gestión de la Seguridad de la Información para la Empresa Eléctrica Regional Norte mediante la aplicación de la norma ISO 27001 para brindar un soporte en la toma de decisiones gerenciales.

1.5.2. Objetivos específicos

1.5.2.1. Analizar las normas técnicas ecuatorianas INEN ISO/IEC 27000 requeridas para el desarrollo del SGSI.

1.5.2.2. Diseñar el Sistema de Gestión de la Seguridad de la Información de acuerdo a la metodología de la norma ISO 27001 para el proceso de levantamiento de un cliente nuevo de la empresa.

1.5.2.3. Automatizar mediante software el mantenimiento, control y medición de los principales índices del SGSI.

1.5.3. Preguntas directrices

1.5.3.1. ¿Cuáles son los riesgos que se originan por la falta de seguridad informática?

1.5.3.2. ¿Cuáles son las normas INEN ISO/IEC que deben aplicarse?

1.5.3.3. ¿Que son los Sistemas de Gestión de la Seguridad de la Información?

1.5.3.4. ¿Cuáles son los principales índices que deben automatizarse del SGSI?

1.5.4. Variables e Indicadores

Variable Independiente

Diseño y automatización Sistema de Gestión de Seguridad de la Información.

Variable Dependiente

Manejo, control y medición de la seguridad de la información de la Empresa Eléctrica Regional Norte.

Operacionalización de la variable independiente:

Tabla 1. *Operacionalización de la variable independiente*

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Es un conjunto de procedimientos para gestionar la protección de la información, asegurando los atributos de confidencialidad, integridad y disponibilidad de los activos de información, identificando riesgos y mitigándolos mediante un Plan de tratamiento de riesgos.	Accesibilidad de la información Riesgos de la seguridad	Disponibilidad de servicios Nivel de riesgos de seguridad informática	¿Cuál es el índice de disponibilidad de los servicios? ¿Cómo se mide el nivel de riesgos informáticos?	Reportes técnicos de disponibilidad de servicios. Encuesta

Fuente: Investigadora

Operacionalización de la variable dependiente:

Tabla 2. *Operacionalización de la variable dependiente*

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
La seguridad informática es salvaguardar la información mediante condiciones de sistema de procesamiento de datos y almacenamiento	Salvaguardar la información Protección de daños de gran	Costos generados por pérdidas de información Tiempo de recuperación ante perdidas	¿Han sido significativos los gastos generados por la pérdida de la información? ¿Con que	Entrevista Entrevista/ Bitácoras

para protegerlos del impacto de daños de gran potencial en los sistemas informáticos o estructuras TIC.	potencial		frecuencia se generan daños potenciales en los sistemas informáticos?	

Fuente: Investigadora

1.6.Viabilidad

Para poder desarrollar el proyecto se tomará en cuenta lo siguiente:

1.6.1. Factibilidad Técnica.- Existe el conocimiento, la información y los recursos necesarios para la realización del presente estudio. Se cuenta además con el apoyo del personal técnico de la Dirección de TIC quienes conocen de cerca la problemática del tema planteado.

1.6.2. Factibilidad Operativa.- El estudio se lo realizará en cooperación con las personas responsables de las diferentes áreas de la Dirección de Tecnología.

1.6.3. Factibilidad Económica.- El proyecto se financiará una parte por el desarrollador del proyecto y otra por la empresa donde será ejecutado, puesto que ya cuenta con infraestructura que puede ser utilizada para su implementación.

1.7.Valor práctico

Con el desarrollo del presente proyecto el principal beneficiario es la Dirección de TIC de Emelnorte, al tener implementado un Sistema de Gestión de Seguridad de Información que le permita mantener la confiabilidad, integridad y disponibilidad de la información, lo que se traduce en un beneficio para los usuarios del servicio eléctrico de toda el área de concesión, que podrán acceder a sus servicios sin inconvenientes.
Los beneficiarios indirectos serán:

- La Empresa Eléctrica Regional Norte en toda su área de concesión, porque el Departamento de Tecnologías es un eje transversal de la misma.

- Desarrollador del proyecto, porque podrá colaborar en la realización de un proyecto que ayudará a solucionar varios inconvenientes en la toma de decisiones de la Dirección.

1.8.Presupuesto

Tabla 3. *Presupuesto*

PRESUPUESTO DETALLADO					
1	EQUIPOS, SOFTWARE Y SERVICIOS	VALOR	2	RECURSOS HUMANOS, TRANSPORTE, SALIDAS DE CAMPO	VALOR
	Equipo informático	1000		Transporte	200
Subtotal 1		1000	Subtotal 2		200
3	MATERIALES Y SUMINISTROS	VALOR	4	MATERIAL BIBLIOGRÁFICO	VALOR
	Suministros	300		Libros	500
				Normas	500
Subtotal 3		300	Subtotal 4		1000
PRESUPUESTO GLOBAL					
ITEM					TOTAL
1	Equipos, Software y Servicios Técnicos				1000
2	Recursos Humanos, Transporte y Salidas de Campo				200
3	Materiales y Suministros				300
4	Material Bibliográfico				1000
				Subtotal	2500
+				10% Imprevistos	250

=	Valor Total	2750

Fuente: Investigadora

1.9.Cronograma de actividades

Tabla 4. *Cronograma de actividades*

Actividades	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.Recopilación bibliográfica																								
2.Elaboración del Marco Teórico																								
3.Elaboración de los Instrumentos																								
4.Prueba de los Instrumentos																								
5.Recolección de Datos																								
6.Procesamiento de Datos																								
7. Análisis de los Datos																								
8. Redacción del Borrador																								
9.Revisión y Corrección del borrador																								
10. Presentación del Informe																								

Fuente: Investigadora

CAPITULO II. MARCO TEÓRICO

En el presente capítulo se proporciona la contextualización del problema planteado y los conceptos básicos que se utilizarán durante el desarrollo del proyecto. Nos ayudarán a comprender la importancia de la seguridad de la información; las amenazas y riesgos a los que están expuestos los datos; y nos permitirá conocer acerca de serie de normas ISO/IEC 27000.

2.1 Seguridad de la Información

La seguridad de la información se define como la protección de activos de información dentro de una empresa. Es importante diferenciarla de la seguridad informática, la cual se refiere a la protección de la infraestructura de las tecnologías de información y comunicaciones que dan soporte al negocio (Institucio Nacional de Tecnologías de a Comunicación, 2017).

Dentro de una empresa se genera una increíble cantidad de información proveniente de diversas fuentes, como son, correos electrónicos, bases de datos, páginas web, presentaciones, documentos, etc. Toda esta información puede encontrarse en diferentes soportes desde el papel, hasta los medios digitales. Adicionalmente, se debe considerar el ciclo de vida de la información ya que existe reglamentación que regula su tiempo de validez, es decir que, la información que hoy puede ser crítica, dentro de algunos años podría dejar de ser necesaria e importante.

Con la utilización del Internet como medio de comunicación global, los incidentes relacionados con sistemas informáticos vienen incrementándose de manera alarmante, haciéndose indispensable para las instituciones la utilización de sistemas de seguridad. "…la seguridad es un proceso continuo multidimensional, que debe tenerse en cuenta en la definición, en la gestión y en la reingeniería de empresas y procesos de negocio." (Areitio, 2008).

Los objetivos de la seguridad son los siguientes:

- **Disponibilidad y accesibilidad**: Capacidad de garantizar que la información se encuentra disponible para los usuarios autorizados en el momento en que ellos lo

requieran. Protege contra intentos deliberados o accidentales de borrado de datos o de cualquier tipo de denegación del servicio de acceso a los mismos.

- **Integridad**: Se encarga de garantizar que la información ha sido modificada únicamente por personal autorizado, con lo cual se garantiza su validez y consistencia.
- **Confidencialidad**: Capacidad de garantizar que la información pueda ser leída o interpretada únicamente por el personal autorizado. La protección de la confidencialidad aplica a los datos desde su almacenamiento y procesamiento, hasta su transmisión.
- **No repudio**: Capacidad de garantizar la participación de las partes en una comunicación. Tanto el emisor como el receptor de un enlace de comunicación, deben tener pruebas irrefutables de la participación de ambas partes. Soporta directamente la disuasión, el aislamiento de fallos, la detección y prevención de intrusiones y después la recuperación y las acciones legales pertinentes (Areitio, 2008).
- **Confiabilidad**: Capacidad de garantizar que los cuatro objetivos anteriores se han cumplido a cabalidad, asegurando que las medidas de seguridad cumplen el objetivo para el que fueron diseñadas.

Para asegurar el entorno en el cual se maneja la información, las empresas pueden ayudarse de un Sistema de Gestión de la Seguridad de la Información.

2.2 SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION

Un SGSI (Sistema de Gestión de la Seguridad de la Información) es una herramienta o metodología basada en la norma ISO 27001 de gestión que permite conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información dentro de una empresa mediante la definición de políticas y procedimientos (Institucio Nacional de Tecnologías de a Comunicación, 2017).

Un SGSI analiza y ordena la estructura de los sistemas de información, facilita la definición de procedimientos de trabajo para mantener su seguridad y ofrece la posibilidad de disponer de controles que permitan medir la eficacia de las medidas tomadas. Con esto se busca proteger a las organizaciones frente a amenazas y riesgos

que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de negocio (Espinoza, 2015).

De esta manera se consigue mantener el riesgo para nuestra información por debajo del nivel asumible por la propia organización. La gestión de los riesgos a través de un Sistema de Gestión de Seguridad de la Información permite preservar la confidencialidad, integridad y disponibilidad de la misma, en el interior de la empresa.

La confidencialidad implica el acceso a la información por parte únicamente de quienes están autorizados. La integridad conlleva el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Y la disponibilidad entraña el acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran (Espinoza, 2015).

La utilización de un SGSI permite proteger la información, junto con los procesos que hacen uso de ella y los activos que intervienen, siendo además, un gran apoyo en el cumplimiento de la legalidad y protección adecuada de los objetivos del negocio. En la gestión efectiva de la seguridad debe participar de forma activa toda la organización, con el apoyo de la gerencia para alcanzar los objetivos deseados mediante un modelo que contemple procedimientos adecuados y la planificación e implantación de controles basados en una evaluación de riesgos.

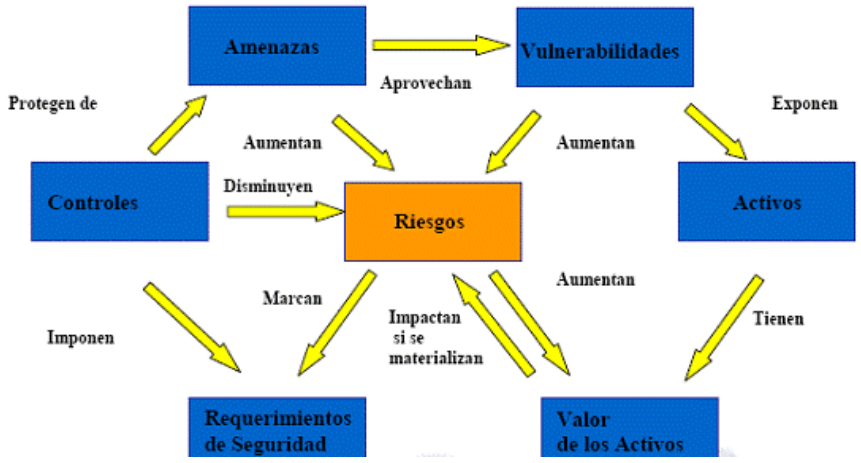


Figura 1. SGSI
Fuente: (El portal de ISO 27001 en Español, 2012)

2.3 Activos de la Seguridad de la Información

Con el paso del tiempo la información ha llegado a considerarse un insumo fundamental para el desarrollo de los procesos de negocio de las organizaciones. A toda esa información y recursos de valor que generan, procesan, almacenan o transmiten y que se deben proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de los negocios se la denomina activos de información.

El objetivo de un SGSI es proteger los activos de seguridad de la información, por esta razón es importante identificar dichos activos para delimitar el alcance que tendrá el estudio. La identificación del inventario de activos de información, permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso (MINTIC, 2016). En este paso se definen los límites del sistema en estudio a la vez que se detallan los recursos y la información que constituyen el sistema.

2.3.1 Tipos de activos

Existen muchas formas de clasificar a los activos según su naturaleza, según la metodología de Magerit (MAGERIT – versión 3.0, 2012), podemos determinar los siguientes tipos:

- Primer tipo: Servicios, se refiere a los procesos de negocio de la organización, sean estos internos o externos, como por ejemplo la gestión de nómina.
- Segundo Tipo: Datos e información generada y manipulada dentro de la organización.
- Tercer tipo: Todo lo que se refiere a aplicaciones de software.
- Cuarto tipo: Equipos informáticos.
- Quinto tipo: personal, abarca desde el personal internos hasta los clientes externos.
- Sexto tipo: En este grupo están las redes de comunicaciones que dan soporte a la transferencia de la información, sean estas propias o contratadas.
- Séptimo tipo: Lo conforman los soportes de información que permiten su almacenamiento por períodos largos de tiempo.

- Octavo tipo: Equipamiento auxiliar de soporte a los sistemas de información que no ha sido incluido en los grupos anteriores.
- Noveno tipo: Instalaciones donde se alojan los sistemas de información.

Es necesario identificar y clasificar los activos identificando claramente sus características y rol dentro de la organización. Las actividades a realizar para obtener un inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información (MINTIC, 2016).

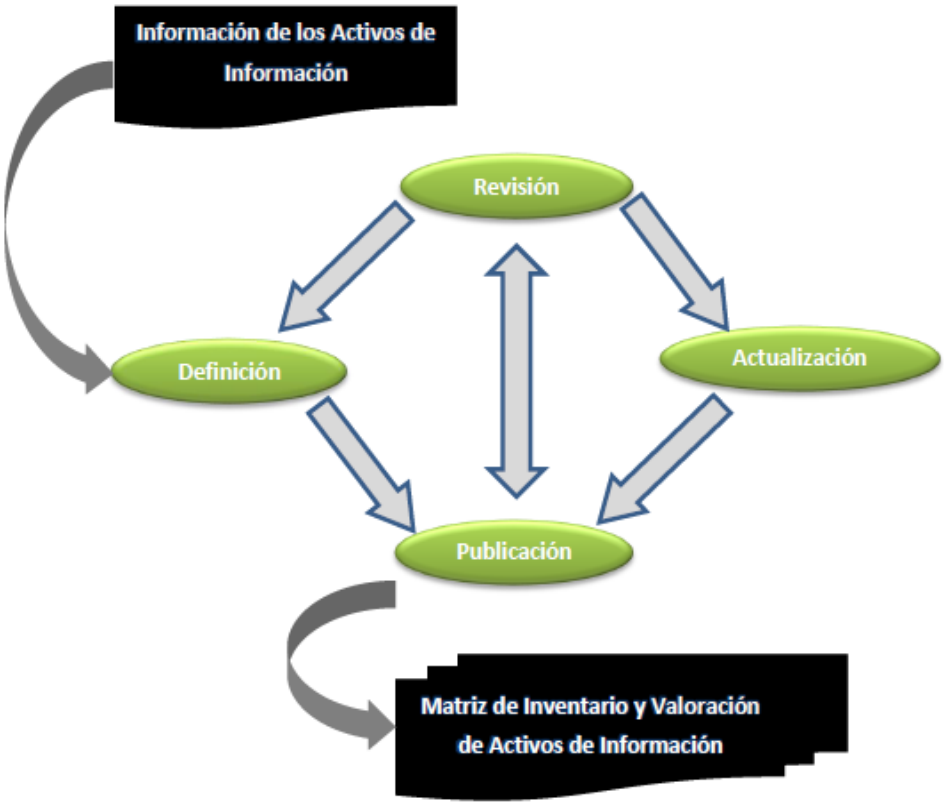


Figura 2. Procedimiento para inventario de activos
Fuente: (MINTIC, 2016).

En el inventario de los activos debe constar como mínimo la información básica del activo como un identificador, proceso al que pertenece, nombre, descripción, tipo, ubicación, clasificación y criticidad.

2.3.2 Valoración de activos

Luego de la identificación de activos, es necesario valorarlos, es decir, estimar el valor y la importancia que tienen para la organización. Para valorar un activo se debe

considerar la pérdida que puede suponer para la organización en caso de que resultara dañado en cuanto a su disponibilidad, integridad y confidencialidad.

La valoración se la puede realizar en una escala cuantitativa o cualitativa. Cuando es posible valorar económicamente la pérdida o daño, se utiliza una escala cuantitativa, pero en la mayoría de los casos se usa la escala cualitativa, por ejemplo: bajo, medio, alto; o una escala numérica, por ejemplo del 1 al 10.

Es necesario involucrar a las áreas de la organización a fin de que esta sea lo más objetiva posible y se pueda obtener una imagen más realista de los activos. Se debe definir parámetros para que los participantes tengan criterios comunes y coherentes, por ejemplo:

- Disponibilidad: Se debe determinar cuál es la importancia o e trastorno que causaría el activo al no estar disponible.
- Integridad: Se debe considerar que importancia tendría si el activo es modificado sin autorización ni control.
- Confidencialidad: Se debe considerar que importancia tendría que el activo sea accedido de manera no autorizada.

La metodología Magerit establece una tabla con los criterios de valoración de activos, la misma puede ser adaptada a los requerimientos de cada institución.

Tabla 5. *Adaptación de criterios de valoración de activos*

VALOR	CRITERIO
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente: Investigadora

El resultado final del procedimiento aplicado a un proceso de negocio de la organización, es el inventario de los activos de información clasificados y valorados, que constituirá en una entrada para el siguiente paso en el desarrollo de un SGSI, la identificación de amenazas y riesgos.

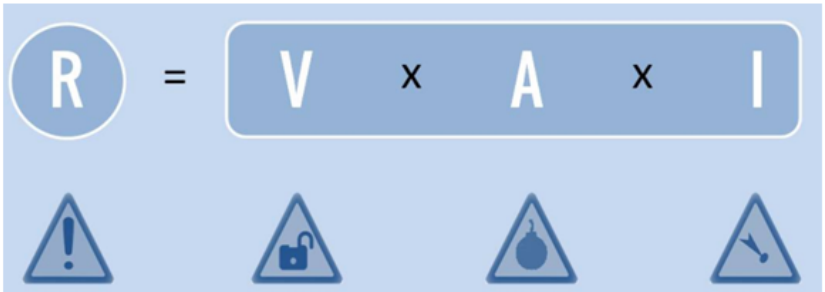
Una buena identificación de activos de información permitirá centrar el esfuerzo en los elementos realmente importantes y de valor para la organización, lo cual agilita el trabajo, reduce el tiempo y facilita la gestión de riesgos y amenazas identificados.

2.4 Riesgos Informáticos

El término "riesgo" representa la exposición ante cualquier situación que genere la posibilidad de sufrir un daño o de estar en peligro. La probabilidad de que una amenaza se convierta en un desastre, utilizando la vulnerabilidad existente de un activo, provocando efectos negativos que lleguen a afectarlo se denomina riesgo (González Viancha, 2014).

Los daños ocasionados pueden variar desde simples errores en el uso de aplicaciones de gestión que comprometan la integridad de los datos, hasta catástrofes que inutilicen la totalidad de los sistemas. Las pérdidas pueden aparecer por la actividad de intrusos externos a la organización, por accesos fraudulentos, por accesos no autorizados, por el uso erróneo de los sistemas por parte de empleados propios, o por la aparición de eventualidades en general destructivas.

Si las vulnerabilidades y las amenazas se presentan por separado no representan ningún peligro, sin embargo, si se juntan, la probabilidad de que ocurra un desastre aumenta, por lo que se convierten en un riesgo. Se puede utilizar la siguiente ecuación para definir un riesgo:



Riesgo	=	Vulnerabilidad	x	Amenaza	x	Impacto
Probabilidad de que las amenazas actúen sobre los activos causando daños o pérdidas		Debilidad o falta de control que permitiría o facilitaría que una amenaza actúe contra un activo		Circunstancia o evento que puede explotar, intencionalmente o no, una vulnerabilidad específica		Daño causado en un activo como resultado de la explotación de una vulnerabilidad por una amenaza

Figura 3. Ecuación del riesgo
Fuente: (Davara, 2015)

Cuando estas vulnerabilidades atañen a los activos informáticos podemos considerar que se trata de un "riesgo informático". Es importante que las organizaciones cuenten con herramientas que garanticen una adecuada gestión de riesgos, desde la identificación y evaluación hasta su valoración, mitigación y control.

2.4.1 Tipos de Riesgos Informáticos

- **Sabotaje informático:** Corresponde a las acciones dirigidas a provocar daños ya sea a nivel físico (hardware) o a nivel lógico (software) de un sistema informático. Se las identifica en dos grupos:
    a) Conductas dirigidas a causar daños físicos.- Comprende todo tipo de acciones dirigidas a causar el daño físico del hardware y software de un sistema por ejemplo: provocar cortocircuitos dentro de un servidor, causar explosiones o incendios, etc.
    b) Conductas dirigidas a causar daños lógicos.- Comprende todo tipo de acciones que causan daños lógicos de un sistema, es decir, que producen como resultado, la alteración o destrucción de los datos de un sistema.

- **Fraude a través de computadoras:** Corresponde a las acciones destinadas a la creación de datos falsos o la manipulación ilícita de los datos de un sistema informáticos con el objetivo de obtener ganancias indebidas. La modificación de los datos se la puede realizar por distintos métodos. La manipulación del input consiste en alterar, omitir datos o ingresar datos falsos en un ordenador. Es posible también interferir con la secuencia de procesamiento lógica de un sistema, alterando su programación; o, alterar el resultado obtenido de un procesamiento, a esta modalidad se la conoce como manipulación del output.

- **Copia ilegal de software y espionaje informático:** Corresponde a aquellas conductas dirigidas a obtener datos, en forma ilegítima, de un sistema informático. Es común el robo de información personal, listas de clientes, cuentas bancarias, listas de correo electrónico, etc. información que tiene un valor económico para una empresa.

- **Uso ilegítimo de sistemas informáticos ajenos:** Esta conducta corresponde a utilización sin autorización de los computadores y programas de un sistema informático, comúnmente por empleados de las mismas instituciones que lo utilizan para fines privados o su beneficio propio, lo cual puede repercutir en un perjuicio económico importante para las instituciones que, por ejemplo, pagan por procesamiento de sus sistemas.

- **Delitos informáticos contra la privacidad:** Corresponde a las acciones de quien sin estar autorizado, se apodere, utilice o modifique datos personales o familiares de un tercero, contenidos en un soporte informático, causando perjuicio mediante la acumulación, archivo y divulgación indebida de los mismos. También corresponde a la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación.

- **Delitos informáticos como instrumento o medio:** En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:
  - Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
  - Variación de los activos y pasivos en la situación contable de las empresas.
  - Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
  - Lectura, sustracción o copiado de información confidencial.
  - Modificación de datos tanto en la entrada como en la salida.
  - Uso no autorizado de programas de cómputo.
  - Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
  - Obtención de información residual impresa en papel luego de la ejecución de trabajos.
  - Acceso a áreas informatizadas en forma no autorizada.

- **Delitos informáticos como fin u objetivo:** En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:
  - Programación de instrucciones que producen un bloqueo total al sistema.
  - Destrucción de programas por cualquier método.
  - Daño a la memoria.
  - Atentado físico contra la máquina o sus accesorios.
  - Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

2.4.2 Metodología Magerit para Análisis y Gestión de Riesgos

Magerit es el acrónimo de Metodología de Análisis y Gestión de Riesgos de Sistemas de Información, creado por el Consejo Superior de Administración Electrónica (CSAE). Es una metodología de carácter público que se aplica para conocer el riesgo al que está sometida la información y como ésta puede ser segura o insegura. Pertenece al Ministerio de Administraciones Públicas de España.

La metodología Magerit es el método formal para investigar los riesgos que afectan a los activos de información. Este instrumento facilita la implementación y aplicación de esquemas de seguridad proporcionando los principios básicos y mínimos para la protección adecuada de la información.

Magerit persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de mitigarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación según corresponda el caso.

En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en

cuenta los riesgos derivados del uso de tecnologías de la información (CONTENTO, 2015).

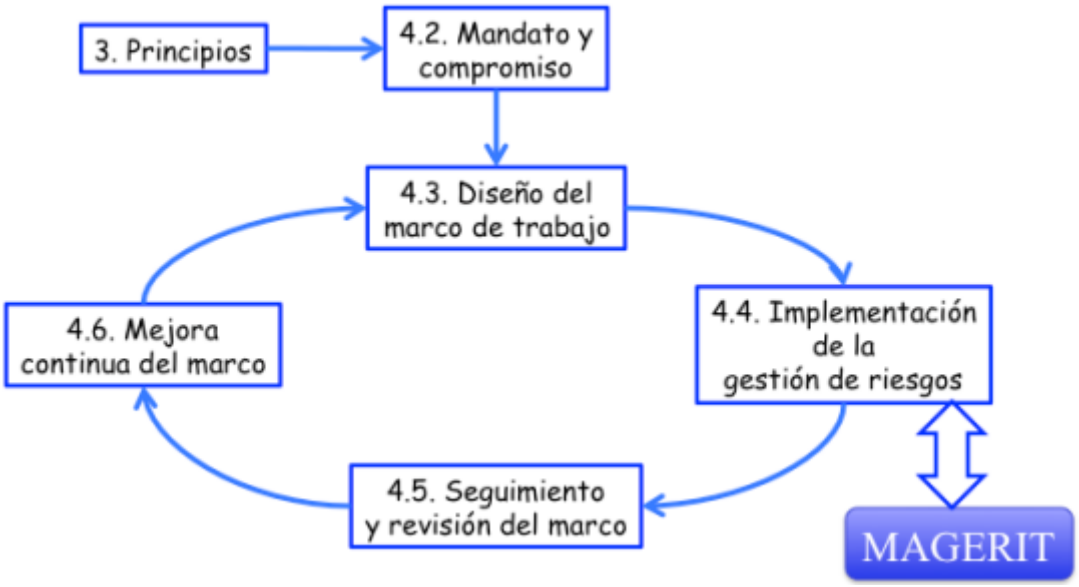


Figura 4. Marco de trabajo para la gestión de riesgos
Fuente: (MAGERIT – versión 3.0, 2012)

MAGERIT versión 3 se ha estructurado en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas". Se estructura de la siguiente forma (MAGERIT – versión 3.0, 2012):

- El capítulo 1 es una fase introductoria a la metodología, pronunciando que organismos lo crearon.
- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Las actividades para el análisis de riesgos que se realizan con esta metodología son las siguientes:

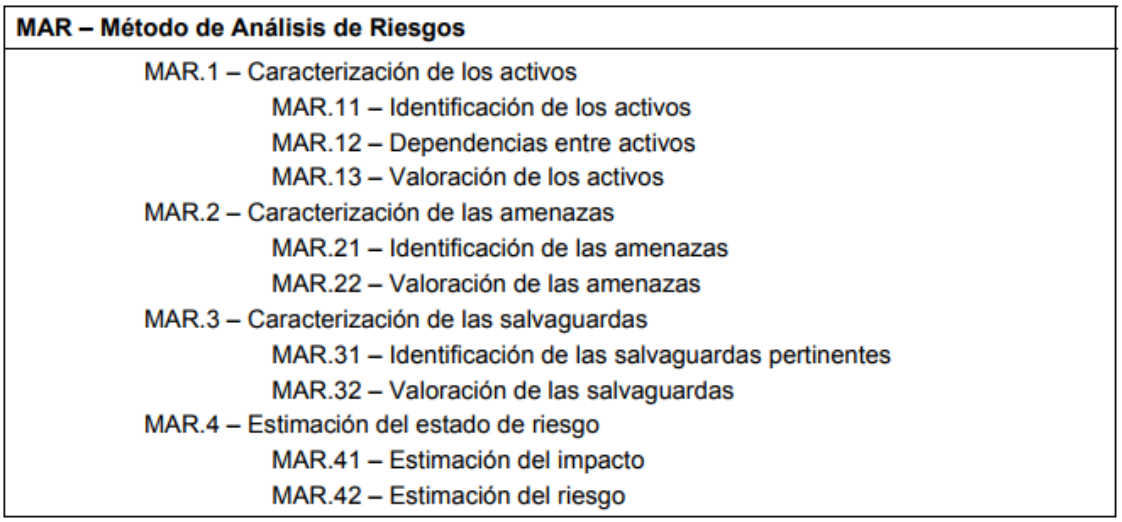


Figura 5. Formalización de actividades Magerit
Fuente: (MAGERIT – versión 3.0, 2012)

2.5 Amenazas y Vulnerabilidades de la Seguridad de la Información

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información, es decir, corresponde a la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

El incremento del uso de la tecnología y la creciente rentabilidad de los ataques trae consigo el incrementado también del número de amenazas a las que se encuentran expuestos los sistemas de información, amenazas que se fortalecen con situaciones

como la falta de capacitación y concientización a los usuarios en el uso de la tecnología y el perfeccionamiento de las técnicas de ingeniería social,

2.5.1 Clasificación de las amenazas

Existen diferentes formas de clasificar las amenazas de acuerdo a su origen, forma de ataque, entre otras. Algunas formas de clasificarlas son las siguientes:

- Intencionales: en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
- No intencionales: en donde se producen acciones u omisiones de acciones que, si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).
- Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:
  - Los usuarios conocen la red y saben cómo es su funcionamiento.
  - Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.
  - Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.
- Amenazas externas: Son aquellas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.
- Amenazas lógicas: Son programas que pueden dañar el sistema: Virus y Malware, accesos no autorizados por puertas traseras, que se crean en aplicaciones grandes o sistemas operativos para facilitar tareas de mantenimiento, y que son descubiertas por los atacantes. Software incorrecto. Los bugs o agujeros son errores cometidos de forma involuntaria por los programadores de sistemas o aplicaciones. Estos errores pueden ser aprovechados para dañar el sistema. Tradicionalmente los virus han sido uno de los principales riesgos de seguridad para los sistemas informáticos. El principal método de propagación es a través de las redes informáticas e Internet, reproduciéndose e infectando equipos conectados.

- Amenazas físicas: Estas amenazas pueden darse por fallos en los dispositivos, fallos de discos duros, cableado de red, suministro de energía, etc., provocando una caída del sistema. Dentro de estas amenazas también tenemos catástrofes naturales (terremotos, inundaciones, etc.).

2.5.2 Tipos de amenazas

Se puede agrupar las amenazas en 5 grandes grupos:

- **Factores Humanos**: Representa la mayor amenaza para un sistema de información, por consecuencia, requiere mayor inversión de recursos para controlar y contrarrestar sus efectos. Existen diferentes factores que motivan a las personas a ingresar a un sistema, que van desde la propia curiosidad, el pago por la información obtenida, causar daño o con fines proselitistas o religiosos, dañar o reducir la funcionalidad de un sistema, obtener información confidencial, etc.
- **Hardware**: Son aquellas amenazas por fallas físicas del hardware sobre el cual opera un sistema de información, que puede darse con defecto de fabricación, variaciones de voltaje, descuido y mal uso, desgaste causado por el uso constante, etc.
- **Red de datos**: Las dos principales amenazas que se presentan a nivel de la red son: la no disponibilidad de la red y la extracción lógica de la información a través de esta. Por ello, suele invertirse recursos para aislar las redes de comunicaciones e instalar sistemas de seguridad perimetral.
- **Software**: Incluye posibles fallas dentro del software de un sistema. Entre ellos tenemos el software malicioso (virus, gusanos informáticos, troyanos, bombas lógicas, etc.), errores de programación y diseño que pueden causar daños o pérdida de información.
- **Desastres naturales**: Representan aquellos eventos cuyo origen es estrictamente natural. Estos eventos representan una amenaza no solo para la información, sino para el sistema completo (infraestructura, equipos, componentes, etc.), entre ellos se encuentran: inundaciones, terremotos, incendios, huracanes, etc.

2.6 NORMAS ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa (Kosutic, 2013). Esta norma proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) adoptando un enfoque por proceso, basado en el Ciclo de Deming: PDCA, por sus siglas en inglés de Plan, Do, Check, Act; que significa Planificar, Hacer, Verificar, Actuar, que la vuelve aplicable a cualquier tipo de organización.

La función principal de la ISO 27001 consiste en proteger los atributos de confidencialidad, integridad y disponibilidad de la información de una institución. Para ello investiga cuáles son los riesgos potenciales que pueden afectar la información, mediante una evaluación de riesgos, para posteriormente definir las acciones necesarias para reducir dichos riesgos, lo cual se conoce como mitigación del riesgo.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad (Kosutic, 2013).

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente (Institucio Nacional de Tecnologías de a Comunicación, 2017).

2.6.1 Ventajas

Mediante la implementación de la ISO27001, una institución puede obtener gran cantidad de ventajas y beneficios en lo que respecta a la seguridad de la información, a continuación se enumeran las más esenciales:

- Cumplir con los requerimientos legales
- Identificar los riesgos y establecer controles para gestionarlos o eliminarlos
- Confidencialidad, permitiendo el acceso a la información solo por personas autorizadas para ello.
- Flexibilidad para adaptar los controles a todas las áreas de su empresa o solo a algunas seleccionadas
- Conseguir que las partes interesadas y los clientes confíen en la protección de los datos
- Demostrar conformidad y conseguir el estatus de proveedor preferente
- Alcanzar las expectativas demostrando conformidad

2.6.2 Estructura de la norma

ISO/IEC 27001:2011, versión adquirida por Emelnorte, se divide en 8 secciones más el anexo A; las secciones 0, 1, 2 y 3 corresponden a una introducción a la norma, las secciones 4 a 8 establecen los requerimientos y el procedimiento a seguir para la implementación de la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad (Kosutic, 2013).

Sección 0 – Introducción: expone el objetivo de ISO 27001, el enfoque por proceso y su compatibilidad con otros sistemas de gestión.

Sección 1 – Generalidades y aplicación: explica el campo de aplicación de la norma.

Sección 2 – Normas de referencia: indica las normas necesarias para la aplicación de la norma ISO/IEC 27000.

Sección 3 – Términos y definiciones: explica las definiciones de la terminología utilizada.

Sección 4 – Requisitos de la documentación: indica la documentación que debe incluir un SGSI, así como el procedimiento para definir las acciones de gestión necesarias.

Sección 5 – Responsabilidad de la dirección: esta sección explica las actividades a cargo de la dirección para asegurar la correcta implementación del SGSI.

Sección 6 – Auditorías internas del SGSI: Explica el procedimiento a seguir para realizar auditorías del SGSI.

Sección 7 – Revisión del SGSI por la dirección: Explica el procedimiento a seguir para que la dirección realice la revisión periódica del SGSI, con el propósito de asegurar su eficacia.

Sección 8 – Mejora del SGSI: explica los requerimientos para las acciones preventivas y correctivas del SGSI.

Anexo A – este anexo proporciona un catálogo de 133 controles (medidas de seguridad) distribuidos en 11 dominios.

2.7 NORMA ISO 27002

La ISO 27002 anteriormente se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799 (Solutions, 2017). La versión más reciente es la ISO/IEC 27002:2013. Corresponde a un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, que proporciona directrices para la implementación de los controles indicados en ISO 27001. Si bien la ISO 27001 especifica los controles que pueden ser utilizados para mitigar los riesgos de seguridad, y la norma ISO 27002 es bastante útil ya que proporciona más información sobre cómo implementar esos controles.

2.7.1 Estructura de la norma

La norma ISO 27002:2015 se encuentra estructurada en 14 capítulos que describen las áreas que se deben considerar para garantizar la seguridad de la información de las que se dispone:

Sección 1 – Políticas de Seguridad de la Información: Dentro de este capítulo se hace hincapié en la importancia que ocupa la disposición de una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

Sección 2 – Organización de la Seguridad de la Información: Los controles indicados en este capítulo buscan estructurar un marco de seguridad eficiente tanto mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles. Tenemos que tener presente que cada vez es mayor el peso que está ocupando el teletrabajo dentro de las empresas, y por ello, se deben tener en cuenta todas sus características especiales para que ningún momento la seguridad de la información de la que se dispone se vea afectada.

Sección 3 – Seguridad relativa a los recursos humanos: Si analizamos los incidentes de seguridad que se producen en una organización nos daremos cuenta de que la gran mayoría de estos tienen su origen en un error humano. Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir.

Sección 4– Gestión de activos: Se centra en la atención en la información como activo y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, quiebras en la seguridad y en la alteración no deseada.

Sección 5 – Control de acceso: Controlar quien accede a la información dentro de un aspecto relevante. Al fin y al cabo no todas las personas de una organización necesitan

acceder para realizar su actividad diarias a todos los datos, sino que tendremos roles que necesitan un mayor acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, gestión de los privilegios de acceso, etc. siendo algunos de los controles que se incluyen en este apartado.

Sección 6 – Criptografía: En el caso de que estemos tratando la información sensible o crítica puede ser interesante utilizar diferentes técnicas criptográficas para proteger y garantizar su autenticidad, confidencialidad e integridad.

Sección 7 – Seguridad física y del entorno: La seguridad no es solo a nivel tecnológico sino también físico, es decir, una simple labor de no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles, por parte del personal externo los documentos con los que se están trabajando no sólo nos permitirán gestionar de forma adecuada la seguridad sino que se acabarán convirtiendo en hábitos que nos aportan eficiencia en la gestión.

Sección 8 – Seguridad de las operaciones: Tiene un marcado componente técnico entrado en todos los aspectos disponibles como la protección del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc.

Sección 9 – Seguridad de las comunicaciones: Partiendo de la base de que la gran mayoría de los intercambios de información y de datos en distintas escalas se llevan a cabo mediante las redes sociales, garantizar la seguridad y proteger de forma adecuada los medios de transmisión de estos datos clave.

Sección 10 – Adquisiciones, desarrollo y mantenimiento de los sistemas de información: La seguridad no es un aspecto de un área en concreto, ni de un determinado proceso, no que es general, abarca toda la organización y tiene que estar presente como elemento transversal clave dentro del ciclo de vida del sistema de gestión.

Sección 12 – Gestión de incidentes de seguridad de la información: No es posible hablar de controles de seguridad sin mencionar un elemento clave, los incidentes en

seguridad. Es necesario estar preparados para cuando estos incidentes ocurran, dando una respuesta rápida y eficiente siendo la calve para prevenirlos en el futuro.

Sección 13 – Aspectos de seguridad de la información para la gestión de la continuidad de negocio: No sabemos lo que necesitábamos un dato hasta que lo hemos perdido. Sufrir una pérdida de información relevante y no poder recuperarla de laguna forma puede poner en peligro la continuidad de negocio de la organización.

Sección 14 – Seguridad de las operaciones: Tiene un marcado componente técnico entrado en todos los aspectos disponibles como la protección del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc.

Sección 15 – Cumplimiento: No es posible hablar de seguridad de la información, sin hablar de legislación, normas y políticas aplicables que se encuentre relacionadas con este campo y con las que conviven en las organizaciones. Es necesario tener presente que ocupan un enorme lugar en cualquier sistema de gestión y deben garantizar que se cumple y que están actualizados con los últimos cambios.

2.8 Modelo de mejores prácticas

El uso de tecnologías de la información y comunicaciones (TIC) supone beneficios evidentes para todos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios. La seguridad no es una disciplina de todo o nada. No existen sistemas 100% seguros, la seguridad gira en torno a la gestión de riesgos (Ardila, 2017).

Además, es necesario que los usuarios incorporen buenas prácticas para proteger el entorno de información, y prevenir aún más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan sacar provecho de las debilidades humanas.

A continuación se muestra una lista de mejores prácticas en seguridad de la información (Vega, 2007):

- ***Alinearse con los objetivos del negocio***: Antes de pensar en la tecnología a implementar y las políticas a seguir para la protección de una empresa, resulta fundamental analizar cuáles son los objetivos del negocio, sus procesos prioritarios, los activos más importantes, los datos más críticos; porque sólo así se asegurará de forma robusta aquello que realmente es importante para el funcionamiento de la compañía (Vega, 2007). Es necesario analizar las leyes, normativas, disposiciones y reglamentos que regulan al negocio. Es importante también conocer cuál es el grado de riesgo tolerable por la máxima autoridad, que nivel de exposición están dispuestos a asumir; además de clasificar y evaluar la información más crítica para dotarla de mayores controles.

- ***Elaborar un mapa de riesgos***: Una vez que se tiene claros los elementos prioritarios de la organización, es necesario hacer un análisis de riesgos para identificar las amenazas que afectan a los activos de información. Éste análisis debe abarcar desde la infraestructura y los procesos hasta el personal mismo que opera los sistemas, con el objetivo de generar un modelo visual del mapa de riesgos de la organización, que permita exponer a las áreas directivas las potenciales pérdidas de los activos frente a las amenazas, alertando sobre los peligros y el impacto, lo cual ayuda a justificar la inversión solicitada para la seguridad (Vega, 2007).

- ***Diseñar un plan o programa estratégico de seguridad de la información***: En base al análisis de riesgo es necesario elaborar un plan, con sus debidas metodologías y prácticas, pero alineado con el de la compañía, para que todo lo hecho por el área de seguridad vaya en sentido de las iniciativas del negocio (Vega, 2007). Con esto se asegura que todos los esfuerzos estén enfocados en aspectos que le agregan valor a la organización.

- ***Definir e implementar políticas y lineamientos de seguridad***: Estas políticas deben ser flexibles para no entorpecer el normal funcionamiento de la organización ni afectar el trabajo de los usuarios y deben ser transmitidas a través de la estructura jerárquica a fin de que sean implementadas y no pasen únicamente a formar parte de un repositorio de datos.

- ***Capacitar para asegurar***: Es necesario educar a los miembros de la organización respecto a las amenazas que atañen a la información, así como la importancia de aplicar las políticas de protección para no abrir vulnerabilidades. Es necesario generar conciencia en el personal sobre los riesgos generados por su falta de cultura de seguridad o su negligencia, especialmente en aquellos usuarios que tienen acceso a información crítica de la organización (Vega, 2007).

- ***Conformar un equipo y un comité de seguridad***: Una práctica muy recomendable es formalizar la función del oficial de seguridad y su comité de trabajo conformado por especialistas en la materia y con conocimientos en diferentes campos de la misma (Vega, 2007). Es importante que el comité de seguridad sea independiente del área de tecnología para evitar conflicto de intereses.

- ***Desarrollar aplicaciones seguras***: El software desarrollado dentro o fuera de la organización, debe contemplar desde su diseño mismo, los requerimientos de seguridad. Comúnmente los programas se diseñan sin las consideraciones necesarias sobre la seguridad de la información, lo cual se convierte en una vulnerabilidad potencial. Para solventar esta situación es necesario el trabajo conjunto del personal de desarrollo de aplicaciones y el personal encargado de la seguridad informática.

- ***Medir el nivel de seguridad en la compañía***: Se recomiendo evaluar periódicamente el avance y cumplimiento de los controles establecidos para minimizar los riesgos, para determinar si los objetivos planteados se están cumpliendo.

- ***Definir y probar un Plan de Recuperación en Caso de Desastres (DRP)***: Cuando se implementan este tipo de contingencias, es necesario validar que éstas funcionan adecuadamente y que se encuentran actualizadas. Además es necesario hacer una análisis de impacto al negocio, para ver si realmente se está respaldando y recuperando lo verdaderamente importante y si se han contemplado todos los escenarios posibles (Vega, 2007).

Desde luego no existe una receta para establecer que prácticas deben establecerse, cada organización deberá utilizar las que le sean más funcionales.

2.9 Sistemas de Gestión de la Seguridad de la Información (SGSI)

La información, junto con los sistemas que la utilizan y procesos que la soportan son los activos más importantes de toda organización. Mantener la confidencialidad, integridad y disponibilidad de los datos constituye un elemento clave para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

El SGSI es el concepto central sobre el cual se construye la ISO 27000, constituye un conjunto de prácticas para administrar la seguridad de la información. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, así como de los sistemas implicados en su tratamiento, dentro de una organización, mediante la aplicación de políticas y procedimientos establecidos en función de los objetivos de negocio de la organización, minimizando a la vez los riesgos de seguridad de la información.

Es necesario que el proceso del SGSI sea documentado y conocido por toda la organización a través de una estructura jerárquica, desde un enfoque de riesgo empresarial, de esta manera se garantiza de que la seguridad de la información sea gestionada correctamente y sobre todo que su aplicación se ejecute a cabalidad con el respaldo de la alta dirección y no pase únicamente a formar parte de un repositorio de datos.

2.9.1 Implantación de un SGSI

El diseño y la implantación de un SGSI debe ser una decisión estratégica que involucre a toda la organización y esté apoyada por la alta dirección para que asegurar su aplicación. Debe estar alineada con los objetivos del negocio ya tradicional en los sistemas de gestión de calidad (Cortés & Ardila, 2012).

Para establecer y gestionar un SGSI basado en la ISO 27001 se utiliza el Ciclo de Deming o también conocido como PDCA (Plan-Do-Check-Act, esto es, Planificar-Hacer-Verificar-Actuar), la cual constituye una herramienta de mejora continua de la calidad. Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales…).

El círculo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para para ser usada en empresas y organizaciones (Bernal J. , 2013).

Las 4 fases del ciclo de Deming son:

- Planificar: es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- Hacer o implementar: es una fase que envuelve la implantación y operación de los controles.
- Verificar o revisar: es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- Actuar: en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

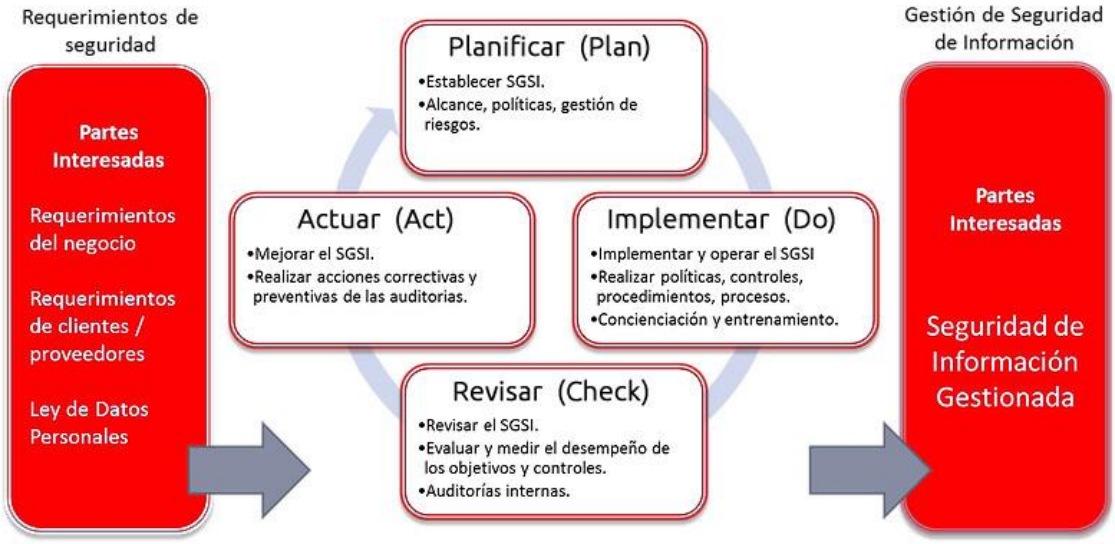


Figura 6. Fases del Sistema de Gestión
Fuente: (ISO 27001 - Sistema de Gestión de Seguridad de la Información)

2.9.2 Beneficios

Innumerables beneficios se derivan de la implementación de un SGSI, beneficios que se centran en los ámbitos empresarial, legal, funcional, comercial, financiero y humano. Aquí una lista de los principales beneficios que aporta:

- Establecer una metodología de Gestión de la Seguridad estructurada y clara y concisa.
- Reducir el riesgo de pérdida de información, ya sea por robo o corrupción de la información sensible.
- Los clientes tienen acceso a la información mediante medidas de seguridad.
- Se realiza una revisión continua de los riesgos a los que se encuentra expuesta la organización, ejecutándose también los controles adecuados.
- Se garantiza la confianza de los clientes y los socios de la organización.
- Las auditorías externas ayudan de forma cíclica a identificar las debilidades del SGSI y las áreas que se deben mejorar.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Permite cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
- La imagen de la organización a nivel internacional mejora.

- Aumenta la confianza y las reglas claras para las personas de la empresa.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

CAPITULO III. METODOLOGÍA

3.1 Descripción del área de estudio

El proyecto se desarrollará en la Empresa Eléctrica Regional Norte Emelnorte cuya matriz se encuentra ubicada en las calles Grijalva 6-54 y Olmedo, en la ciudad de Ibarra, provincia de Imbabura.

Emelnorte es una institución de carácter regional que brinda el servicio de suministro eléctrico en las provincias de Imbabura, Carchi, Esmeraldas, norte de Pichincha y Sucumbíos. Cuenta con agencias de atención al cliente ubicadas estratégicamente en las cabeceras cantonales para brindar un servicio de calidad y más cercano a los clientes (Emelnorte, ACTUALIZACIÓN PLAN ESTRATÉGICO 2014 - 2017, 2014).

La siguiente información ha sido tomada del documento del Plan estratégico Institucional elaborado por la institución en el año 2014:

3.1.1 Visión

Seremos al año 2017, una empresa pública que entregue a la comunidad, el servicio de energía eléctrica, en concordancia con los índices fijados por los organismos de control, con excelencia de categoría internacional, compromiso social y ambiental.

3.1.2 Misión

Brindar el servicio público de energía eléctrica con calidad, calidez, responsabilidad social y ambiental a la población del área de cobertura.

3.1.3 Unidad Ejecutora

El presente proyecto se desarrollará en la Dirección de Tecnologías de Información y Comunicaciones, que se encuentran en el edificio matriz de Emelnorte ubicado en la calle Grijalva 6-54 y Olmedo de la ciudad de Ibarra, provincia de Imbabura.

3.1.4 Beneficiarios

El proyecto tiene impacto sobre toda el área de concesión de Emelnorte que incluye las provincias de Esmeraldas, Carchi, Imbabura, Sucumbíos y Pichincha, en las cuales se ubican agencias para recaudación y atención al público. El trabajo se desarrollará sobre un proceso de negocio de la empresa, el cual se ejecuta tanto en la matriz como en todas las agencias de la institución.

3.2 Tipo de investigación

La investigación tendrá un enfoque cuantitativo por cuanto se usarán instrumentos de medición para tabular las encuestas realizadas y medir el impacto de los riesgos encontrados. El software para la automatización del SGSI realizará el registro y análisis de los indicadores determinados para medir la seguridad del proceso piloto.

La modalidad de la investigación será bibliográfica y de campo por cuanto se hará uso de la bibliografía existente para su desarrollo, así como también se buscará información de los procesos que se ejecutan dentro de la institución.

3.3 Diseño de la Investigación

3.3.1 Modalidad de Investigación

Para llevar a efecto la presente indagación se utilizó algunos tipos de investigación como es: de Campo, Documental, bibliográfica.

- **Investigación de Campo.-** Se realiza la observación de los deferentes equipos, sistemas, componentes que se maneja en la Dirección de TIC y en las áreas de atención al cliente para verificar los fenómenos objetos de estudio.

- **Investigación Documental.-**. Se realiza la revisión de la información que dispone la Dirección de TIC en cuanto a procedimientos, políticas, reglamentación interna, etc.; información que infiere directamente sobre el objeto de estudio.

- **Investigación Bibliográfica.-** Se realiza la revisión de la bibliografía existente para estudiar todos los aspectos que se encuentran involucrados con el proyecto, conocer el estado del arte sobre el tema planteado y desarrollar así la fundamentación científica, filosófica y legal.

3.3.2 Niveles de Investigación

- **Investigación Exploratoria:** Se realizó una investigación de campo a un nivel exploratorio para determinar el nivel de satisfacción y conocimiento que tienen los usuarios sobre la seguridad de la información. Este estudio se realizó a usuarios del área comercial, financiero y de tecnología.

- **Investigación Descriptiva.-** Se realizó un estudio para determinar el estado actual de la seguridad de la información en Emelnorte.

3.4 Métodos

Deductivo: "La deducción es un proceso que parte de un principio general ya conocido para inferir de él, consecuencias particulares" (Gutiérrez, 2006).

Este método permite partir de modelos generales para el diseño de las estrategias y recursos que se implementarán en el Plan de Seguridad de la Información de Emelnorte.

Inductivo: "Este Método utiliza el razonamiento para obtener conclusiones que parten de hechos particulares aceptados como válidos, para llegar a conclusiones cuya aplicación sea de carácter general. El método se inicia con un estudio individual de los hechos y se formulan conclusiones universales que se postulan como leyes, principios o fundamentos de una teoría" (Bernal C. A., 2010).

Permitirá analizar los datos obtenidos en el diagnóstico para llegar a determinar las estrategias, recursos, materiales y medios que intervienen en el proceso de desarrollo e implementación del Plan de Seguridad Informático.

Analítico – Sintético: "El análisis consiste en descomponer en partes algo complejo, en desintegrar un hecho o una idea en sus partes, para mostrarlas,

describirlas, numerarlas y para explicar las causas de los hechos o fenómenos que constituyen el todo" (Leiva, 2010).

Con este método se realizará un análisis del tipo de información que se manejará al alcance de la Dirección de Tecnologías, servirá de base para los procesos de implementación de las herramientas de gestión.

3.5 Estrategias Técnicas

Se utilizarán las siguientes técnicas:

- Entrevista: Se aplicará al personal de la Dirección de Tecnologías de la Información y Comunicaciones.

- Encuesta: Una técnica que se usará en la investigación para poder medir los riesgos detectados en los usuarios de los sistemas informáticos, específicamente, en los usuarios del Sistema Comercial en el área de atención al cliente.

- Observación Directa: Se la realizará mediante visitas a las instalaciones de la Institución en el Departamento de Tecnologías y poder verificar el funcionamiento de los sistemas, equipos y demás, así como las actividades que se desarrollan sobre el enfoque del tema planteado.

3.6 Instrumentos

Los instrumentos que se emplearán serán:

- Para el caso de la entrevista y la encuesta las preguntas del cuestionario,
- Para la observación se utilizará como instrumento la ficha de observación.
- Celular; como equipo de comunicación.
- Cámara fotográfica, que facilite recabar evidencia de la investigación

3.7 Aplicación de la encuesta

La encuesta aplicada tiene como objetivo conocer de forma general el estado de la seguridad de la información dentro de la empresa. Las preguntas de la encuesta están dirigidas a conocer las medidas de seguridad básicas que deben tener los usuarios para mantener la seguridad de la información y para conocer además el nivel de satisfacción del servicio y seguridad brindado por TIC.

Las entrevistas se las realizará al personal de la Dirección de Tecnologías y las encuentras se ejecutarán a un total de 50 usuarios del Sistema Comercial y usuarios de TICs.

3.7.1 Población y Muestra

4 Se considera como población al grupo de usuarios que tienen acceso a los servicios informáticos de Emelnorte en cualquiera de los sistemas de producción. La muestra corresponde a los usuarios del área comercial y área de TICs, que de alguna forma acceden a los sistemas informáticos para registro de información, ejecución de procesos, etc.

4.1.1 Recolección de la Información

Para la recolección de la información se aplicó una encuesta a 50 empleados que laboran dentro de la institución. Par realizar le encuesta se utilizó la herramienta gratuita de google para formularios.

La encuesta practicada se diseñó para medir criterios de seguridad general, en las dimensiones de disponibilidad, confidencialidad e integridad de la información, como la disponibilidad de los servicios, respaldo de información y acceso de usuarios a sistemas informáticos; criterios que son tratados por la norma ISO 27001.

A continuación se muestra la encuesta realizada:

Encuesta sobre seguridad - EMELNORTE

La encuesta aplicada tiene como objetivo conocer de forma general el estado de la seguridad de la información dentro de la empresa. Las preguntas de la encuesta están dirigidas a conocer las medidas de seguridad básicas que deben tener los usuarios para mantener la seguridad de la información.

1. **¿Dispone de clave de seguridad para acceder a su computador?**
   Selecciona todos los que correspondan.
   - ☐ SI
   - ☐ NO

2. **¿Con que frecuencia cambia la clave de seguridad para acceder a su computador?**
   Selecciona todos los que correspondan.
   - ☐ Cada 15 días
   - ☐ Cada 30 días
   - ☐ Más de 30 días

3. **Califique de un nivel de 1 a 5 el servicio de sistemas informáticos prestado por TIC**
   Marca solo un óvalo.

1	2	3	4	5
◯	◯	◯	◯	◯

4. **En la escala del 1 al 5, con que frecuencia se producen suspensiones de los sistemas informáticos, donde 1 es poco frecuente y 5 es muy frecuente**
   Marca solo un óvalo.

1	2	3	4	5
◯	◯	◯	◯	◯

5. **¿Dispone de un respaldo de los archivos más importantes de su computador?**
   Selecciona todos los que correspondan.
   - ☐ SI
   - ☐ NO

6. **¿Conoce sobre políticas de seguridad establecidas en su institución?**
   Selecciona todos los que correspondan.
   - ☐ SI
   - ☐ NO

Figura 7. Fases del Sistema de Gestión
Fuente: Investigadora

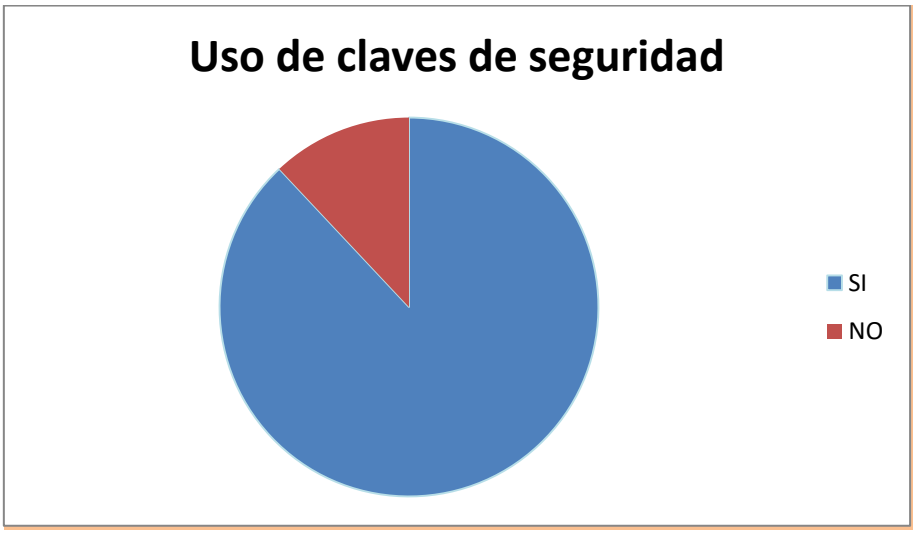
4.1.2 Análisis e interpretación de resultados

De la aplicación de la encuesta y el procesamiento de los resultados se obtiene los siguientes cuadros de resumen:

Pregunta 1: ¿Dispone de clave de seguridad para acceder a su computador?

Alternativas	Número	Porcentaje
SI	44	88 %
NO	6	12 %
Total	50	100%

Elaborado por: Investigadora

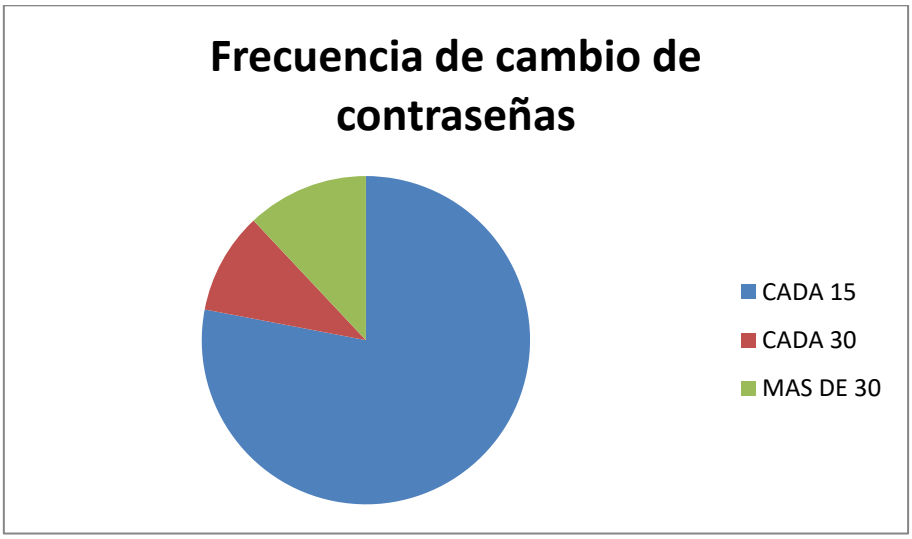


Interpretación: La mayoría de usuarios disponen de una clave de seguridad para ingresar a su computador, esta es una política de la Dirección de TIC para asegurar la información de los usuarios. Los computadores de los usuarios que no disponen de clave de seguridad no se encuentran registrados dentro del dominio.

Pregunta 2: ¿Con qué frecuencia cambia la clave de seguridad para acceder a su computador?

Alternativas	Número	Porcentaje
CADA 15	39	78 %
CADA 30	5	10 %
MAS DE 30	6	12%
TOTAL	50	100%

Elaborado por: Investigadora



Interpretación: El cambio de contraseña es una política del dominio de red que mantiene la institución. La mayoría de los usuarios realizan el cambio de clave cumpliendo con la política establecida.

Pregunta 3: Califique de un nivel de 1 a 5 el servicio de sistemas informáticos prestado por TIC, donde, 5 es excelente y 1 es malo.

Alternativas	Número	Porcentaje
NIVEL 1	2	4 %
NIVEL 2	6	12%
NIVEL 3	5	10%
NIVEL 4	27	54%
NIVEL 5	10	20%
TOTAL	50	100%

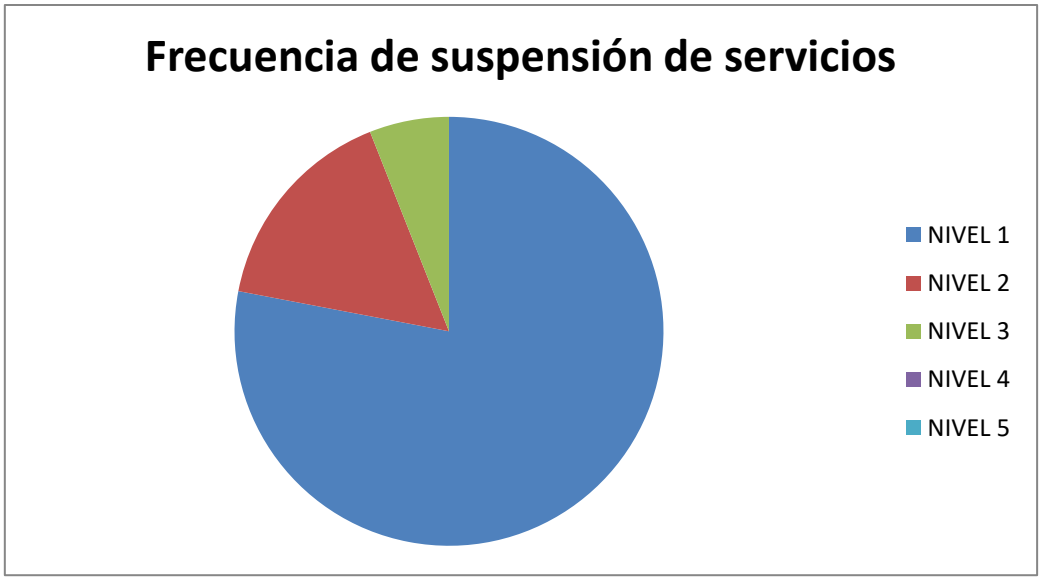
Elaborado por: Investigadora

Interpretación: En general, los usuarios de los sistemas informáticos tienen buena aceptación de los servicios prestados por TIC.

Pregunta 4: Califique del 1 al 5 la frecuencia con la que se producen suspensiones de los sistemas informáticos, donde 1 es poco frecuente y 5 es muy frecuente.

Alternativas	Número	Porcentaje
NIVEL 1	39	78%
NIVEL 2	8	16%
NIVEL 3	3	6%
NIVEL 4	0	0%
NIVEL 5	0	0%
TOTAL	50	100%

Elaborado por: Investigadora

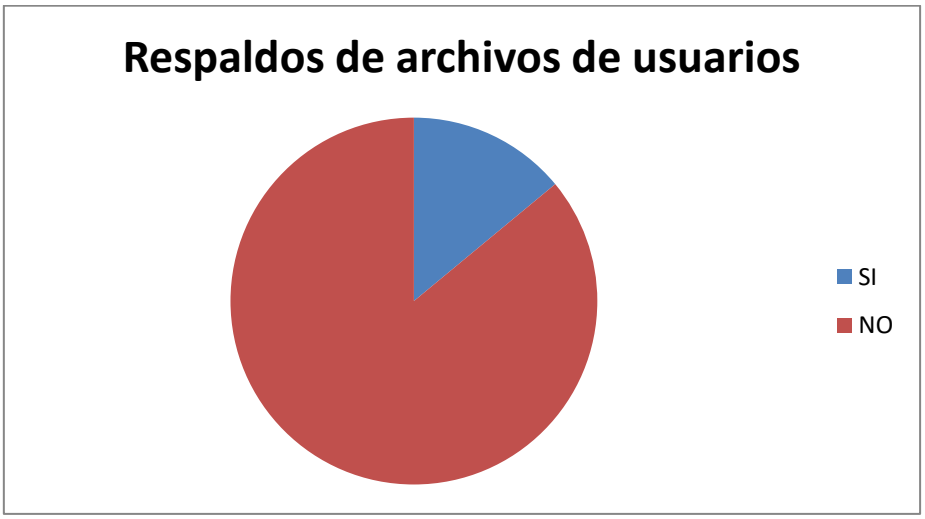


Interpretación: Para la mayoría de usuarios, las caídas de los sistemas son muy poco frecuentes Existen caídas de los servicios debido a errores inesperados o mantenimientos mal planificados.

Pregunta 5: ¿Dispone de un respaldo de los archivos más importantes de su computador?

Alternativas	Número	Porcentaje
SI	7	14%
NO	43	86%
TOTAL	50	100%

Elaborado por: Investigadora

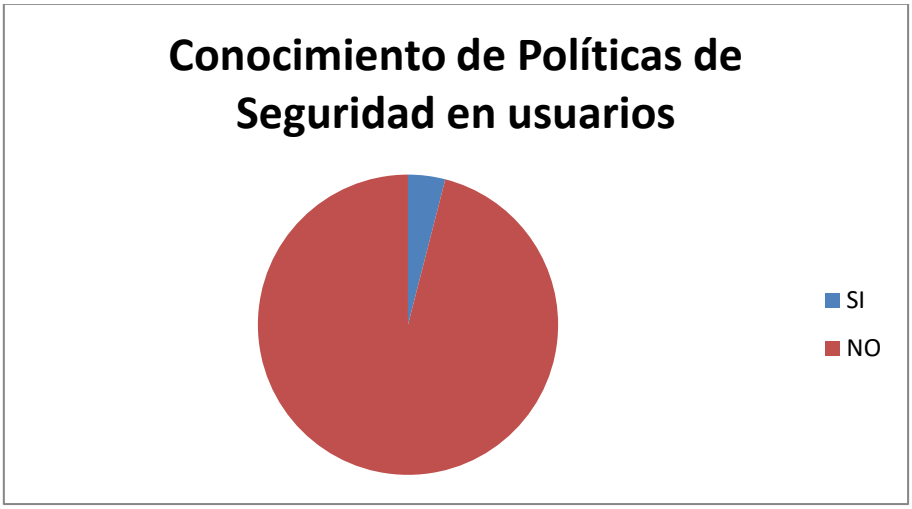


Interpretación: La mayoría de los usuarios no disponen de respaldos de su información por lo que en caso de daños de hardware, la información no puede ser recuperada.

Pregunta 6: ¿Conoce sobre políticas de seguridad establecidas en su institución?

Alternativas	Número	Porcentaje
SI	2	4%
NO	48	96%
TOTAL	50	100%

Elaborado por: Investigadora



Interpretación: No existe un conocimiento general sobre políticas de seguridad de la información, no existen procedimientos formales establecidos.

4.2 Aplicación de le entrevista

Se aplicó la entrevista al personal de la Dirección de Tecnologías de Información y Comunicaciones.

4.2.1 Entrevista personal de Redes y Comunicaciones.

Se entrevistó al Ing. Xavier Brito para conocer el estado de la seguridad a nivel de la red de la empresa. Se obtuvo la siguiente información:

- **Pregunta**: ¿Disponen ustedes de un equipo de seguridad perimetral?
  Respuesta: Si, disponemos de en equipo firewall Checkpoint adquirido en el año 2010, que da servicio a toda todas las agencias de la empresa.

- **Pregunta**: ¿Qué tipo de comunicaciones se manejan para la comunicación de los usuarios?
  Respuesta: Tenemos comunicaciones con cobre, fibra óptica, antena, y un enlace satelital.

- **Pregunta**: ¿Con cuántos servidores disponen en el Centro de Datos?
  Respuesta: Actualmente tenemos alrededor de 37 servidores físicos y 20 servidores virtuales.

- **Pregunta**: ¿Qué sistema de virtualización tienen implementado?
  Respuesta: Tenemos instalado vmware 6.1 con una consola de administración Vcenter para la gestión y monitoreo de los servidores virtuales.

- **Pregunta**: ¿Disponen de políticas de respaldos de información?
  Respuesta: Tenemos una política desarrollada pero no aprobada. Se obtienen respaldos diarios de bases de datos y semanales de aplicaciones.

4.2.2 Entrevista personal de Soporte y Atención a usuarios.

Se entrevistó al Ing. Vinicio Vallejos para conocer el proceso de atención y soporte a usuarios, conocer las vulnerabilidades y ataques comunes entre los usuarios de la empresa. Se obtuvo la siguiente información:

- **Pregunta**: ¿Disponen actualmente de antivirus corporativo?
  Respuesta: Si, tenemos instalado ESET EndPoint, el cual se encuentra instalado en 343 computadores entre computadores de usuario y servidores.

- **Pregunta**: ¿Con cuántos usuarios de sistemas informáticos cuentan?
  Respuesta: Al momento contamos con 347 usuarios distribuidos en agencias y edificio matriz.

- **Pregunta**: ¿Se obtienen respaldos de equipos de usuarios?
  Respuesta: No, al momento cada usuario es responsable de su información.

- **Pregunta**: ¿Cuántos incidentes o problemas por virus se reportan semanalmente?
  Respuesta: En los últimos 7 días se han detectado 237 amenazas, según el reporte del antivirus ESET.

4.3 Metodología de Desarrollo

El desarrollo del programa informático requerirá de la aplicación de una metodología de desarrollo ágil, en este caso se utiliza Extreme Programming (XP), con la que se obtiene métodos sencillos para el desarrollo de software de calidad (Wells, 2003), tomando en cuenta el proceso de software que implica las siguientes fases.

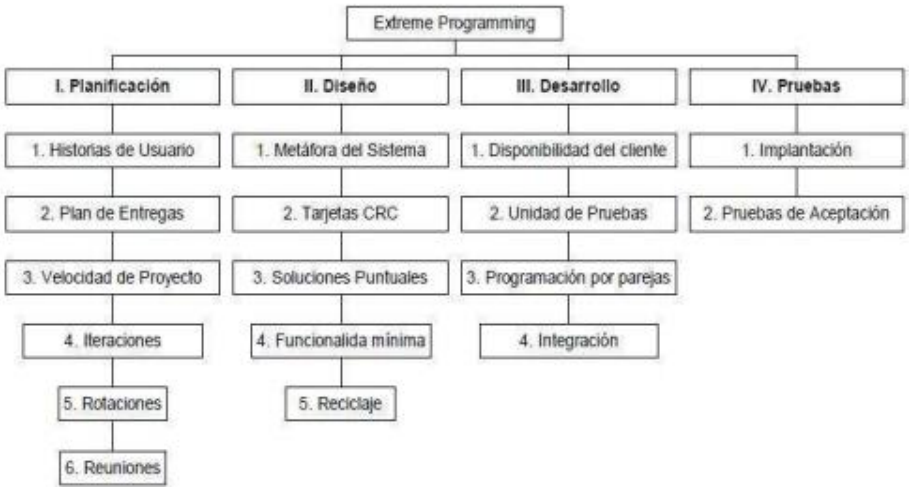


Figura 8. Fases de la Metodología XP
Fuente: (Batalla, 2006)

4.3.1 Fase de Planificación

En esta etapa se planifica el proyecto en sí, se identifica el problema y se definen las historias de usuarios, las mismas que se cumple entre el cliente y los programadores, además permite conocer el proceso de negocio. Cabe mencionar que la planificación del proyecto se realiza de manera general para determinar el alcance, la duración y el costo. Una vez que el cliente acepta llevar a cabo las tareas de desarrollo, se establecen las reuniones con el usuario, el mismo que permitirá cumplir con las fases de la metodología ágil seleccionada (Batalla, 2006).

Historias de usuario: El primer paso de cualquier proyecto que siga la metodología X.P es definir las historias de usuario con el cliente. Las historias de usuario tienen la misma finalidad que los casos de uso, pero con algunas diferencias: Constan de 3 ó 4 líneas escritas por el cliente en un lenguaje no técnico sin hacer mucho hincapié en los detalles; no se debe hablar ni de posibles algoritmos para su implementación ni de diseños de base de datos adecuados, etc.

Son usadas para estimar tiempos de desarrollo de la parte de la aplicación que describen. También se utilizan en la fase de pruebas, para verificar si el programa cumple con lo que especifica la historia de usuario. Cuando llega la hora de implementar una historia de usuario, el cliente y los desarrolladores se reúnen para concretar y detallar lo que tiene que hacer dicha historia. El tiempo de desarrollo ideal para una historia de usuario es entre 1 y 3 semanas (Canós & Penadés, 2004).

4.3.2 Fase de Diseño

En esta fase se genera las especificaciones de casos de uso para que el proyecto cumpla con los requerimientos definidos en la fase anterior, además de artefactos como: metáfora del sistema, modelo de clases y diseño de los prototipos en papel, que deberán contemplar las posibles modificaciones que se den al aplicativo.

4.3.3 Fase de Construcción

El propósito de esta fase es desarrollar los prototipos que servirán de base para la determinación de los criterios de usabilidad, para ello se clarifica los requisitos pendientes y todas las características se prueban a fondo. Así mismo, en esta etapa los involucrados en el desarrollo deberán tomar decisiones sobre la inclusión de nuevas características a la versión actual.

Esta fase incluye varias iteraciones sobre el sistema antes de ser entregado. El Plan de Entrega está compuesto por iteraciones de no más de tres semanas. En la primera iteración se puede intentar establecer una arquitectura del sistema que pueda ser utilizada durante el resto del proyecto. Esto se logra escogiendo las historias que fuercen la creación de esta arquitectura, sin embargo, esto no siempre es posible ya que es el cliente quien decide qué historias se implementarán en cada iteración (para maximizar el valor de negocio). Al final de la última iteración el sistema estará listo para entrar en producción. Los elementos que deben tomarse en cuenta durante la elaboración del Plan de la Iteración son: historias de usuario no abordadas, velocidad del proyecto, pruebas de aceptación no superadas en la iteración anterior y tareas no terminadas en la iteración anterior. Todo el trabajo de la iteración es expresado en tareas de programación, cada una de ellas es asignada a un programador como responsable, pero llevadas a cabo por parejas de programadores (Fowler, 2003).

4.3.4 Fase de Implantación

En esta fase se requiere de pruebas adicionales y revisiones de rendimiento antes de que el sistema sea trasladado al entorno del cliente. Al mismo tiempo, se deben tomar decisiones sobre la inclusión de nuevas características a la versión actual, debido a cambios durante esta fase. Es posible que se rebaje el tiempo que toma cada iteración, de tres a una semana. Las ideas que han sido propuestas y las sugerencias son documentadas para su implementación (Jeffries, 2001).

CAPITULO IV. PROPUESTA

4.1 Introducción

Emelnorte es una empresa dedicada a la generación, distribución y venta de energía eléctrica con más de 50 años de vida institucional, tiempo durante el cual ha implementado y afinado sus procesos para convertirse en una de las mejores del país.

Actualmente, Emelnorte cuenta con procesos de negocios claramente definidos y la tecnología necesaria para implementarlos de una forma óptima, sin embargo no se ha trabajado en lo correspondiente a la seguridad de la información basada en estándares y normas. Por esta razón se desarrolla el presente trabajo como un proyecto piloto que deberá ser aplicado e implementado en todos los procesos de negocio de la institución.

4.2 Alcance del SGSI

El Sistema de Gestión de Seguridad de la Información debe desarrollarse para todos los procesos de negocio de la organización, utilizando el ciclo de Deming o PDCA, sin embargo, para el desarrollo del presente trabajo, se tomará como piloto el proceso de ATENCIÓN DE NUEVOS CLIENTES que corresponde al macro proceso de COMERCIALIZACIÓN DE ENERGÍA ELÉCTRICA que se ejecuta en la Dirección Comercial, el cual es considerado como un proceso crítico dentro de la institución.

4.3 Procesos de Negocio

EmelNorte	**MACROPROCESO:** COMERCIALIZACIÓN DE ENERGÍA ELÉCTRICA	**CODIGO** COM.1. **VERSION** 1.0 **FECHA DE ELABORACIÓN:** 23-08-2011
CARACTERIZACIÓN	**PROCESO** ATENCION DE NUEVOS CLIENTES	**FECHA ULTIMA REVISIÓN:** 23-08-2011 **PÁGINA**

A. OBJETIVO:

Regular las actividades de instalación del servicio de energía eléctrica en la zona de concesión de la empresa Eléctrica del Norte.

B. ALCANCE:

El proceso de atención de nuevos clientes comienza con la solicitud de instalación del servicio por parte del cliente y culmina con el ingreso de los clientes al sistema para facturación.

C. RESPONSABLE:

- Director de comercialización
- Jefe de agencias
- Jefe de acometidas y medidores
- Jefe de clientes

D. REQUISITOS LEGALES:

- Ley de régimen del sector eléctrico y su reglamento
- Ley de defensa del consumidor
- Reglamentos y Regulaciones del CONELEC

E. POLÍTICAS INTERNAS:

F. SUBPROCESOS:

El proceso de atención de nuevos clientes tiene lo siguientes subprocesos:

SUBPROCESO	PERIODICIDAD
Ingreso de Clientes	Continuo

Figura 9. Proceso de Atención de nuevos clientes
Fuente: (Emelnorte, Levantamiento de procesos de negocio, 2012)

EmelNorte	**MACROPROCESO:**	**CODIGO** COM.1.1
	COMERCIALIZACIÓN DE ENERGÍA ELÉCTRICA	**VERSION** 1.0
	PROCESO:	**FECHA DE ELABORACION:** 23-08-2011
	ATENCIÓN DE CLIENTES NUEVOS	**FECHA ULTIMA REVISION** 23-08-2011
DIAGRAMA DE FLUJO FUNCIONAL	**SUBPROCESO:**	**PAGINA**
	INGRESO DE CLIENTES	

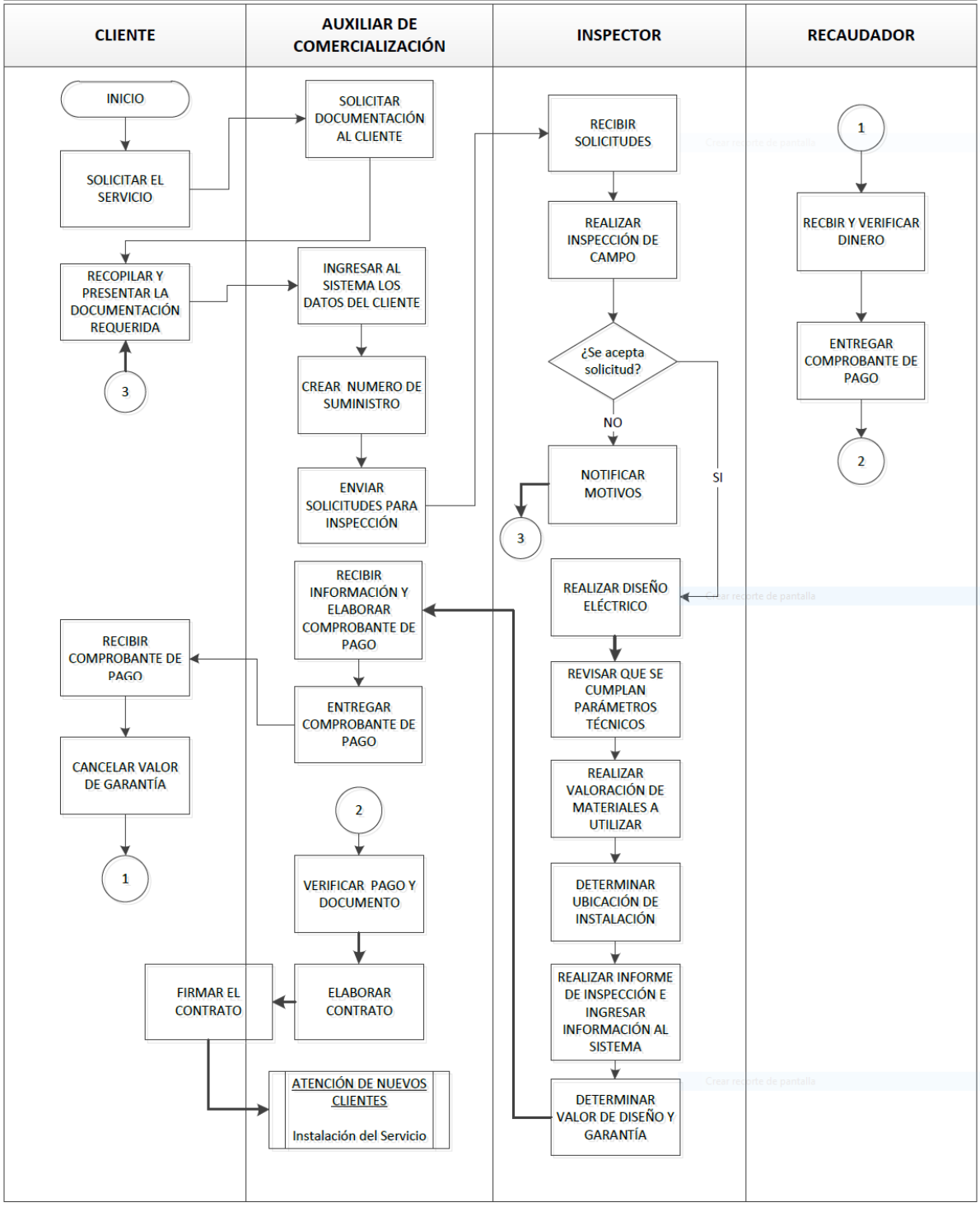


Figura 10. Subproceso Ingreso de clientes
Fuente: (Emelnorte, Levantamiento de procesos de negocio, 2012)

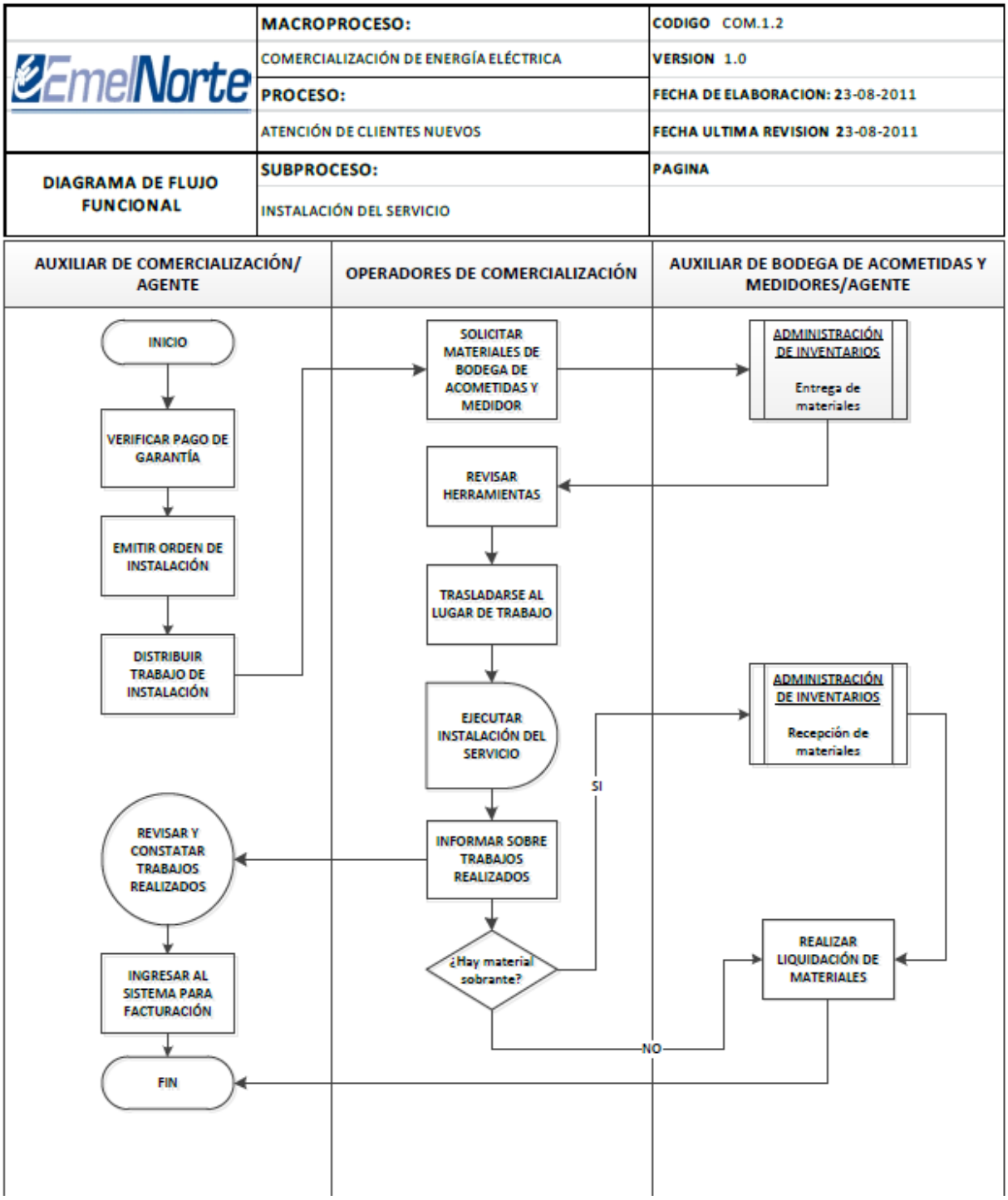


Figura 11. Subproceso de instalación del servicio
Fuente: (Emelnorte, Levantamiento de procesos de negocio, 2012)

4.4 Organigrama estructural

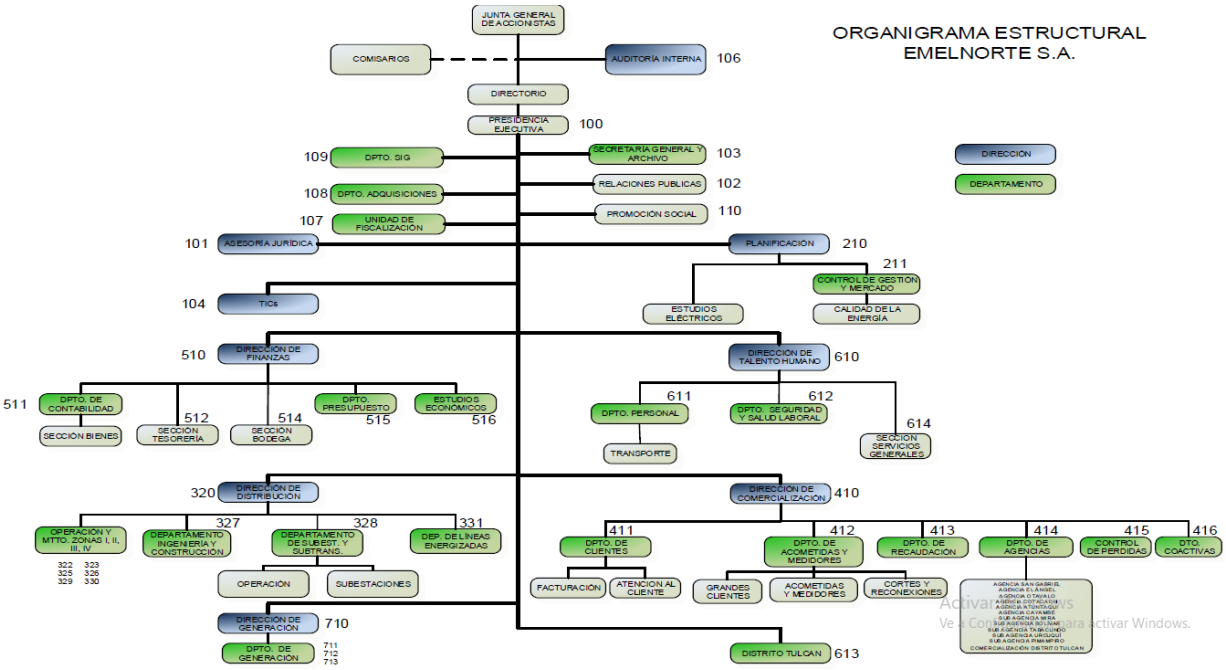


Figura 12. Organigrama estructural de Emelnorte
Fuente: (Emelnorte, ACTUALIZACIÓN PLAN ESTRATÉGICO 2014 - 2017, 2014)

4.5 Política del SGSI

La Dirección Tecnologías de la Información y Comunicaciones de Emelnorte reconoce la importancia de identificar y proteger los activos de información de la organización, evitando la destrucción, divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, servicios, y otros conceptos relacionados. En consecuencia, se compromete a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de asegurar la confidencialidad, disponibilidad e integridad de la información.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas (MINTIC, 2016):

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de sus clientes, socios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de EMELNORTE
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ EMELNORTE, a través de la Dirección de TICs, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Es estos efectos, la Dirección de TICs se compromete:

- Se establezcan anualmente objetivos con relación a la Seguridad de la Información.
- Se desarrolle un proceso de análisis del riesgo y de acuerdo a su resultado, se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables.
- Se establezcan los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgos surjan del proceso de análisis de riesgos manejado.
- Se cumpla con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad
- Se brinde concientización y entrenamiento en materia de seguridad de la información a todo el personal.
- Se establezcan los medios necesarios para garantizar la continuidad del funcionamiento de la institución.
- Se sancione cualquier violación a esta política y a cualquier política o procedimiento del SGSI.

- Todo funcionario es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.
- Todo funcionario es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.
- Nombrar un Jefe de Seguridad de la Información, el cual será responsable directo sobre el mantenimiento de esta política, por brindar consejo y guía para su implementación, e investigar toda violación reportada por el personal del Instituto.

4.6 Análisis de Riesgos

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización. El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y vulnerabilidades (MAGERIT – versión 3.0, 2012).

El levantamiento de información para el análisis de riesgos se lo realizó con la ayuda del personal de la Dirección Comercial y la Dirección de TIC que son los directamente involucrados.

4.6.1 Caracterización de los activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia (MAGERIT – versión 3.0, 2012).

4.6.1.1 Identificación de activos

Objetivo: Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados.

En esta actividad se identifica todos los activos de información que se relacionan con el proceso de ATENCION DE NUEVOS CLIENTES.

Tabla de tipos de activos:

Tabla 6. *Tabla tipos de activos*

CODIGO TIPO	DESCRIPCIÓN
[D]	Datos / Información
[K]	Claves criptográficas
[S]	Servicios
[SW]	Software / Aplicaciones informáticas
[HW]	Equipamiento informático(hardware)
[COM]	Redes de Comunicaciones
[Media]	Soportes de información
[AUX]	Equipamiento Auxiliar
[L]	Instalaciones
[P]	Personal

Fuente: (MAGERIT – versión 3.0, 2012)

4.6.1.2 Valoración de activos

Los activos de información se deben valorar de acuerdo a su impacto en términos de la pérdida de los tres principios básicos de la seguridad de la información que son: la Confidencialidad, la Integridad y la Disponibilidad.

En sistemas dedicados a servicios de la sociedad de la información como puedan ser los de administración electrónica o comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos que pudieran darse. En esos casos es útil valorar la autenticidad y la trazabilidad.

Las dimensiones en las que se valoran los activos son:

- **[D] Disponibilidad**: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren (MAGERIT – versión 3.0, 2012).
- **[I] Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada (MAGERIT – versión 3.0, 2012).
- **[C] Confidencialidad**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados (MAGERIT – versión 3.0, 2012).

Partiendo de las tres características de la seguridad de la información y el valor económico, se establece la escala de calificación que contempla cinco niveles de impacto:

Tabla 7. *Adaptación de escala para valoración de activos*

VALORACIÓN	VALORACIÓN CUALITATIVA

CUANTITATIVA	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente: (MAGERIT – versión 3.0, 2012)
Modificado por: Investigadora

Para la valoración del activo en cada principio de seguridad se utiliza las siguientes consideraciones:

Valoración en Confidencialidad (C):

Tabla 8. *Tabla para valoración de la confidencialidad del activo*

ESCALA CUANTITATIVA	ESCALA CUALITATIVA	DESCRIPCION
1	Muy Bajo	Se puede acceder por cualquier usuario.
2	Bajo	Se puede acceder solo por empleados o contratistas de la organización.
3	Medio	Se puede acceder por Líderes de Proceso.
4	Alto	Sólo es posible el acceso para las personas citadas en lista de control de acceso
5	Muy Alto	Solo es posible el acceso por personal de la Alta Dirección

Fuente: (MAGERIT – versión 3.0, 2012)
Modificado por: Investigadora

Valoración en Integridad (I):

Tabla 9. *Tabla para valoración de la integridad del activo*

ESCALA CUANTITATIVA	ESCALA CUALITATIVA	DESCRIPCION
1	Muy Bajo	Puede ser modificado en cualquier momento por cualquier usuario.
2	Bajo	Es posible la modificación por cualquier funcionario o contratista de la organización.
3	Medio	Es posible la modificación por líderes de proceso.
4	Alto	Sólo se modifica bajo autorización del comité de gerencia.
5	Muy Alto	Solo se modifica con autorización de la Alta Dirección.

Fuente: (MAGERIT – versión 3.0, 2012)
Modificado por: Investigadora

Valoración en Disponibilidad (D):

Tabla 10. *Tabla para valoración de la disponibilidad del activo*

ESCALA CUANTITATIVA	ESCALA CUALITATIVA	DESCRIPCION
1	Muy Bajo	El activo no está disponible por 1 semana y no afecta a la Organización.
2	Bajo	El activo no está disponible hasta por 3 días y no afecta a la organización.
3	Medio	El activo no está disponible hasta por 1 día y no afecta a la organización.
4	Alto	El activo no está disponible hasta por 4 horas.
5	Muy Alto	El activo debe estar disponible siempre.

Fuente: (MAGERIT – versión 3.0, 2012)
Modificado por: Investigadora

El valor del activo está dado por:

Valor del activo = C + D + I

Dónde:

C= Confidencialidad, D=Disponibilidad, I=Integridad

Tabla 11. *Activos identificados*

CODIGO	NOMBRE	DESCRIPCION	TIPO	U. RESP.	PER. RESP.	UBICACION	CANT.	D	I	C	VALOR
SW_SIEEQ	SIEEQ	Sistema Comercial de la EEQ	SW	TICS	Ing. Fernando Rea	Servidor srvcitrix Data Center matriz	1	5	5	4	14
SW_CTX	APLICACION CITRIX	Aplicación Citrix instalada en el servidor	SW	TICS	Ing. Fernando Rea	Servidor srvcitrix Data Center matriz	1	5	5	4	14
SW_SO_CTX	SISTEMA OPERATIVO CITRIX	Sistema operativo del servidor citrix	SW	TICS	Ing. Catalina Gordillo	Servidor srvcitrix Data Center matriz	1	5	5	4	14
SW_ESX	VIRTUALIZACIÓN DE SERVIDORES	Sotfware para virtualización de servidores	SW	TICS	Ing. Catalina Gordillo	Servidores blade Data Center matriz	8	4	5	4	13
SW_BD_EERN	BASE DE DATOS EERN	Sistema de gestión de base de datos para el Sistema Comercial	SW	TICS	Ing. Catalina Gordillo	Servidor srvdbeern Data Center matriz	1	5	5	4	14
SW_SO_BD	SISTEMA OPERATIVO BDD	Sistema operativo del servidor de base de datos EERN	SW	TICS	Ing. Catalina Gordillo	Servidor srvdbeern Data Center matriz	1	5	5	4	14
SW_SO_DOM	SISTEMA OPERATIVO DOMINIO	Sistema operativo del servidor de dominio principal	SW	TICS	Ing. Catalina Gordillo	Servidor srvdcp Data Center matriz	1	4		4	8
SW_SO_DOM_SEC	SISTEMA OPERATIVO DOMINIO SEC	Sistema operativo del servidor de dominio secundario	SW	TICS	Ing. Catalina Gordillo	Servidor ml3503gperdidas Data Center matri	1	4		4	8
SW_SO_MAIL	SISTEMA OPERATIVO MAIL	Sistema operativo del servidor de correo institucional	SW	TICS	Ing. Catalina Gordillo	Servidor mail Data Center matriz	1	4		4	8
SW_SO_ATVR	SISTEMA OPERATIVO ANTIVIRUS	Sistema operativo del servidor de antivirus	SW	TICS	Ing. Catalina Gordillo	Servidor srveset Data Center matriz	1	1			1
SW_SO_TELF	SISTEMA OPERATIVO TELEFONIA	Sistema operativo del servidor de telefonía	SW	TICS	Ing. Cristina Orejuela	Servidor srvteliba Data Center matriz	1	4		4	8
HW_SRVBL	SERVIDORES BLADE	Servidor donde se alojan las máquinas virtuales	HW	TICS	Ing. Catalina Gordillo	Chasis blade Data Center matriz	8	4			4
HW_CHASIS	CHASIS BLADE	Equipo donde se conectan los servidores blade	HW	TICS	Ing. Catalina Gordillo	Data Center matriz	1	5	4		9
HW_SAN	SISTEMA DE ALMACENAMIENTO	Sistema de almacenamiento donde se alojan los servidores virt	HW	TICS	Ing. Catalina Gordillo	Data Center matriz	1	5	5	4	14
HW_DOM	SERVIDOR DE DOMINIO	Equipo servidor de dominio principal	HW	TICS	Ing. Catalina Gordillo	Data Center matriz	1	4			4
HW_DOM_SEC	SERVIDOR DE DOMINIO SECUNARIO	Equipo servidor de dominio secundario	HW	TICS	Ing. Catalina Gordillo	Data Center matriz	1	4			4
HW_MAIL	SERVIDOR DE CORREO INSTITUCION	Equipo servidor de correo institucional	HW	TICS	Ing. Catalina Gordillo	Data Center matriz	1	4			4
HW_TELF	SERVIDOR TELEFONIA	Servidor de telefonía	HW	TICS	Ing. Cristina Orejuela	Data Center matriz	1	4		4	8
HW_FIREWALL	FIREWALL	Equipo de seguridad perimetral	HW	TICS	Ing. Xavier Brito	Data Center matriz	1	4	5	4	13
HW_SW_ACC	SWITCH ACCESO	Switch de acceso de cada agencia de la empresa	HW	TICS	Ing. Xavier Brito	Agencias de Emelnorte	13	4			4
HW_SW_CORE	SWITCH CORE	Switch core del edificio matriz	HW	TICS	Ing. Xavier Brito	Data Center matriz	1	5	5	4	14
HW_AAB	ADMINISTRADOR ANCHO DE BAND/	Equipo administrador de ancho de banda	HW	TICS	Ing. Xavier Brito	Data Center matriz	1	1			1
HW_RT	ROUTER	Equipos de ruteo	HW	TICS	Ing. Xavier Brito	Agencias de Emelnorte	1	3			3
S_DOM	DOMINIO	Servicio de Dominio	S	TICS	Ing. Xavier Brito	Servidor srvdcp Data Center matriz	1				0
S_TS	TERMINAL SERVER	Servicio de terminal server para conectarse a citrix	S	TICS	Ing. Xavier Brito	Servidor ml35036perdidas Data Center matri	1				0
S_MAIL	SERVICIO DE CORREO	Servicio de correo institucional	S	TICS	Ing. Alexandra Cruz	Servidor mail Data Center matriz	1				0
S_ATVR	SERVICIO ANTIVIRUS	Servicio de antivirus institucional	S	TICS	Ing. Vinicio Vallejos	Servidor srveset Data Center matriz	1				0
S_TELF	SERVICIO TELEFONIA	Servicio de telefonía interna	S	TICS	Ing. Cristina Orejuela	Servidor srvteliba Data Center matriz	1				0
S_INTERNET	SERVICIO DE INTERNET	Servicio de internet institucional	S	TICS	Ing. Xavier Brito	Data Center matriz	1	3			3
COM_ENLACES	ENLACES AGENCIAS	Enlaces de comunicaciones a agencias	COM	TICS	Ing. Xavier Brito	Agencias de Emelnorte	12	3			3
COM_ENLANT	ENLACE ANTENA ASUR	Enlace de antena con la Agencia SUR	COM	TICS	Ing. Xavier Brito	Agencia Sur	1	3			3
COM_FIBRA	ENLACE FIBRA EDBORRERO	Enlace de fibra con el edificio Borrero	COM	TICS	Ing. Xavier Brito	Edificio Borrero	1	4			4
AUX_CLIMATIZACIC	EQUIPOS CLIMATIZACION	Equipos de climatización	AUX	TICS	Ing. Catalina Gordillo	Data Center matriz	2	4	3		7
AUX_UPS	RESPALDO DE ENERGIA	Equipos de respaldo de energía del Data Center	AUX	TICS	Ing. Catalina Gordillo	Data Center matriz	2	5	3		8
AUX_INCENDIOS	EXTINCION DE INCENDIOS	Sistema de extinción de incendios del Data Center	AUX	TICS	Ing. Catalina Gordillo	Data Center matriz	1	1			1
AUX_GENERADOR	GENERADOR DE ENERGIA	Equipo auxiliar de generación de energía	AUX	TICS	Ing. Catalina Gordillo	Edificio matriz Subsuelo	1	2			2

4.6.2 Caracterización e identificación de amenazas

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cómo de probable es que pase. Podemos resumirlo en la expresión "conoce a tu enemigo" (MAGERIT – versión 3.0, 2012).

Una vez determinada que una amenaza puede perjudicar a un activo, hay que estimar si afecta a la confidencialidad, integridad y disponibilidad del SGSI. La organización puede contar con mecanismos de protección que reducen la probabilidad de ocurrencia de dichas amenazas.

Para la caracterización de amenazas Magerit establece un catálogo de amenazas clasificadas en 4 grupos:

Tabla 12. *Tipos de amenazas*

[N] Desastres Naturales
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataque intencionados

Fuente: (MAGERIT – versión 3.0, 2012)

4.6.2.1 Identificación de amenazas

E objetivo es identificar las amenazas a las que se exponen los activos dentro del alcance del SGSI y las vulnerabilidades que pueden ser explotadas por las amenazas

4.6.2.2 Valoración de amenazas

Objetivo:

- Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo en base al registro de ocurrencia en los últimos 5 años.
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse

Para valorar las amenazas de cada activo se ha considerado las siguientes escalas de degradación del valor y probabilidad de ocurrencia:

Tabla 13. *Degradación del valor del activo*

CODIGO	DESCRIPCION
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente: (MAGERIT – versión 3.0, 2012)
Modificado por: Investigadora

Tabla 14. *Probabilidad de ocurrencia*

CODIGO	DESCRIPCIÓN
1	Muy raro
2	Poco probable
3	Posible
4	Muy alto
5	Casi seguro

Fuente: (MAGERIT – versión 3.0, 2012)
Modificado por: Investigadora

4.6.2.3 Determinación de vulnerabilidades

Entre las vulnerabilidades más comunes tenemos:

- Seguridad lógica
- Seguridad de recursos humanos
- Seguridad física y ambiental
- Seguridad de gestión de operaciones y comunicaciones
- Mantenimiento, desarrollo y adquisición de sistemas de información

4.6.2.4 Determinación de salvaguardas

Se define como salvaguardas o contra medidas a aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras, seguridad física y, por último, está la política de personal.

Para valorar las salvaguardas y determinar su eficacia o nivel de madurez se puede emplear una escala que recoja en forma de factor la confianza que merece el proceso de gestión de la salvaguarda (MAGERIT – versión 3.0, 2012):

Eficacia	Nivel	Madurez	Estado
0%	L0	inexistente	inexistente
10%	L1	inicial/ad hoc	iniciado
50%	L2	reproducible, pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Figura 13. Niveles de madurez
Fuente: (MAGERIT – versión 3.0, 2012)

4.6.2.5 Determinación del impacto

Se denomina impacto potencial a la medida del daño sobre el activo derivado de la materialización de una amenaza (MAGERIT – versión 3.0, 2012). Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es el impacto directo que estas tendrán sobre el sistema.

El impacto residual se calcula a partir del impacto potencial sobre un activo y las salvaguardas desplegadas para las amenazas sobre dicho activo.

$$\text{Impacto residual} = \text{impacto potencial} \times (1-e^i)$$

Donde

$e^i = 0$ para un sistema de salvaguardas totalmente ineficaz; y

$e^i = 1$ para un sistema de salvaguardas plenamente eficaz

4.6.2.6 Determinación el Riesgo

El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos (MAGERIT – versión 3.0, 2012). Es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (MAGERIT – versión 3.0, 2012):

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo
- zona 3 – riesgos improbables y de bajo impacto
- zona 4 – riesgos improbables pero de muy alto impacto

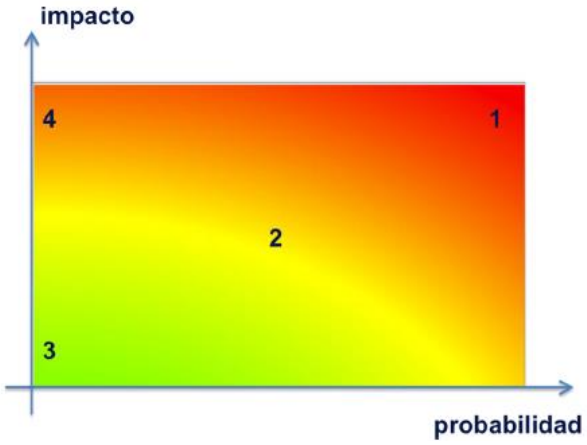


Figura 14. Niveles de madurez
Fuente: (MAGERIT – versión 3.0, 2012)

El riesgo en función del impacto y la probabilidad

El cálculo del riesgo se lo realiza mediante la siguiente fórmula:

Riesgo= Probabilidad*Impacto+Valoración

Los riesgos no se pueden eliminar, solo mitigar, es por ello que se establece un nivel de tolerancia:

Tabla 15. *Niel de tolerancia de riesgos*

TOLERANCIA	RANGO
Totalmente Tolerable TT	0 – 15
Regularmente Tolerable RT	16 – 25
No Tolerable NT	25 - 40

Fuente: (MAGERIT – versión 3.0, 2012)
Modificado por: Investigadora

Aplicando la fórmula a los activos y amenazas ingresadas y valoradas se obtiene la siguiente tabla de riesgos:

Tabla 16. *Definición riesgos*

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
SIEEQ	14	Avería de origen físico o lógico	2	0	24	RT
		Errores de los usuarios	3	4	26	NT
		Errores del administrador	1	3	17	RT
		Errores de mantenimiento/actualización de programas SW	3	0	23	RT

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
		Abuso de privilegios de acceso	2	4	22	RT
		Acceso no autorizado	2	0	24	RT
		Modificación deliberada de la información	3	0	29	NT
		Destrucción de información	1	0	19	RT
		Manipulación de programas	1	5	19	RT
APLICACION CITRIX	14	Avería de origen físico o lógico	3	0	29	NT
		Errores del administrador	2	3	20	RT
		Difusión de software dañino	2	3	20	RT
		Errores de mantenimiento/actualización de programas SW	3	0	23	RT
SISTEMA OPERATIVO CITRIX	14	Avería de origen físico o lógico	3	0	29	NT
		Errores del administrador	3	3	23	RT
		Difusión de software dañino	3	3	23	RT
		Errores de mantenimiento/actualización de programas SW	1	0	17	RT
		Acceso no autorizado	2	0	24	RT
VIRTUALIZACIÓN DE SERVIDORES	13	Avería de origen físico o lógico	3	0	25	RT
		Errores del administrador	1	3	16	RT
		Difusión de software dañino	1	3	16	RT
		Errores de mantenimiento/actualización de programas SW	2	0	19	RT
BASE DE DATOS EERN	14	Avería de origen físico o lógico	4	0	34	NT
		Errores del administrador	2	3	20	RT
		Modificación deliberada de la información	3	0	29	NT
		Destrucción de información	2	0	22	RT
SISTEMA OPERATIVO BDD	14	Avería de origen físico o lógico	3	0	29	NT
		Errores del administrador	2	3	20	RT
		Acceso no autorizado	3	0	29	NT
SISTEMA OPERATIVO DOMINIO	8	Avería de origen físico o lógico	3	0	23	RT
		Errores del administrador	2	3	14	TT
		Difusión de software dañino	3	3	17	RT
		Acceso no autorizado	3	0	23	RT
SISTEMA OPERATIVO DOMINIO SEC	8	Avería de origen físico o lógico	3	0	23	RT
		Errores del administrador	2	3	14	TT
		Difusión de software dañino	3	3	17	RT
		Acceso no autorizado	3	0	23	RT

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
SISTEMA OPERATIVO MAIL	8	Avería de origen físico o lógico	3	0	14	TT
		Errores del administrador	2	3	14	TT
		Acceso no autorizado	3	0	23	RT
SISTEMA OPERATIVO ANTIVIRUS	1	Avería de origen físico o lógico	3	0	4	TT
		Errores del administrador	2	3	7	TT
		Acceso no autorizado	3	0	16	RT
SISTEMA OPERATIVO TELEFONIA	8	Avería de origen físico o lógico	3	0	14	TT
		Errores del administrador	2	3	14	TT
		Acceso no autorizado	3	0	23	RT
SERVIDORES BLADE	4	Fuego	1	0	9	TT
		Daños por agua	1	0	9	TT
		Desastres naturales	1	0	9	TT
		Desastres industriales	2	0	12	TT
		Contaminación mecánica	2	0	12	TT
		Avería de origen físico o lógico	3	0	16	RT
		Corte del suministro eléctrico	4	0	20	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	16	RT
		Errores del administrador	2	3	10	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	8	TT
		Caída del sistema por agotamiento de recursos	2	0	12	TT
CHASIS BLADE	9	Fuego	1	0	14	TT
		Daños por agua	1	0	14	TT
		Desastres naturales	1	0	14	TT
		Desastres industriales	2	0	17	RT
		Contaminación mecánica	2	0	17	RT
		Avería de origen físico o lógico	3	0	21	RT
		Corte del suministro eléctrico	4	0	25	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	21	RT
		Errores del administrador	2	3	15	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	13	TT
		Caída del sistema por agotamiento de recursos	2	0	17	RT
SISTEMA DE ALMACENAMIENTO	14	Fuego	1	0	19	RT
		Daños por agua	1	0	19	RT

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
		Desastres naturales	1	0	19	RT
		Desastres industriales	2	0	22	RT
		Contaminación mecánica	2	0	22	RT
		Avería de origen físico o lógico	3	0	26	NT
		Corte del suministro eléctrico	4	0	30	NT
		Condiciones inadecuadas de temperatura o humedad	3	0	26	NT
		Errores del administrador	2	3	20	RT
		Errores de mantenimiento / actualización de equipos HW	1	0	18	RT
		Caída del sistema por agotamiento de recursos	2	0	22	RT
SERVIDOR DE DOMINIO	4	Fuego	1	0	9	TT
		Daños por agua	1	0	9	TT
		Desastres naturales	1	0	9	TT
		Desastres industriales	2	0	12	TT
		Contaminación mecánica	2	0	12	TT
		Avería de origen físico o lógico	3	0	16	RT
		Corte del suministro eléctrico	4	0	20	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	16	RT
		Errores del administrador	2	3	10	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	8	TT
		Caída del sistema por agotamiento de recursos	2	0	12	TT
SERVIDOR DE DOMINIO SECUNARIO	4	Fuego	1	0	9	TT
		Daños por agua	1	0	9	TT
		Desastres naturales	1	0	9	TT
		Desastres industriales	2	0	12	TT
		Contaminación mecánica	2	0	12	TT
		Avería de origen físico o lógico	3	0	16	RT
		Corte del suministro eléctrico	4	0	20	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	16	RT
		Errores del administrador	2	3	10	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	8	TT
		Caída del sistema por agotamiento de recursos	2	0	12	TT

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
SERVIDOR DE CORREO INSTITUCIONAL	4	Fuego	1	0	9	TT
		Daños por agua	1	0	9	TT
		Desastres naturales	1	0	9	TT
		Desastres industriales	2	0	12	TT
		Contaminación mecánica	2	0	12	TT
		Avería de origen físico o lógico	3	0	16	RT
		Corte del suministro eléctrico	4	0	20	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	16	RT
		Errores del administrador	2	3	10	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	8	TT
		Caída del sistema por agotamiento de recursos	2	0	12	TT
SERVIDOR TELEFONIA	8	Fuego	1	0	13	TT
		Daños por agua	1	0	13	TT
		Desastres naturales	1	0	13	TT
		Desastres industriales	2	0	16	RT
		Contaminación mecánica	2	0	16	RT
		Avería de origen físico o lógico	3	0	20	RT
		Corte del suministro eléctrico	4	0	24	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	20	RT
		Errores del administrador	2	3	14	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	12	TT
		Caída del sistema por agotamiento de recursos	2	0	16	RT
FIREWALL	13	Fuego	1	0	18	RT
		Daños por agua	1	0	18	RT
		Desastres naturales	1	0	18	RT
		Desastres industriales	2	0	21	RT
		Contaminación mecánica	2	0	21	RT
		Avería de origen físico o lógico	3	0	25	RT
		Corte del suministro eléctrico	4	0	29	NT
		Condiciones inadecuadas de temperatura o humedad	3	0	25	RT
		Errores del administrador	2	3	19	RT
		Errores de mantenimiento / actualización de equipos HW	1	0	17	RT
		Caída del sistema por agotamiento de recursos	2	0	21	RT

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
SWITCH ACCESO	4	Fuego	1	0	9	TT
		Daños por agua	1	0	9	TT
		Desastres naturales	1	0	9	TT
		Desastres industriales	2	0	12	TT
		Contaminación mecánica	2	0	12	TT
		Avería de origen físico o lógico	3	0	16	RT
		Corte del suministro eléctrico	4	0	20	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	16	RT
		Errores del administrador	2	3	10	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	8	TT
		Caída del sistema por agotamiento de recursos	2	0	12	TT
SWITCH CORE	14	Fuego	1	0	19	RT
		Daños por agua	1	0	19	RT
		Desastres naturales	1	0	19	RT
		Desastres industriales	2	0	22	RT
		Contaminación mecánica	2	0	22	RT
		Avería de origen físico o lógico	3	0	26	NT
		Corte del suministro eléctrico	4	0	30	NT
		Condiciones inadecuadas de temperatura o humedad	3	0	26	NT
		Errores del administrador	2	3	20	RT
		Errores de mantenimiento / actualización de equipos HW	1	0	18	RT
		Caída del sistema por agotamiento de recursos	2	0	22	RT
ADMINISTRADOR ANCHO DE BANDA	1	Fuego	1	0	6	TT
		Daños por agua	1	0	6	TT
		Desastres naturales	1	0	6	TT
		Desastres industriales	2	0	9	TT
		Contaminación mecánica	2	0	9	TT
		Avería de origen físico o lógico	3	0	13	TT
		Corte del suministro eléctrico	4	0	17	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	13	TT
		Errores del administrador	2	3	7	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	5	TT
		Caída del sistema por agotamiento de recursos	2	0	9	TT
ROUTER	3	Fuego	1	0	8	TT

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
		Daños por agua	1	0	8	TT
		Desastres naturales	1	0	8	TT
		Desastres industriales	2	0	11	TT
		Contaminación mecánica	2	0	11	TT
		Avería de origen físico o lógico	3	0	15	TT
		Corte del suministro eléctrico	4	0	19	RT
		Condiciones inadecuadas de temperatura o humedad	3	0	15	TT
		Errores del administrador	2	3	9	TT
		Errores de mantenimiento / actualización de equipos HW	1	0	7	TT
		Caída del sistema por agotamiento de recursos	2	0	11	TT
SERVICIO DE INTERNET	3	Fallo de servicios de comunicaciones	2	2	7	TT
		Errores del administrador	2	0	7	TT
		Repudio	2	0	13	TT
		Suplantación de la identidad del usuario	4	3	15	TT
		Uso no previsto	2	0	9	TT
ENLACES AGENCIAS	3	Fallo de servicios de comunicaciones	3	0	12	TT
		Errores del administrador	2	2	7	TT
		Suplantación de la identidad del usuario	2	0	13	TT
		Acceso no autorizado	2	0	9	TT
		Análisis de tráfico	2	0	13	TT
		Interceptación de información (escucha)	2	0	13	TT
ENLACE ANTENA ASUR	3	Fallo de servicios de comunicaciones	3	0	12	TT
		Errores del administrador	2	2	7	TT
		Suplantación de la identidad del usuario	2	0	13	TT
		Acceso no autorizado	2	0	9	TT
		Análisis de tráfico	2	0	13	TT
		Interceptación de información (escucha)	2	0	13	TT
ENLACE FIBRA EDBORRERO	4	Fallo de servicios de comunicaciones	3	0	13	TT
		Errores del administrador	2	2	8	TT
		Suplantación de la identidad del usuario	2	0	14	TT
		Acceso no autorizado	2	0	10	TT
		Análisis de tráfico	2	0	14	TT
		Interceptación de información (escucha)	2	0	14	TT
EQUIPOS CLIMATIZACION	7	Fuego	1	0	12	TT
		Daños por agua	2	0	17	RT

NOMBRE	VALOR	DESCRIPCION	PROB.	IMPACTO	RIESGO	TOLERANCIA
		Desastres naturales	1	0	12	TT
		Desastres industriales	1	0	11	TT
		Contaminación mecánica	2	0	15	TT
		Avería de origen físico o lógico	3	0	19	RT
		Corte del suministro eléctrico	4	0	27	NT
		Condiciones inadecuadas de temperatura o humedad	2	0	15	TT
		Errores del administrador	2	3	13	TT
RESPALDO DE ENERGIA	8	Fuego	1	0	13	TT
		Daños por agua	2	0	18	RT
		Desastres naturales	1	0	13	TT
		Desastres industriales	1	0	12	TT
		Contaminación mecánica	2	0	16	RT
		Avería de origen físico o lógico	3	0	20	RT
		Corte del suministro eléctrico	4	0	28	NT
		Condiciones inadecuadas de temperatura o humedad	2	0	16	RT
		Errores del administrador	2	3	14	TT
EXTINCION DE INCENDIOS	1	Fuego	1	0	6	TT
		Daños por agua	2	0	11	TT
		Desastres naturales	1	0	6	TT
		Desastres industriales	1	0	5	TT
		Contaminación mecánica	2	0	9	TT
		Avería de origen físico o lógico	3	0	13	TT
		Corte del suministro eléctrico	4	0	21	RT
		Condiciones inadecuadas de temperatura o humedad	2	0	9	TT
		Errores del administrador	2	3	7	TT
GENERADOR DE ENERGIA	2	Fuego	1	0	7	TT
		Daños por agua	2	0	12	TT
		Desastres naturales	1	0	7	TT
		Desastres industriales	1	0	6	TT
		Contaminación mecánica	2	0	10	TT
		Avería de origen físico o lógico	3	0	14	TT
		Corte del suministro eléctrico	4	0	22	RT
		Condiciones inadecuadas de temperatura o humedad	2	0	10	TT
		Errores del administrador	2	3	8	TT

Fuente: Investigadora

4.6.3 Riesgos No Tolerables identificados

Del análisis de riegos realizado se obtiene un listado de los riesgos clasificados como NO TOLERABLES, para los cuales se debe realizar la selección de controles establecidos en la norma ISO27002.

Tabla 17. *Resumen de riesgos NO TOLERABLES*

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
APLICACION CITRIX	Avería de origen físico o lógico	3	5	29
SISTEMA OPERATIVO CITRIX	Avería de origen físico o lógico	3	5	29
VIRTUALIZACIÓN DE SERVIDORES	Avería de origen físico o lógico	3	4	25
BASE DE DATOS EERN	Avería de origen físico o lógico	4	5	34
SISTEMA OPERATIVO BDD	Avería de origen físico o lógico	3	5	29
SISTEMA DE ALMACENAMIENTO	Avería de origen físico o lógico	3	4	26
FIREWALL	Avería de origen físico o lógico	3	4	25
SWITCH CORE	Avería de origen físico o lógico	3	4	26
CHASIS BLADE	Corte del suministro eléctrico	4	4	25
SISTEMA DE ALMACENAMIENTO	Corte del suministro eléctrico	4	4	30
FIREWALL	Corte del suministro eléctrico	4	4	29
SWITCH CORE	Corte del suministro eléctrico	4	4	30
EQUIPOS CLIMATIZACION	Corte del suministro eléctrico	4	5	27
RESPALDO DE ENERGIA	Corte del suministro eléctrico	4	5	28
SISTEMA DE ALMACENAMIENTO	Condiciones inadecuadas de temperatura o humedad	3	4	26
FIREWALL	Condiciones inadecuadas de temperatura o humedad	3	4	25
SWITCH CORE	Condiciones inadecuadas de temperatura o humedad	3	4	26
SIEEQ	Errores de los usuarios	3	4	26
SISTEMA OPERATIVO BDD	Acceso no autorizado	3	5	29

SIEEQ	Modificación deliberada de la información	3	5	29
BASE DE DATOS EERN	Modificación deliberada de la información	3	5	29

Fuente: Investigadora

4.7 Selección de controles

Para cada riesgo considerado NO TOLERABLE se selecciona una lista de controles a seguir, controles seleccionados de la norma ISO 27001.

Tabla 18. *Definición de control*

Riesgo	General
Activo	Todos
Procesos afectados	Atención de nuevos clientes
Acciones - Control	
Dominio	5. Política de seguridad
Objetivo	5.1 Política de la seguridad de la información La dirección proporcionará indicaciones y dará apoyo a la seguridad de la información de acuerdo con los requisitos del negocio y con la legislación y las normativas aplicables.
Control	5.1.1 Documento de la política de la seguridad de la información. La dirección debería aprobar un documento de política de la seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.
Indicadores	Elaborar la política de seguridad de la información, aprobarla por la alta dirección y difundirla a toda la organización. Fórmula: Política elaborada, aprobada y difundida Cumplimiento: 50%
Dominio	13. Gestión de los incidentes de la seguridad de la información
Objetivo	13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información Asegurarse de que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información se comunican de manera que sea posible emprender las acciones correctivas oportunas.
Control	13.1.1 Reporte sobre los eventos de la seguridad de la información Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.
Indicadores	Elaborar el procedimiento para tratamiento de eventos de seguridad de la información. Fórmula: Procedimiento elaborado y aprobado por la Dirección Cumplimiento: 0%
	Elaborar formato para reporte de eventos de seguridad de la información. Fórmula: Formato elaborado Cumplimiento: 0%

Elaborado por: Investigadora

Tabla 19. *Definición de control para Errores de usuario*

Riesgo	Errores de los usuarios
Activo	SIEEQ
Procesos afectados	Atención de nuevos clientes
Acciones - Control	
Dominio	10. Gestión de comunicaciones y operaciones
Objetivo	10.1 Procedimientos operacionales y responsabilidades Asegurar la operación correcta y segura de los servicios de procesamiento de información.
Control	10.1.1 Documentación de los procesos de operación Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesitan.
Indicadores	Elaborar los procesos de operación detallando las acciones a ejecutar para cada trabajo. Fórmula: Número procedimientos elaborados/Número de procedimientos a levantar Cumplimiento: 80%
	Copias de respaldo Fórmula: Respaldos programados/Sistemas a respaldar Cumplimiento: 90
	Procedimientos de inicio y recuperación de sistemas Fórmula: Procedimientos levantados/Número de sistemas Cumplimiento: 50%
	Registros de auditoría Fórmula: Sistemas auditados/Sistemas a auditar Cumplimiento: 50%

Elaborado por: Investigadora

Tabla 20. *Definición de control para Modificación deliberada de información*

Riesgo	Modificación deliberada de información
Activo	SIEEQ
Procesos afectados	Atención de nuevos clientes
Acciones - Control	
Dominio	10. Gestión de comunicaciones y operaciones
Objetivo	10.1 Procedimientos operacionales y responsabilidades Asegurar la operación correcta y segura de los servicios de procesamiento de información.
Control	10.1.1 Documentación de los procesos de operación Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesitan.
Indicadores	Elaborar los procesos de operación detallando las acciones a ejecutar para cada trabajo. Fórmula: Número procedimientos elaborados/Número de

	procedimientos a levantar Cumplimiento: 80%
	Copias de respaldo Fórmula: Respaldos programados/Sistemas a respaldar Cumplimiento: 90
	Procedimientos de inicio y recuperación de sistemas Fórmula: Procedimientos levantados/Número de sistemas Cumplimiento: 50%
	Registros de auditoría Fórmula: Sistemas auditados/Sistemas a auditar Cumplimiento: 50%
Control	10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.
Indicadores	Levantar ambientes de desarrollo y prueba de los sistemas Fórmula: Sistemas de prueba levantados/Sistemas en producción Cumplimiento: 70%
Objetivo	10.5 Respaldo Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.
Control	10.5.1 Respaldo de la información Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
Indicadores	Se debe realizar copias de respaldo de la información más sensible. Fórmula: Copias de respaldo realizadas/Copias de respaldo planificadas Cumplimiento: 90%
Dominio	11. Control de acceso
Objetivo	11.1 Requisitos del negocio para el control de acceso Controlar el acceso a la información
Control	11.1.1 Política de control de acceso Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.
Indicadores	Levantar una política de control de accesos a los sistemas Fórmula: Política levantada Cumplimiento: 0%
Objetivo	11.2 Gestión del acceso a usuarios Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.
Control	11.2.1 Registro de usuarios Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el

	acceso a todos los sistemas y servicios de información.
Indicadores	Levantar un procedimiento para la creación y eliminación de usuarios y asignación de funciones. Fórmula: Procedimiento levantado Cumplimiento: 0%
Objetivo	11.3 Responsabilidades de los usuarios Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de información o de recursos de tratamiento de información.
Control	11.3.1 Uso de contraseñas Se debería exigir a los usuarios el cumplimiento de buenas prácticas de la seguridad en la selección y el uso de las contraseñas.
Indicadores	Promulgar y verificar el cumplimiento de buenas prácticas en el uso de contraseñas Fórmula: Usuarios informados/total de usuarios Cumplimiento: 50%

Elaborado por: Investigadora

Tabla 21. *Definición de control para Avería de origen físico o lógico*

Riesgo	Avería de origen físico o lógico
Activo	Aplicación Citrix, Sistemas operativos, Sistema de almacenamiento, Firewall
Procesos afectados	Atención de nuevos clientes
Acciones - Control	
Dominio	9. Seguridad física y del entorno
Objetivo	9.2 Seguridad de los equipos Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.
Control	9.2.4 Mantenimiento de los equipos Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
Indicadores	Realizar mantenimiento periódico de equipos Fórmula: Mantenimientos realizados/Mantenimientos programados. Cumplimiento: 70%
Control	9.2.2 Servicios de suministro Los equipos deberían estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.
Indicadores	Los equipos deben protegerse contra fallas del suministro eléctrico. Fórmula: Equipos protegidos/Total de equipos Cumplimiento: 100%
Control	9.2.3 Seguridad de cableado El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debería estar protegido contra interceptaciones o daños.
Indicadores	Cableado eléctrico y de telecomunicaciones protegido Fórmula: Cableado protegido Cumplimiento: 90%
Dominio	7 Gestión de activos Gestión de activos
Objetivo	7.1 Responsabilidad por los activos Conseguir y mantener una protección adecuada de los activos de la organización
Control	7.1.1 Inventario de activos Todos los activos deberían estar claramente identificados y se debería elaborar y mantener un inventario de todos los activos importantes.
Indicadores	Elaborar el inventario detallado de los equipos Fórmula: Equipos inventariados/Total de equipos Cumplimiento: 70%

Elaborado por: Investigadora

Tabla 22. *Definición de control para Acceso no autorizado*

Riesgo	Acceso no autorizado
Activo	Sistemas operativos
Procesos afectados	Atención de nuevos clientes
Acciones - Control	
Dominio	9 Seguridad física y del entorno
Objetivo	9.1 Áreas seguras Evitar el acceso físico no autorizado, el daño o la interferencia las instalaciones y a la información de la organización.
Control	9.1.1 Perímetro de la seguridad física Se deberían utilizar perímetros de la seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.
Indicadores	El Centro de Datos debe ubicarse en un ambiente construido con el fin de almacenar equipos informáticos. Fórmula: Ambiente de Centro de Datos construido adecuadamente. Cumplimiento: 100%
Control	9.1.2 Controles de acceso físico Las áreas seguras deberían estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
Indicadores	Elaborar bitácora de acceso de personal externo al Centro de Datos. Fórmula: Bitácora elaborada Cumplimiento: 100%
	Instalar controles de acceso a áreas seguras. Fórmula: Número de controles de acceso/Número de áreas seguras Cumplimiento: 100%

Elaborado por: Investigadora

Tabla 23. *Definición de control para Avería de origen físico o lógico*

Riesgo	Avería de origen físico o lógico
Activo	Bases de datos
Procesos afectados	Atención de nuevos clientes
Acciones - Control	
Dominio	14 Gestión de la continuidad del negocio
Objetivo	14.1 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio. Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.
Control	14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información Se deberían desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.
Indicadores	Desarrollar procedimientos para recuperación, restauración y continuidad de los servicios. Fórmula: Número de procedimientos/Número de servicios Cumplimiento: 40%

Elaborado por: Investigadora

4.7.1 Evaluación del SGSI

4.7.1.1 Resumen de cumplimiento de controles seleccionados

A continuación se presenta el resumen de cumplimiento de los controles seleccionados para el desarrollo del presente trabajo:

Tabla 24. *Evaluación de controles seleccionados del SGSI*

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
5 Política de seguridad	5.1 Política de la seguridad de la información	Documento de la política de la seguridad de la información	50%
7 Gestión de activos	7.1 Responsabilidad por los activos	Inventario de activos	70%
9 Seguridad física y del entorno	9.1 Áreas seguras	Perímetro de la seguridad física	100%

		Controles de acceso físico	100%
	9.2 Seguridad de los equipos	Servicios de suministro	100%
		Seguridad de cableado	90%
		Mantenimiento de los equipos	70%
10 Gestión de comunicaciones y operaciones	10.1 Procedimientos operacionales y responsabilidades	Documentación de los procesos de operación	67.5%
		Separación de las instalaciones de desarrollo, ensayo y operación	70%
	10.5 Respaldo	Respaldo de la información	90%
11 Control de acceso	11.1 Requisitos del negocio para el control de acceso	Política de control de acceso	0%
	11.2 Gestión del acceso a usuarios	Registro de usuarios	0%
	11.3 Responsabilidades de los usuarios	Uso de contraseñas	50%
13 Gestión de los incidentes de la seguridad de la información	13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información	Reporte sobre los eventos de la seguridad de la información	0%
14 Gestión de la continuidad del negocio	14.1 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	40%

Fuente: Investigadora

4.7.1.2 Evaluación general de la norma ISO 27001

El siguiente cuadro es únicamente informativo, muestra una evaluación general del SGSI, tomando en cuenta los controles seleccionados y no seleccionados para el presente trabajo.

Tabla 25. *Evaluación general de la norma ISO 27001*

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
5 Política de seguridad	51 Política de la seguridad de la información	Documento de la política de la seguridad de la información	50%
		Revisión de la política de la seguridad de la información	0%
6 Organización de la seguridad de la información	61 Organización interna	Compromiso de la dirección con la seguridad de la información	0%
		Coordinación de la seguridad de la información	0%
		Asignación de responsabilidades para la seguridad de la información	0%
		Procesos de autorización para los servicios de procesamiento de la información	0%
		Acuerdos sobre confidencialidad	0%
		Contacto con las autoridades	0%
		Contacto con grupo de interés especiales	0%
		Revisión independiente de la seguridad de la información	0%
	62 Partes externas	Identificación de los riesgos relacionados con las partes externas	0%
		Consideraciones de la seguridad cuando se trata con los clientes	0%
		Consideraciones de la seguridad en los	0%

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
		acuerdos con terceras partes	
7 Gestión de activos	71 Responsabilidad por los activos	Inventario de activos	70%
		Responsable de los activos	0%
		Uso aceptable de los activos	0%
	72 Clasificación de la información	Directrices de clasificación	0%
		Etiquetado y manejo de la información	0%
8 Seguridad de los recursos humanos	81 Previo a la contratación laboral	Funciones y responsabilidades	0%
		Selección	0%
		Términos y condiciones laborales	0%
	82 Durante la vigencia del contrato laboral	Responsabilidades de la dirección	0%
		Educación, formación y concienciación sobre la seguridad de la información	0%
		Proceso disciplinario	0%
	83 Terminación o cambio de la contratación laboral	Responsabilidades en la terminación del contrato	0%
		Devolución de activos	0%
		Retiro de los derechos de acceso	0%
9 Seguridad física y del entorno	91 Áreas seguras	Perímetro de la seguridad física	100%
		Controles de acceso físico	100%
		Seguridad de oficinas, recintos e instalaciones	0%
		Protección contra amenazas externas y ambientales	0%
		Trabajo en áreas seguras	0%
		Áreas de carga, despacho y acceso público	0%
	92 Seguridad de los equipos	Ubicación y protección de los equipos	0%
		Servicios de suministro	100%
		Seguridad de cableado	90%
		Mantenimiento de los	70%

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
		equipos	
		Seguridad de los equipos fuera de las instalaciones	0%
		Seguridad en la reutilización o eliminación de equipos	0%
		Retiro de activos de la propiedad	0%
10 Gestión de comunicaciones y operaciones	101 Procedimientos operacionales y responsabilidades	Documentación de los procesos de operación	67.5%
		Gestión del cambio	0%
		Distribución de funciones	0%
		Separación de las instalaciones de desarrollo, ensayo y operación	70%
	102 Gestión de la presentación del servicio por terceras partes	Prestación del servicio	0%
		Monitoreo y revisión de los servicios por terceros	0%
		Gestión de los cambios en los servicios por terceras partes	0%
	103 Planificación y aceptación del sistema	Gestión de la capacidad	0%
		Aceptación del sistema	0%
	104 Protección contra códigos maliciosos y móviles	Controles contra códigos maliciosos	0%
		Controles contra códigos móviles	0%
	105 Respaldo	Respaldo de la información	90%
	106 Gestión de la seguridad de las redes	Controles de las redes	0%
		Seguridad de los servicios de la red	0%
	107 Manejo de los medios	Gestión de los medios removibles	0%
		Eliminación de los medios	0%
		Procedimientos para el manejo de la información	0%
		Seguridad de la documentación del sistema	0%

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
	108 Intercambio de la información	Políticas y procedimientos para el intercambio de la información	0%
		Acuerdos para el intercambio	0%
		Medios físicos en tránsito	0%
		Mensajería electrónica	0%
		Sistemas de información del negocio	0%
	109 Servicios de comercio electrónico	Comercio electrónico	0%
		Transacciones en línea	0%
		Información disponible al público	0%
	1010 Monitoreo	Registro de auditorías	0%
		Monitoreo de uso del sistema	0%
		Protección del registro de la información	0%
		Registros del administrador y del operador	0%
		Registro de fallas	0%
		Sincronización de relojes	0%
11 Control de acceso	111 Requisitos del negocio para el control de acceso	Política de control de acceso	0%
	112 Gestión del acceso a usuarios	Registro de usuarios	0%
		Gestión de privilegios	0%
		Gestión de contraseñas para usuarios	0%
		Revisión de los derechos de acceso de los usuarios	0%
	113 Responsabilidades de los usuarios	Uso de contraseñas	50%
		Equipo de usuario desatendido	0%
		Política de escritorio despejado y de pantalla despejada	0%
	114 Control de acceso a las redes	Política de uso de los servicios de red	0%
		Autenticación de usuarios para conexiones externas	0%

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
		Identificación de los equipos en las redes	0%
		Protección de los puertos de configuración y diagnóstico remoto	0%
		Separación en las redes	0%
		Control de conexión a las redes	0%
		Control de enrutamiento en la red	0%
	115 Control de acceso al sistema operativo	Procedimientos de registro de inicio seguro	0%
		Identificación y autenticación de usuarios	0%
		Sistema de gestión de contraseñas	0%
		Uso de las utilidades del sistema	0%
		Tiempo de inactividad de la sesión	0%
		Limitación del tiempo de conexión	0%
	116 Control de acceso a las aplicaciones y a la información	Restricción del acceso a la información	0%
		Aislamiento de sistemas sensibles	0%
	117 Computación móvil y trabajo remoto	Computación y comunicaciones móviles	0%
		Trabajo remoto	0%
12 Adquisición, desarrollo y mantenimiento de sistemas de información	121 Requisitos de la seguridad de los sistemas de información	Análisis y especificación de los requisitos de la seguridad	0%
	122 Procesamiento correcto en las aplicaciones	Validación de los datos de entrada	0%
		Control de procesamiento interno	0%
		Integridad del mensaje	0%
		Validación de los datos de salida	0%
	123 Controles criptográficos	Políticas sobre el uso de controles criptográficos	0%
		Gestión de claves	0%
	124 Seguridad de los archivos del	Control del software operativo	0%

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
	sistema	Protección de los datos de prueba del sistema	0%
		Control de acceso al código fuente de los programas	0%
	125 Seguridad en los procesos de desarrollo y soporte	Procedimientos de control de cambios	0%
		Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	0%
		Restricciones en los cambios a los paquetes de software	0%
		Fuga de información	0%
		Desarrollo de software contratado externamente	0%
		Control de las vulnerabilidades técnicas	0%
13 Gestión de los incidentes de la seguridad de la información	131 Reporte sobre los eventos y las debilidades de la seguridad de la información	Reporte sobre los eventos de la seguridad de la información	0%
		Reporte sobre las debilidades en la seguridad	0%
	132 Gestión de los incidentes y las mejoras en la seguridad de la información	Responsabilidades y procedimientos	0%
		Aprendizaje debido a los incidentes de seguridad de la información	0%
		Recolección de evidencias	0%
14 Gestión de la continuidad del negocio	141 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio	Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio	0%
		Continuidad del negocio y evaluación de riesgos	0%
		Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	40%

DOMINIO	OBJETIVO	CONTROL	CUMPLIMIENTO
		Estructura para la planificación de la continuidad del negocio	0%
		pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	0%
15 Cumplimiento	151 Cumplimiento de los requisitos legales	Identificación de la legislación aplicable	0%
		Derechos de propiedad intelectual (DPI)	0%
		Protección de los registros de la organización	0%
		Protección de los datos y privacidad de la información personal	0%
		Prevención del uso inadecuado de los servicios de procesamiento de información	0%
		Reglamentación de los controles criptográficos	0%
	152 Cumplimiento de las políticas y las normas de la seguridad y cumplimiento técnico	Cumplimiento de las políticas y las normas de la seguridad	0%
		Verificación del cumplimiento técnico	0%
	153 Consideraciones de la auditoría de los sistemas de información	Controles de auditoría de los sistemas de información	0%
		Protección de las herramientas de auditoría de los sistemas de información	0%

Fuente: Investigadora

4.8 Plan de tratamiento de riesgos

A continuación se presenta el Plan de Tratamiento de los Riesgos (PTR) mediante los controles seleccionados. Con este PRT se pretende disminuir el impacto de los riesgos sobre los activos afectados.

Tabla 26. *Historia de usuario – Integración con la arquitectura de software*

Nro.	MECANISMO DE PROTECCIÓN		ACTIVIDADES	PLAZO	RESPONSABLE
1	Elaborar la política de seguridad de la información, aprobarla por la alta dirección y difundirla a toda la organización	1.1	Revisar la política de seguridad	1s	Dirección TIC
		1.2	Aprobar la política de seguridad	1s	Dirección TIC
		1.3	Difundir la política de seguridad	1d	Dirección TIC
2	Elaborar el inventario detallado de los equipos	2.1	Elaborar plantilla de inventario	3m	Dirección TIC
		2.2	Levantamiento de información de inventario		Dirección TIC
3	Realizar mantenimiento periódico de equipos	3.1	Seleccionar equipos para el mantenimiento preventivo	2d	Dirección TIC
		3.2	Elaborar el plan de mantenimiento preventivo	3d	Dirección TIC
		3.3	Elaborar procedimiento para el mantenimiento de cada equipo	10d	Dirección TIC
4	Elaborar los procesos de operación para ejecución de trabajos manuales, detallando las acciones a ejecutar.	4.1	Determinación de trabajos manuales ejecutados sobre el SIEEQ	3d	Dirección TIC
		4.2	Elaboración de plantilla del proceso	1d	Dirección TIC
		4.3	Elaboración de procesos detallados	1m	Dirección TIC
5	Copias de respaldo	5.1	Determinar que copias de respaldo son necesarias	3d	Dirección TIC
		5.2	Elaborar política de respaldos de información	5d	Dirección TIC
		5.3	Aprobar política	5d	Dirección TIC
		5.4	Elaborar procedimiento de respaldos	15d	Dirección TIC
		5.5	Elaborar procedimiento de pruebas de respaldos	10d	Dirección TIC
6	Procedimientos de inicio y	6.1	Elaborar procedimiento de reinicio del SIEEQ	5d	Dirección TIC

Nro.	MECANISMO DE PROTECCIÓN		ACTIVIDADES	PLAZO	RESPONSABLE
	recuperación de sistemas	6.2	Elaborar procedimiento de reinicio de las bases de datos	5d	Dirección TIC
7	Registros de auditoría	7.1	Activar auditoría de la base de datos SIEEQ	5d	Dirección TIC
8	Levantar una política de control de accesos a los sistemas	8.1	Elaborar política	10d	Dirección TIC
		8.2	Revisar y aprobar política	10d	Dirección TIC
		8.3	Elaborar procedimiento de aplicación	5d	Dirección TIC
9	Levantar un procedimiento para el creación y eliminación de usuarios y asignación de funciones	9.1	Elaborar procedimiento	5d	Dirección TIC
		9.2	Revisar y aprobar procedimiento	5d	Dirección TIC
10	Promulgar y verificar el cumplimiento de buenas prácticas en el uso de contraseñas	10.1	Elaborar manual de buenas prácticas de seguridad	5d	Dirección TIC
		10.2	Revisar y aprobar manual	5d	Dirección TIC
		10.3	Difundir manual de buenas prácticas	1d	Dirección TIC
11	Elaborar formato para reporte de eventos de seguridad de la información	11.1	Elaborar formato	2d	Dirección TIC
		11.2	Revisar y aprobar formato	2d	Dirección TIC
12	Elaborar el procedimiento para tratamiento de eventos de seguridad de la información	12.1	Elaborar procedimiento	10d	Dirección TIC
		12.2	Revisar y aprobar procedimiento	5d	Dirección TIC
13	Desarrollar procedimientos para recuperación, restauración y continuidad de los servicios.	13.1	Elaborar procedimiento de restauración del SIEEQ en caso de daño	15d	Dirección TIC
		13.2	Revisar y aprobar procedimiento	5d	Dirección TIC
		13.3	Elaborar procedimiento de prueba del procedimiento	5d	Dirección TIC

Fuente:

4.9 Desarrollo del aplicativo para control y manejo del SGSI

Para el desarrollo del aplicativo de control y manejo del SGSI se realiza el levantamiento de los requerimientos especificados por el Director de TIC y los responsables del área de desarrollo de la Institución.

Esos requerimientos están especificados en las historias de usuarios definidas por la metodología ágil Extreme Programming.

4.9.1 Fase 1. Planificación

En esta fase se elabora las historias de usuario en base al análisis de los requerimientos del sistema, los mismos que se dan a conocer al equipo de trabajo, se plasma las tareas y funcionalidades del sistema, el mismo que deberán considerar las características de usabilidad que los usuarios quieren alcanzar, sobre los cuales se orientan al proceso de desarrollo de una aplicación informática.

4.9.1.1 Análisis de usuarios.

De acuerdo con los requerimientos especificados por el área de TICs se define los siguientes usuarios del sistema:

Tabla 27. *Historia de usuario – Integración con la arquitectura de software*

Datos Informativos	**Descripción**
Nombre de la Institución	Empresa Eléctrica Regional Norte
Usuario	Analista TI
Rol	Analista
Actividades	Ingresar y actualizar información

Datos Informativos	**Descripción**
Nombre de la Institución	Empresa Eléctrica Regional Norte
Usuario	Director TI
Rol	Visualizador
Actividades	Generar y visualizar reportes para la toma de decisiones

Fuente: investigadora

4.9.1.2 Historias de Usuario

Mediante la entrevista realizada al Director de TIC y al personal del área de desarrollo se obtienen las siguientes especificaciones de tareas, las mismas que se convierten en historias de usuario, descritas a continuación.

Tabla 28. *Historia de usuario – Integración con la arquitectura de software*

		Historia de Usuario
Número: T01	**Usuarios**: Analista	**Tipo de actividad:** Nueva
Nombre historia:	Integración con la arquitectura existente en Emelnorte	
Prioridad en negocio: Alta		**Rango en desarrollo**: Alta / Media / Baja
Iteración asignada:	1	
Descripción		
El aplicativo a desarrollarse debe estar totalmente integrado a la arquitectura de software implementada en Emelnorte.		
Observaciones:		

Fuente: investigadora

Tabla 29. *Historia de usuario - Ingreso de activos*

		Historia de Usuario
Número: T02	**Usuarios**: Analista	**Tipo de actividad:** Nueva
Nombre historia:	Ingreso de activos	
Prioridad en negocio: Alta		**Rango en desarrollo**: Alta / Media / Baja
Iteración asignada:	2	
Descripción		
El aplicativo debe permitir llevar un registro y control de los activos de información identificados. Se deberá almacenar prioritariamente la siguiente información: - Nombre del activo - Descripción - Tipo de activo - Persona responsable - Ubicación - Valoración del activo en las dimensiones de Disponibilidad, Integridad y Confidencialidad.		

Se debe establecer la relación de los activos identificados por cada proceso de negocio de la institución.
Observaciones: La relación entre el activo y el proceso de negocio se lo hará mediante una tabla de relación, puesto que el activo debe ser definido una sola vez.

Fuente: investigadora

Tabla 30. *Historia de usuario - Ingreso de amenazas*

		Historia de Usuario
Número: T03	**Usuarios**: Analista	**Tipo de actividad:** Nueva
Nombre historia:	Ingreso de amenazas	
Prioridad en negocio: Alta		**Rango en desarrollo**: Alta / Media / Baja
Iteración asignada:	2	
Descripción		
El aplicativo debe permitir almacenar un catálogo de posibles amenaza, así como vincular dichas amenazas con los activos, asignándoles un valor para: - Probabilidad de ocurrencia - Degradación de la amenaza sobre el activo en las dimensiones de Disponibilidad, Integridad y Confidencialidad Las amenazas vinculadas con los activos deberán ser valoradas de acuerdo a la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.		
Observaciones: Se almacenará un catálogo general de amenazas que podrán relacionarse con los activos ingresados. La valoración de la amenaza en cada dimensión del activo será ingresado por el analista del sistema.		

Fuente: investigadora

Tabla 31. *Historia de usuario – Ingreso de controles*

		Historia de Usuario
Número: T04	**Usuarios**: Analista	**Tipo de actividad:** Nueva
Nombre historia:	Ingreso de controles	
Prioridad en negocio: Alta		**Rango en desarrollo**: Alta / Media / Baja
Iteración asignada:	3	
Descripción		
Para los riesgos determinados, el aplicativo deberá permitir la selección de controles para su mitigación. En el registro del control seleccionado se registrará: - La fórmula de cálculo del indicador - La fecha de revisión - El porcentaje de cumplimiento		
Observaciones: Para la selección de controles se basará en un catálogo de controles establecido por la norma ISO 27002		

Fuente: investigadora

Tabla 32. *Historia de usuario – Cuadro de mando y reportes*

		Historia de Usuario
Número: T05	**Usuarios**: Analista / Visualizador	**Tipo de actividad:** Nueva
Nombre historia:	Cuadro de mando y reportes	
Prioridad en negocio: Alta		**Rango en desarrollo**: Alta / Media / Baja
Iteración asignada:	4	
Descripción		
El aplicativo debe permitir visualizar un resumen claro y práctico del estado del SGSI. Debe incluir un módulo de reportes para: - Visualizar el catálogo de activos - Visualizar activos por proceso - Visualizar el catálogo de amenazas - Visualizar reporte de riesgos - Visualizar controles ingresados		
Observaciones:		

Fuente: investigadora

Una vez que se obtuvo las historias de usuarios, se realizó un resumen acerca del orden de la implementación del software.

Tabla 33. *Resumen de las iteraciones del software*

Nro.	Iteración	Semanas	Descripción de Historia de Usuario
1	1	1	Integración con la arquitectura de software existente
2	2	2	Módulo de Activos
3	2	2	Módulo de Amenazas
4	3	2	Módulo de Riesgos y Controles
5	4	2	Módulo de Reportes

Fuente: investigadora

4.9.1.3 Especificación de requisitos funcionales

La funcionalidad del sistema se compone de cuatro módulos descritos a continuación en los requisitos funcionales y no funcionales de la aplicación.

Tabla 34. *Requisito Funcional 1*

RQF001	Ingreso de procesos
Descripción	El usuario deberá poder ingresar los diferentes procesos de negocio de la institución previo al ingreso de los activos. Se ingresará la siguiente información: - Código - Nombre - Detalle
Usuario	Analista
Historia de Usuario	T02
Prioridad	Alta
Precondición	N/A

Fuente: investigadora

Tabla 35. *Requisito Funcional 2*

RQF002	Ingreso de Activos
Descripción	El usuario deberá poder ingresar los activos con todos sus datos al sistema, como son: - Código - Nombre - Descripción - Tipo de activo - Unidad responsable - Persona responsable - Ubicación del activo - Proceso de negocio al que está vinculado Los datos de tipo de activo, unidad responsable y persona responsable deben seleccionarse desde un catálogo.
Usuario	Analista
Historia de Usuario	T02
Prioridad	Alta
Precondición	RQF001

Fuente: investigadora

Tabla 36. *Requisito Funcional 3*

RQF003	Valoración de Activos
Descripción	Por cada activo ingresado el usuario podrá ingresar una valoración numérica en las dimensiones de: - Disponibilidad - Integridad - Confidencialidad El valor del activo se calculará automáticamente mediante la sumatoria de los valores en cada dimensión.
Usuario	Analista
Historia de Usuario	T02
Prioridad	Alta
Precondición	RQF002

Fuente: investigadora

Tabla 37. *Requisito Funcional 4*

RQF004	Catálogo de amenazas
Descripción	El usuario debe poder ingresar y administrar un catálogo general de posibles amenazas para los activos. Este catálogo debe contener: - Código - Descripción - Dimensiones a las que afecta la amenaza - Información detallada de la amenaza
Usuario	Analista
Historia de Usuario	T03
Prioridad	Alta
Precondición	

Fuente: investigadora

Tabla 38. *Requisito Funcional 5*

RQF005	Asignación de amenazas a activos
Descripción	El usuario debe poder vincular las amenazas a los activos, de tal manera que, cada activo puede tener 1 o más amenazas. Para esto, por cada código de activos se asignará: - Código de la amenaza - Probabilidad de ocurrencia de la amenaza - Degradación del activo en la Disponibilidad - Degradación del activo en la Integridad - Degradación del activo en la Confidencialidad
Usuario	Analista
Historia de Usuario	T03
Prioridad	Alta
Precondición	RQF002, RQF004

Fuente: investigadora

Tabla 39. *Requisito Funcional 6*

RQF006	Matriz de riesgos
Descripción	En base a la información ingresada, el sistema debe calcular el impacto y el nivel de riesgo de los activos, clasificándolos de la siguiente manera: - Totalmente tolerables - Regularmente tolerables - No tolerables
Usuario	Todos
Historia de Usuario	T04
Prioridad	Alta
Precondición	RQF005

Fuente: investigadora

Tabla 40. *Requisito Funcional 7*

RQF007	Ingreso de controles
Descripción	Por cada uno de los riesgos determinados como No Tolerables y Regularmente Tolerables se debe ingresar los controles seleccionados de la norma ISO 27002. El usuario deberá registrar: - El código del control seleccionado - Fórmula de cálculo - Porcentaje de cumplimiento - Fecha de revisión
Usuario	Analista
Historia de Usuario	T04
Prioridad	Alta
Precondición	RQF006

Fuente: investigadora

Tabla 41. *Requisito Funcional 8*

RQF008	Reportes
Descripción	El usuario debe disponer de una pantalla inicial que le permita tener información de primera mano sobre el estado del SGSI. Debe disponer además de una opción para obtener los siguientes reportes: - Reporte de catálogo de activos - Reporte de activos por proceso - Reporte de catálogo de amenazas - Reporte de riesgos - Reporte de controles ingresados
Usuario	Todos
Historia de Usuario	T05
Prioridad	Alta
Precondición	

Fuente: investigadora

4.9.1.4 Especificación de requisitos no funcionales

Los requisitos no funcionales aplicados al sistema se presentan a continuación:

Tabla 42. *Requisito No Funcional 1*

RQNF001	Software base
Descripción	El sistema de funcionar en plataformas Linux o Windows.
Usuario	N/A
Historia de Usuario	T01
Prioridad	Alta
Precondición	

Fuente: investigadora

Tabla 43. *Requisito No Funcional 2*

RQNF002	Arquitectura
Descripción	El sistema se debe desarrollar en ambiente web con prime faces y EJBs para poder escalar con facilidad.
Usuario	N/A
Historia de Usuario	T01
Prioridad	Alta
Precondición	

Fuente: investigadora

Tabla 44. *Requisito No Funcional 3*

RQNF003	Base de datos
Descripción	La base de datos del sistema debe estar sobre Oracle 11g. La conexión hacia la base debe realizarse con JPA.
Usuario	N/A
Historia de Usuario	T01
Prioridad	Alta
Precondición	

Fuente: investigadora

Tabla 45. *Requisito No Funcional 3*

RQNF003	Base de datos
Descripción	La base de datos del sistema debe estar sobre Oracle 11g. La conexión hacia la base debe realizarse con JPA.
Usuario	N/A
Historia de Usuario	T01
Prioridad	Alta
Precondición	

Fuente: investigadora

4.9.1.5 Tecnología y arquitectura de desarrollo

Por especificación de requisitos no funcionales se adopta la tecnología y arquitectura de desarrollo existente en Emelnorte, las información de esta arquitectura ha sido tomada de la tesis de maestría DISEÑO DE LA ARQUITECTURA EMPRESARIAL DE APLICACIONES INFORMATICAS PARA LA EMPRESA EMELNORTE MEDIANTE ESTANDARES ABIERTOS Y SOFTWARE LIBRE (Rea, 2014), desarrollada por el Ing. Mauricio Rea Msc.

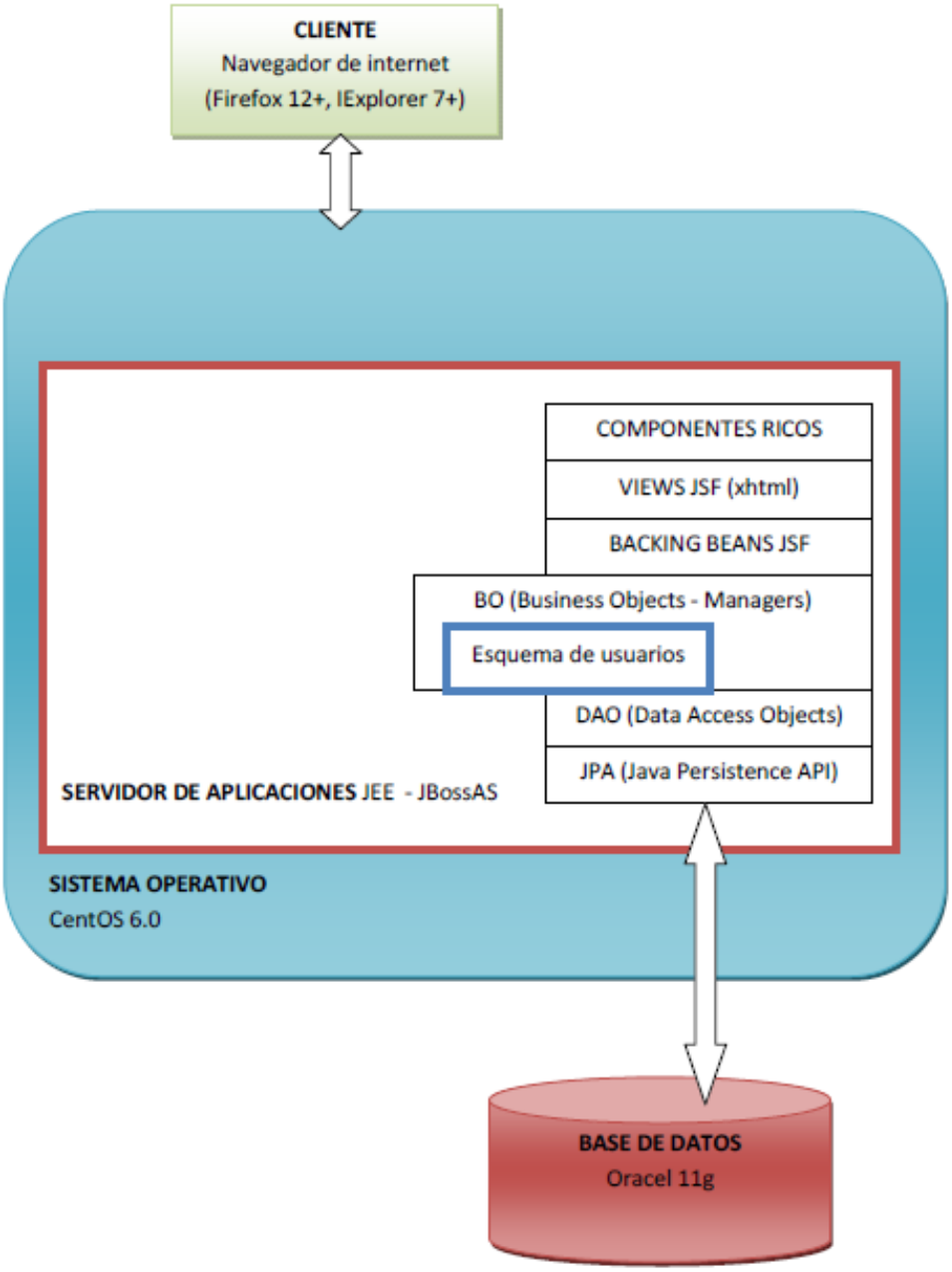


Figura 15. Arquitectura de Aplicaciones ERP de Emelnorte
Fuente: (Rea, 2014)

Patrones de arquitectura:

- Arquitectura de n-capas: que permite una mayor modularidad de los sistemas y mejor definición, distribución e integración de funciones entre componentes.
- Modelo, Vista y Controlador (MVC): para la organización básica de los componentes, sobre todo en la explotación de aplicaciones de tipo web.

Otros patrones de diseño utilizados en la plataforma de software de Emelnorte:

- Data Transfer Object (DTO)
- Data Access Object (DAO)

- Singleton
- Factory

Frameworks de trabajo:

- JavaServer Faces (JSF) como framework principal de desarrollo.
- Java Persistence API (JPA) para el manejo de persistencia de información.
- eXtensible HyperText Markup Language (XHTML) para la definición base de la Vista.
- PrimeFaces para crear clientes ricos.

4.9.2 Fase 2. Diseño

4.9.2.1 Especificación de casos de uso

4.9.2.1.1 Casos de uso Módulo de Activos

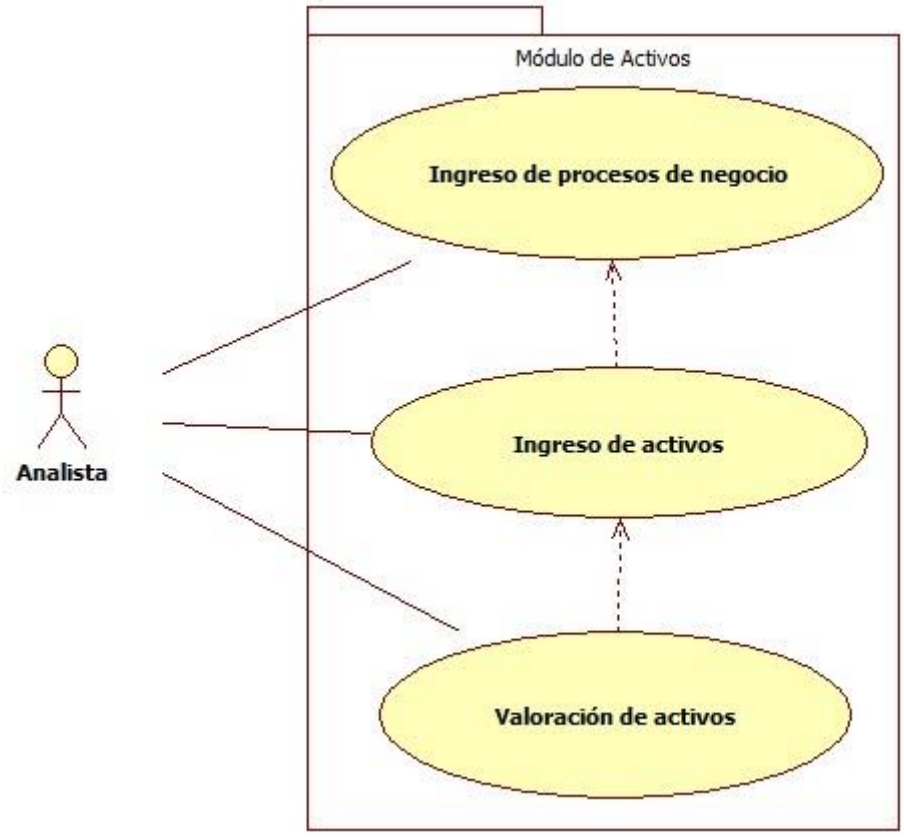


Figura 16. Caso de uso Módulo de Activos
Fuente: Investigadora

Tabla 46. *Especificación Caso de Uso Registro de Procesos*

Módulo de Activos	
Descripción	Este caso de uso describe el procedimiento de caso de uso REGISTRO DE PROCESOS.
Actores	Analista
Precondición	El usuario debe loguearse a través de la interfaz de SIGEERN
Flujo Principal	
1. El usuario ingresa a la opción de registro de procesos de negocio. 2. El usuario ingresa los datos de código, nombre y detalle del proceso de negocio de la institución. 3. El usuario Presiona el botón “Ingresar” 4. El Sistema almacena automáticamente la información en la base de datos. 5. El caso de uso termina.	
Post-Condición:	

Fuente: investigadora

Tabla 47. *Especificación Caso de Uso Ingreso de Activos*

Módulo de Activos	
Descripción	Este caso de uso describe el funcionamiento del caso de uso INGRESO DE ACTIVO.
Actores	Analista
Precondición	El usuario debe registrar los procesos de negocio.
Flujo Principal	
1. El usuario ingresa a la opción de ingreso de activos. 2. El usuario ingresa los datos del activo: código, nombre, descripción, tipo, responsable, ubicación y proceso de negocio al que pertenece. 3. El usuario presiona el botón “Ingresar” 4. El Sistema almacena automáticamente la información en la base de datos y actualiza el catálogo de activos. 5. El caso de uso termina.	
Post-Condición:	

Fuente: investigadora

Tabla 48. *Especificación Caso de Uso Valoración de Activos*

Módulo de Activos	
Descripción	Este caso de uso describe el funcionamiento del caso de uso VALORACIÓN DE ACTIVOS.
Actores	Analista
Precondición	El usuario debe registrar los activos de información.
Flujo Principal	
1. El usuario ingresa a la opción de valoración de activos 2. El sistema presenta el catálogo de activos registrados 3. El usuario selecciona la opción EDITAR en el activo correspondiente 4. El usuario ingresa o modifica los valores del activo en las dimensiones de: Disponibilidad, Integridad y Confidencialidad 5. El usuario selecciona la opción de guardar 6. El sistema almacena la información en la base de datos y actualiza el catálogo de activos. 7. El caso de uso termina.	
Post-Condición:	

Fuente: investigadora

4.9.2.1.2 Caso de uso Módulo de Amenazas

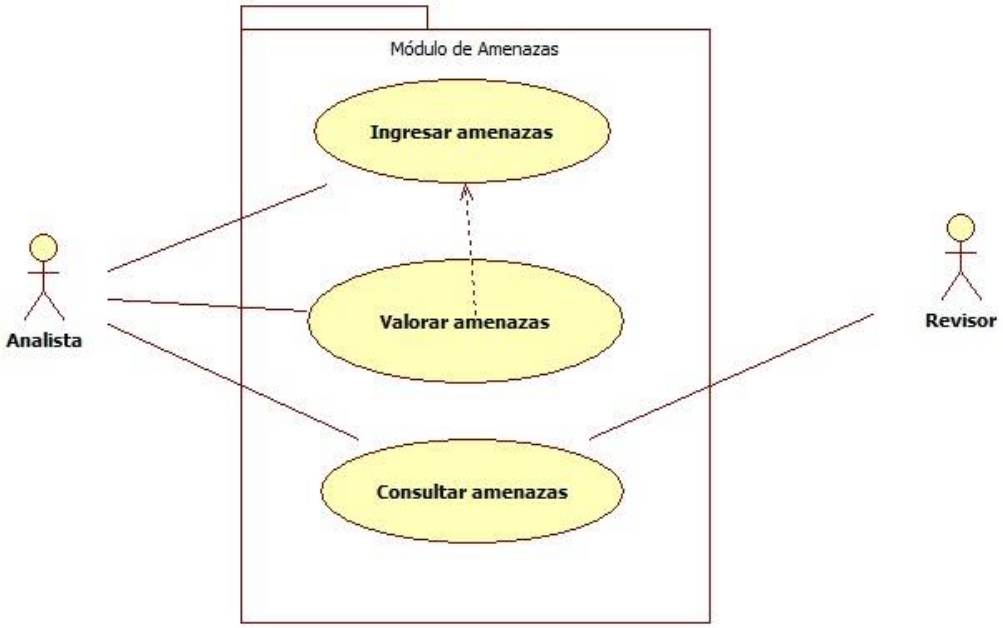


Figura 17. Caso de uso Módulo de Amenazas
Fuente: Investigadora

Tabla 49. *Especificación Caso de Uso Ingreso de Amenazas*

Módulo de Amenazas	
Descripción	Este caso de uso describe el funcionamiento del caso de uso INGRESO DE AMENAZAS.
Actores	Analista
Precondición	
Flujo Principal	
1. El usuario ingresa a la opción de INGRESAR AMENAZAS 2. El sistema presenta el catálogo de amenazas ingresadas 3. El usuario ingresa los datos de la nueva amenaza para el catálogo: código y descripción 4. El usuario selecciona la opción de guardar 5. El sistema almacena la información en la base de datos y actualiza el catálogo de amenazas. 6. El caso de uso termina.	

Post-Condición:

Fuente: investigadora

Tabla 50. *Especificación Caso de Uso Valoración de Amenazas*

Módulo de Amenazas	
Descripción	Este caso de uso describe el funcionamiento del caso de uso CONSULTAR AMENAZAS.
Actores	Analista, Revisor
Precondición	
Flujo Principal	
1. El usuario se logue a en el sistema 2. El usuario ingresa a la opción de registro de amenazas 3. El sistema muestra la lista de amenazas ingresadas que pueden ser filtradas por su nombre	
Post-Condición:	

Fuente: investigadora

Tabla 51. *Especificación Caso de Uso Valoración de Amenazas*

Módulo de Amenazas	
Descripción	Este caso de uso describe el funcionamiento del caso de uso VALORACIÓN DE AMENAZAS.
Actores	Analista
Precondición	Ingresar el catálogo de amenazas
Flujo Principal	

4. El usuario ingresa a la opción de VALORAR AMENAZAS 5. El sistema presenta el catálogo de amenazas seleccionadas para los activos y sus valoraciones 6. El usuario selecciona el activo para el cual se ingresarán las amenazas 7. El usuario selecciona la amenaza seleccionada para el activo 8. El usuario ingresa el valor de *probabilidad de ocurrencia* 9. El usuario ingresa el valor de la degradación del activo para la amenaza seleccionada en las dimensiones de: Disponibilidad, Integridad y Confidencialidad. 10. El usuario selecciona la opción *guardar* 11. El sistema guarda los datos en la base de datos y actualiza el catálogo 12. Para modificar los datos de la valoración de la amenaza el usuario debe seleccionar la opción editar en la lista mostrada, modificar los datos y seleccionar la opción guardar. 13. El caso de uso termina.
Post-Condición:

Fuente: investigadora

4.9.2.1.3 Caso de uso Módulo de Riesgos y Controles

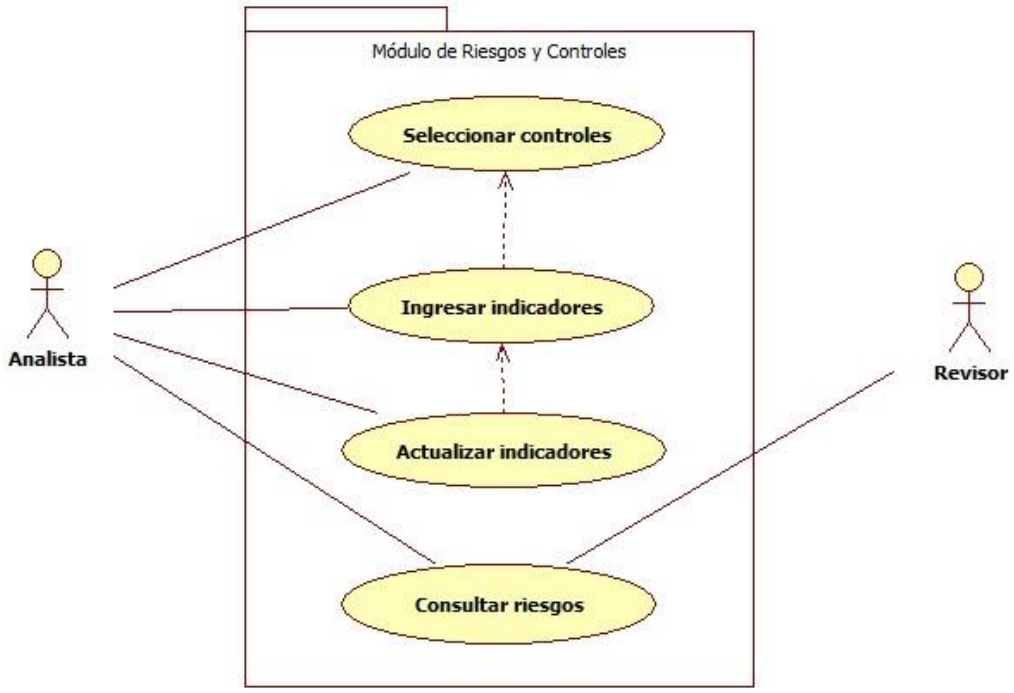


Figura 18. Caso de uso Módulo de Riesgos y Controles
Fuente: Investigadora

Tabla 52. *Especificación Caso de Uso Gestión de Riesgos*

Módulo de Riesgos	
Descripción	Este caso de uso describe el funcionamiento del caso de uso SELECCIONAR CONTROLES.
Actores	Analista
Precondición	Ingresar y valorar activos y amenazas
Flujo Principal	
1. El usuario se loguea en el sistema 2. El usuario ingresa al módulo de riesgos 3. El usuario selecciona el riesgo sobre el que desea parametrizar controles 4. El usuario selecciona el control a agregar para el riesgo seleccionado 5. El sistema asigna el control seleccionado al riesgo. 6. El caso de uso termina.	
Post-Condición:	

Fuente: investigadora

Tabla 53. *Especificación Caso de Uso Gestión de Riesgos*

Módulo de Riesgos	
Descripción	Este caso de uso describe el funcionamiento del caso de uso INGRESAR INDICADORES.
Actores	Analista
Precondición	Ingresar y valorar activos y amenazas
Flujo Principal	
7. El usuario se loguea en el sistema 8. El usuario ingresa al módulo de riesgos 9. El usuario selecciona el control para el cual desea ingresar los indicadores 10. El usuario ingresa los datos de: detalle, fórmula, porcentaje de cumplimiento y fecha de revisión, del nuevo indicador 11. El sistema guarda la información registrada. 12. El caso de uso termina.	
Post-Condición:	

Fuente: investigadora

Tabla 54. *Especificación Caso de Uso Gestión de Riesgos*

Módulo de Riesgos	
Descripción	Este caso de uso describe el funcionamiento del caso de uso ACTUALIZAR INDICADORES.
Actores	Analista
Precondición	Ingresar y valorar activos y amenazas
Flujo Principal	

13. El usuario se loguea en el sistema 14. El usuario ingresa al módulo de riesgos 15. El usuario selecciona el indicador que desea modificar 16. El usuario modifica los datos de porcentaje de cumplimiento y fecha de revisión 17. El sistema guarda la información registrada. 18. El caso de uso termina.
Post-Condición:

Fuente: investigadora

Tabla 55. *Especificación Caso de Uso Gestión de Riesgos*

Módulo de Riesgos	
Descripción	Este caso de uso describe el funcionamiento del caso de uso CONSULTAR INDICADORES.
Actores	Analista, Revisor
Precondición	Ingresar y valorar activos y amenazas
Flujo Principal	
19. El usuario se loguea en el sistema 20. El usuario ingresa al módulo de riesgos 21. El sistema presenta el listado de los riesgos registrados hasta el momento con los datos de probabilidad de ocurrencia, impacto, riesgo potencial, riesgo residual, y tolerancia. 22. El caso de uso termina.	
Post-Condición:	

Fuente: investigadora

4.9.2.1.4 Caso de uso Módulo de Reportes

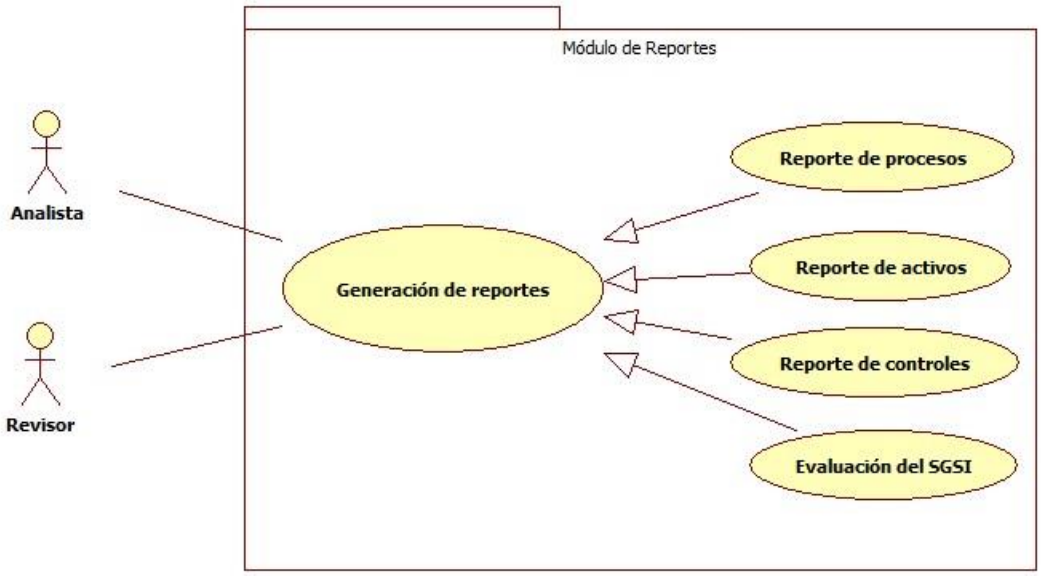


Figura 19. Caso de uso Módulo de Reportes
Fuente: Investigadora

Tabla 56. *Especificación Caso de Uso Generación de Reportes*

Módulo de Riesgos	
Descripción	Este caso de uso describe el funcionamiento del caso de uso GENERACIÓN DE REPORTES.
Actores	Analista
Precondición	
Flujo Principal	
1. El usuario ingresa a la opción de REPORTES 2. El sistema presenta el catálogo de reportes que pueden generarse 3. El usuario selecciona el reporte a generar 4. El usuario ingresa los parámetros solicitados por el reporte 5. El usuario selecciona la opción *generar* 6. El sistema genera el reporte 7. El caso de uso termina.	
Post-Condición:	

Fuente: investigadora

4.9.2.2 Diagrama Entidad Relación

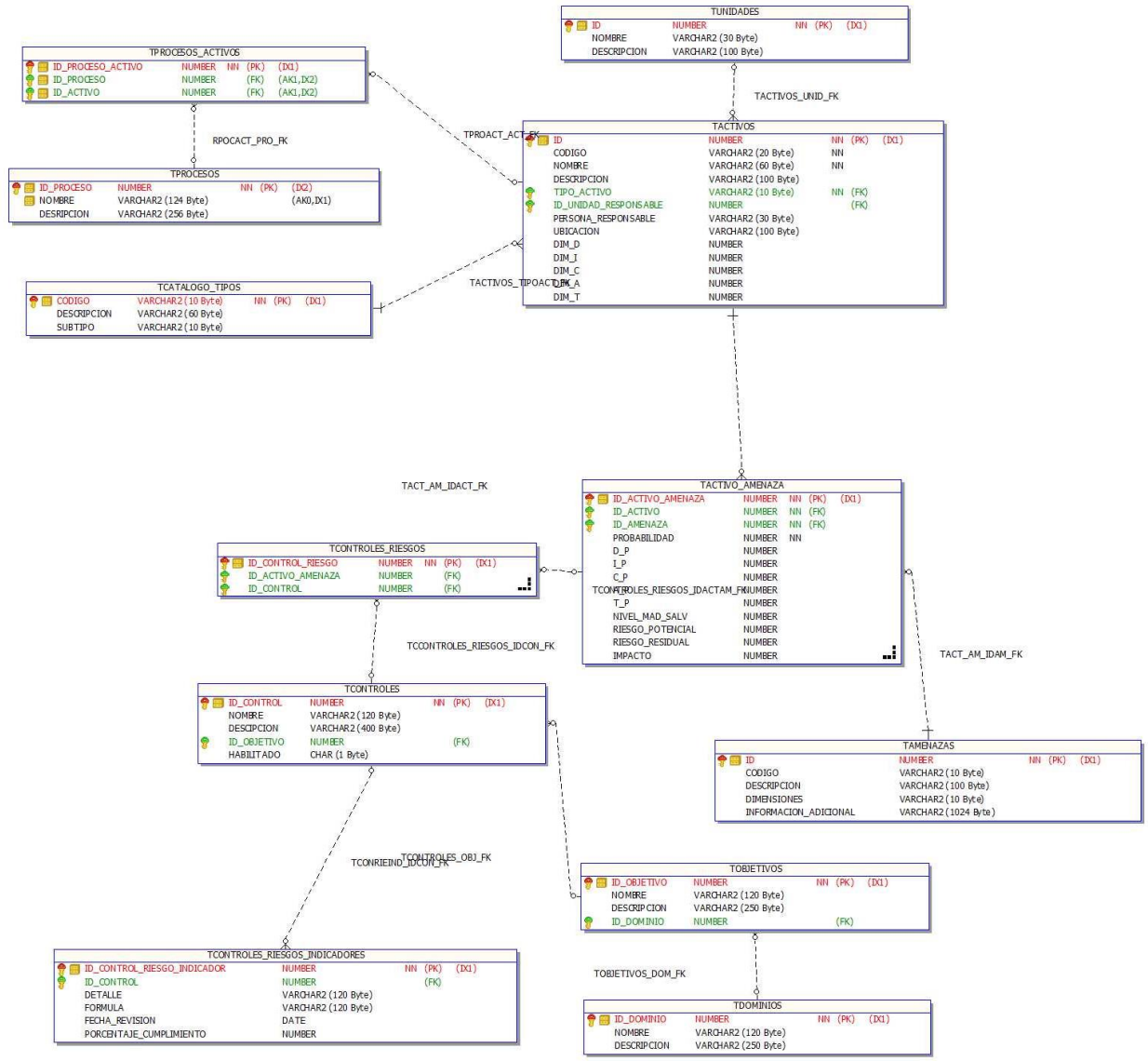


Figura 20. Diagrama Entidad-Relación
Fuente: Investigadora

4.9.2.3 Diagrama de módulos

El software propuesto consta de cuatro módulos que abarcan la funcionalidad básica solicitada por el usuario. El siguiente diagrama muestra la distribución de la funcionalidad entre los módulos:

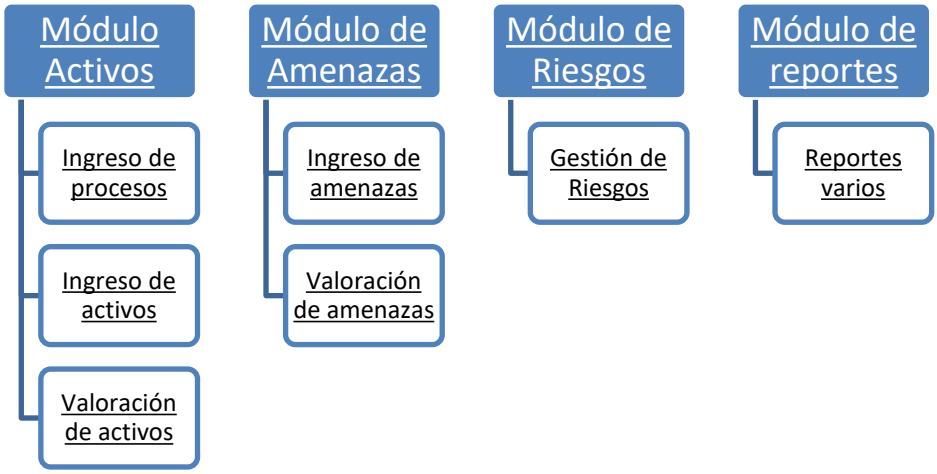


Figura 21. Diagrama de módulos
Fuente: Investigadora

4.9.3 Fase 3. Desarrollo

Para el desarrollo del software, por requerimiento de usuario, se adoptó la arquitectura de software existente en Emelnorte, incluyendo el diseño de interfaz.

4.9.3.1 Diseño de Interfaces

Se desarrollaron las siguientes interfaces para los módulos propuestos:

4.9.3.1.1 Interfaz Módulo de Activos

Figura 22. Acceso al Módulo de Activos
Fuente: Investigadora

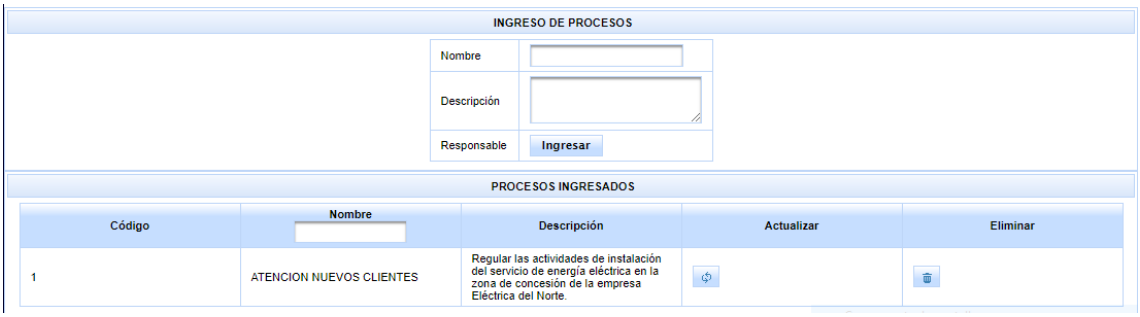


Figura 23. Pantalla de ingreso de procesos
Fuente: Investigadora

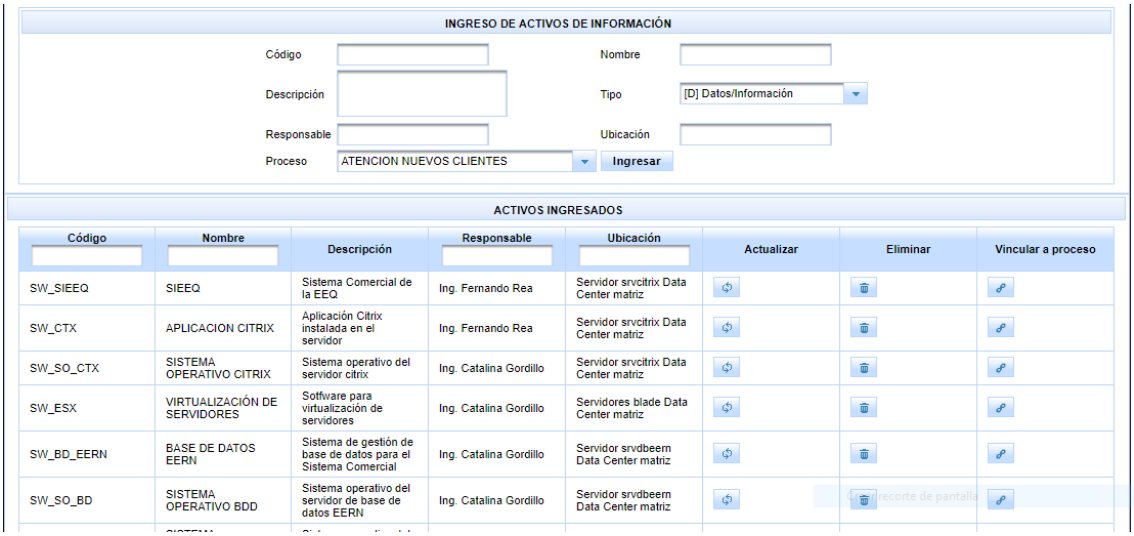


Figura 24. Pantalla de ingreso de activos
Fuente: Investigadora

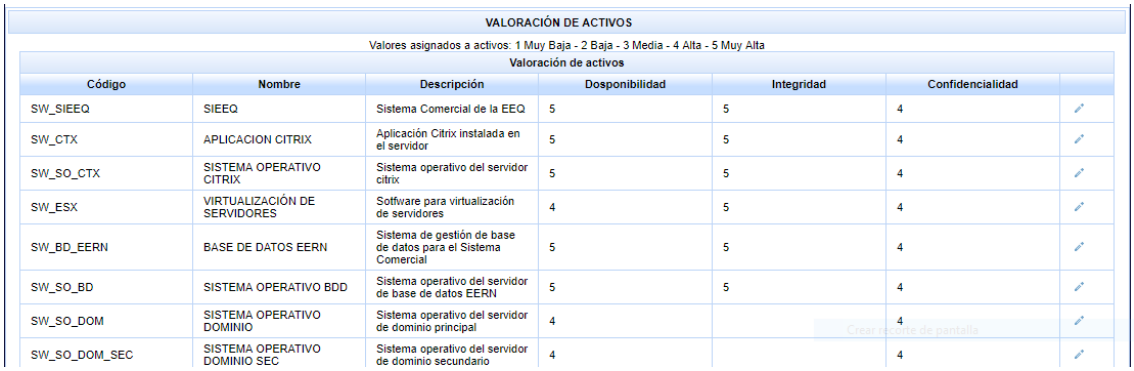


Figura 25. Pantalla de valoración de activos
Fuente: Investigadora

4.9.3.1.2 Interfaz Módulo de Amenazas

Figura 26. Acceso al Módulo de Amenazas
Fuente: Investigadora

Figura 27. Pantalla de ingreso de amenazas
Fuente: Investigadora

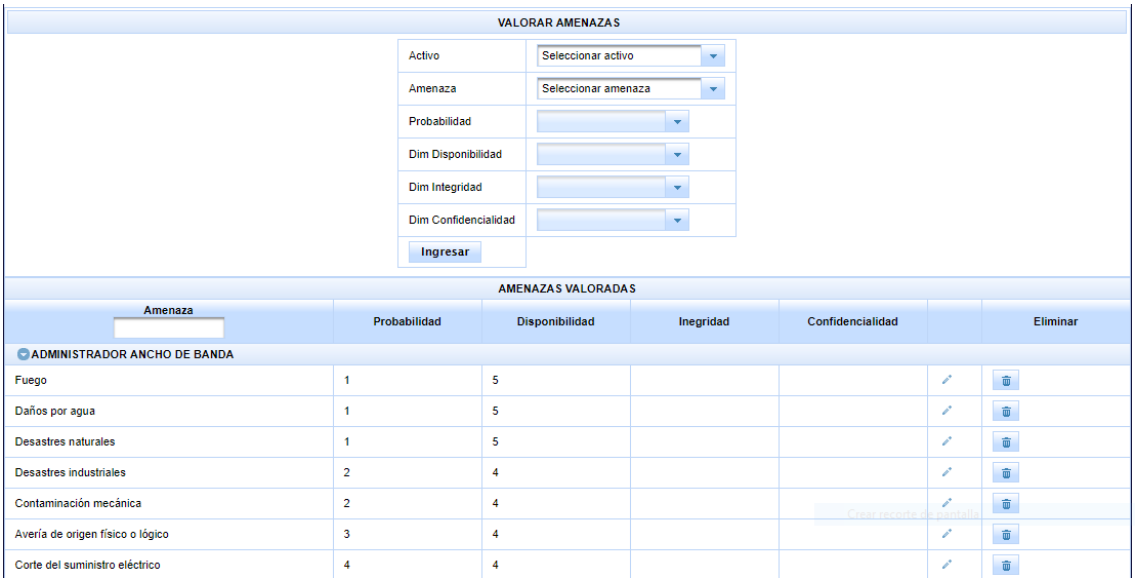


Figura 28. Pantalla de valoración de amenazas
Fuente: Investigadora

4.9.3.1.3 Interfaz Módulo de Riesgos

Figura 29. Ingreso Módulo Gestión de Riesgos
Fuente: Investigadora

Figura 30. Pantalla de Gestión de Riesgos
Fuente: Investigadora

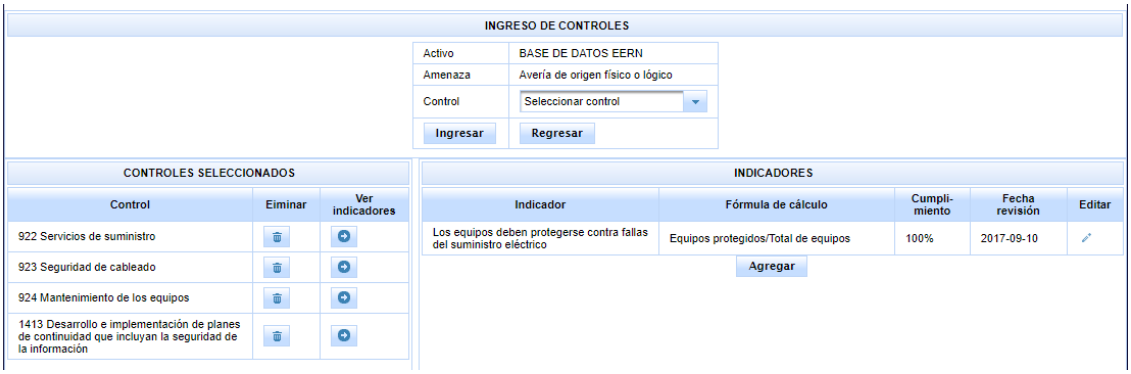


Figura 31. Pantalla de Ingreso de controles
Fuente: Investigadora

4.9.3.1.4 Interfaz Módulo de Reportes

Figura 32. Ingreso al Módulo de Reportes
Fuente: Investigadora

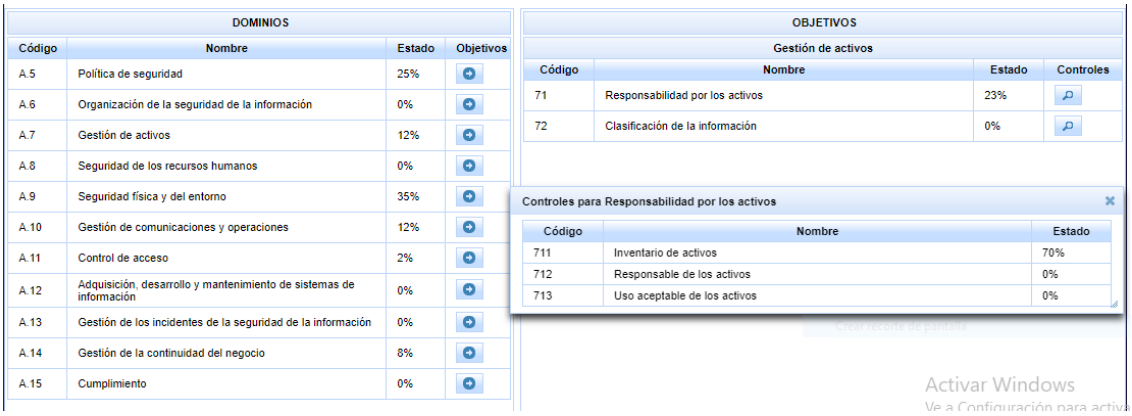


Figura 33. Pantalla de Reporte de implantación de controles
Fuente: Investigadora

4.9.4 Fase 4. Pruebas

Las pruebas de aceptación, en esta fase, son pruebas de caja negra que permite asegurar las funcionalidades del sistema con los requerimientos de las historias de usuario. En esta metodología, estas pruebas son únicamente responsabilidad del cliente ya que en cada iteración se reflejó las funcionales que se deseaba obtener, llegando así a determinar el correcto funcionamiento del sistema.

Los criterios de usabilidad se definen en base a los requisitos implementados en los prototipos de cada uno de los módulos y descritos en los casos de prueba.

4.9.4.1 Pruebas de Aceptación

4.9.4.1.1 Casos de prueba

Este módulo contiene dos funcionalidades básicas que son el ingreso del activo y la valoración del mismo. Se determinaron los siguientes casos de prueba:

Tabla 57. *Caso de prueba 1*

CP001	**Iniciar la aplicación**
RQF	RQF01
Descripción	El usuario deberá poder ingresar los diferentes procesos de negocio de la institución previo al ingreso de los activos. Se ingresará la siguiente información: - Código - Nombre - Detalle
Pre condiciones	N/A
Pasos y condiciones de ejecución	- El usuario ingresa a la opción *Ingresar Procesos* del módulo de activos. - El usuario ingresa los datos de: o Código o Nombre o Descripción - El usuario presiona el botón *Ingresar* - El sistema actualiza la lista con el nuevo proceso - El sistema despliega el mensaje de *Ingreso correcto*
Resultado esperado 1	Proceso Ingresado
Estado Caso de prueba	Superada

Fuente: investigadora

Tabla 58. *Caso de prueba 2*

CP002	**Iniciar la aplicación**
RQF	RQF02
Descripción	El usuario deberá poder ingresar los activos con todos sus datos al sistema, como son: - Código - Nombre - Descripción - Tipo de activo - Unidad responsable - Persona responsable - Ubicación del activo - Proceso de negocio al que está vinculado Los datos de tipo de activo, unidad responsable y persona responsable deben seleccionarse desde un catálogo.
Pre condiciones	N/A

Pasos y condiciones de ejecución	- El usuario ingresa a la opción *Ingresar Activos* del módulo de activos. - El usuario ingresa los datos de: o Código o Nombre o Descripción o Selecciona el tipo de Activo o Responsable o Ubicación o Proceso al cual se encuentra vinculado el activo - El usuario presiona el botón *Ingresar* - El sistema actualiza la lista con el nuevo activo - El sistema despliega el mensaje de *Ingreso correcto*
Resultado esperado 1	Activo Ingresado
Estado Caso de prueba	Superada

Fuente: investigadora

Tabla 59. *Caso de prueba 3*

CP003	**Iniciar la aplicación**
RQF	RQF03
Descripción	Por cada activo ingresado el usuario podrá ingresar una valoración numérica en las dimensiones de: - Disponibilidad - Integridad - Confidencialidad El valor del activo se calculará automáticamente mediante la sumatoria de los valores en cada dimensión.
Pre condiciones	N/A
Pasos y condiciones de ejecución	- El usuario ingresa a la opción *Valorar Activos* del módulo de activos. - El usuario selecciona el activo a valorar y presiona el botón editar - El usuario edita los valores para las dimensiones Disponibilidad, Integridad y Confidencialidad - El usuario presiona el botón *Ok* - El sistema actualiza los valores cambiados

	- El sistema despliega el mensaje de *Actualización correcta*
Resultado esperado 1	Valoración ingresada
Estado Caso de prueba	Superada

Fuente: investigadora

Tabla 60. *Caso de prueba 4*

CP004	**Iniciar la aplicación**
RQF	RQF04
Descripción	El usuario debe poder ingresar y administrar un catálogo general de posibles amenazas para los activos. Este catálogo debe contener: - Código - Descripción - Dimensiones a las que afecta la amenaza - Información detallada de la amenaza.
Pre condiciones	N/A
Pasos y condiciones de ejecución	- El usuario ingresa a la opción *Ingresar Amenazas* del módulo de amenazas. - El usuario ingresa los datos de o Código o Descripción - El usuario presiona el botón I*ngresar* - El sistema actualiza la lista con la amenaza ingresada - El sistema despliega el mensaje de *Ingreso correcto*
Resultado esperado 1	Amenaza ingresada
Estado Caso de prueba	Superada

Fuente: investigadora

Tabla 61. *Caso de prueba 5*

CP005	**Iniciar la aplicación**
RQF	RQF05
Descripción	El usuario debe poder vincular las amenazas a los activos, de tal manera que, cada activo puede tener 1 o más amenazas. Para esto, por cada código de activos se asignará: - Código de la amenaza

	- Probabilidad de ocurrencia de la amenaza - Degradación del activo en la Disponibilidad - Degradación del activo en la Integridad - Degradación del activo en la Confidencialidad
Pre condiciones	N/A
Pasos y condiciones de ejecución	- El usuario ingresa a la opción *Valorar Amenazas* del módulo de amenazas. - El usuario ingresa los siguientes datos: o Selecciona el activo o Selecciona la amenaza o Selecciona la probabilidad de ocurrencia o Selecciona el valor para la dimensión Disponibilidad o Selecciona el valor para la dimensión Integridad o Selecciona el valor para la dimensión Confidencialidad - El usuario presiona el botón I*ngresar* - El sistema actualiza la lista con los datos ingresados - El sistema despliega el mensaje de *Ingreso correcto*
Resultado esperado 1	Valoración de Amenaza ingresada
Estado Caso de prueba	Superada

Fuente: investigadora

Tabla 62. *Caso de prueba 6*

CP006	**Iniciar la aplicación**
RQF	RQF07
Descripción	En base a la información ingresada, el sistema debe calcular el impacto y el nivel de riesgo de los activos, clasificándolos de la siguiente manera: - Totalmente tolerables - Regularmente tolerables - No tolerables
Pre condiciones	N/A
Pasos y condiciones de ejecución	- El usuario ingresa a la opción *Gestionar Riesgos* del módulo de riesgos. - El sistema presenta el listado de riesgos clasificados

	por: o Totalmente tolerables o Regularmente tolerables o No tolerables - El usuario selecciona el riesgo para el que desea ingresar controles - El usuario presiona el botón *Ingresar controles* - El sistema presenta la pantalla de ingreso de controles - El usuario ingresa los datos de : o Control o Detalle o Fórmula o Porcentaje de cumplimiento o Fecha revisión - El usuario presiona el botón *Ingresar* - El sistema actualiza el listado con el control ingresado - El sistema despliega el mensaje de *Ingreso correcto*
Resultado esperado 1	Control ingresado
Estado Caso de prueba	Superada

Fuente: investigadora

4.9.5 Fase 5. Implantación

El software fue implementado y puesto en producción en los servidores de Emelnorte, los cuales implementan la siguiente arquitectura:

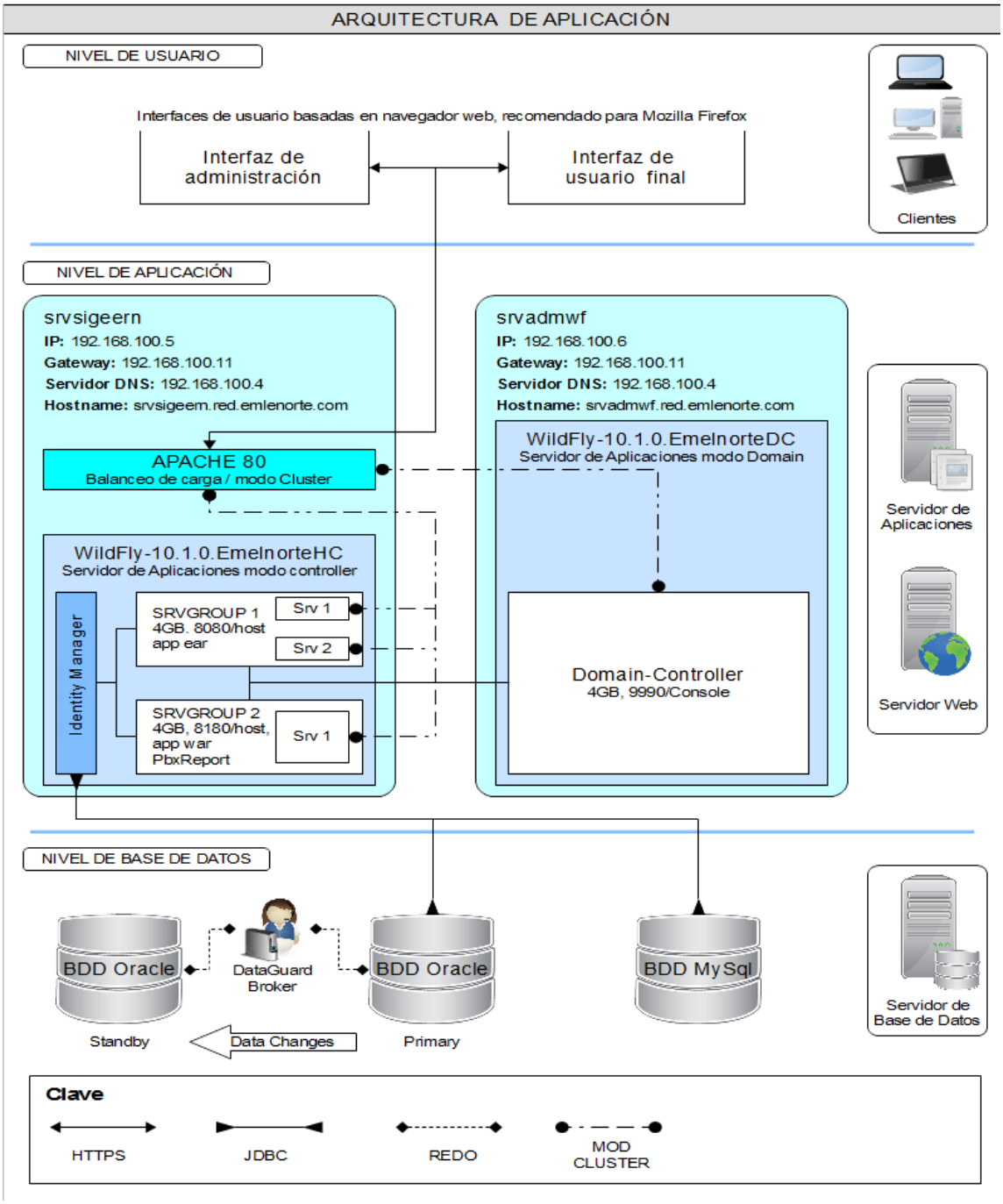


Figura 34. Arquitectura de servidores de aplicaciones
Fuente: (Grijalva, 2017)

La figura anterior muestra el esquema de alta disponibilidad implementado para el despliegue de aplicaciones levantadas en el servidor Wildfly 10, el cual consta de un servidor instalado en modo Domain, donde se tiene un punto central de administración. Un servidor instalado en modo Host Controller con dos instancias que realizan balanceo de aplicaciones. Las aplicaciones se conectan a las diferentes bases de datos mediante datasources creados en los servidores de aplicaciones.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El uso del estándar ISO/IEC 27001 se ha convertido en una tendencia de las instituciones que cuentan con una infraestructura de TI robusta y consolidada, puesto que el aseguramiento de la información constituye un pilar fundamental en la continuidad del negocio.

- Con el análisis de riesgos de los activos de información en Emelnorte, se pudo evidenciar que el 39% de estos activos se ven afectados por riesgos no tolerables, los cuales deben ser tratados de manera inmediata para reducir el riesgo con la aplicación del Plan de tratamiento de riesgos definido para este efecto, a fin de asegurar la continuidad del negocio.

- Es necesario el uso de un sistema informático para mantener, controlar y evaluar un SGSI de manera óptima, ya que la información manejada puede llegar a ser muy extensa dificultando su correcto tratamiento e interpretación, en estos casos, el uso de un software desarrollado a medida se convierte en una herramienta clave para la gestión.

- El desarrollo de un sistema a medida e integrado con la arquitectura empresarial existente en Emelnorte representa un factor de éxito puesto que el software se encuentra implementado bajo una plataforma robusta y probada que permite asegurar su disponibilidad y seguridad.

5.2 Recomendaciones

- Se recomienda la revisión periódica del SGSI y la retroalimentación de los controles e indicadores planteados para afinar el plan de seguridad.

- Se recomienda seguir con la utilización de la metodología de gestión de riesgos, aplicándola al resto de procesos de negocio de la institución, para lograr la reducción de riesgos de los activos asociados a dichos procesos y conseguir un mayor cumplimiento de la norma ISO 27001.

- Se recomienda formar y capacitar de manera periódica al personal en temas de seguridad de la información para lograr un empoderamiento por parte de los usuarios en la seguridad y alcanzar las metas planteadas con mayor facilidad.

- Se recomienda mantener una constante revisión de la política del SGSI y verificar el cumplimiento de la misma por parte de los empleados de la organización.

CAPITULO VI. BIBLIOGRAFÍA

(s.f.). Obtenido de Términos de uso información iso27000: http://www.iso27000.es/sgsi.html

Navarro Cadavid, A., Fernández Martínez, J., & Morales Vélez, J. (2013). Revisión de metodologías para el desarrollo de software. *Prospect*.

El portal de ISO 27001 en Español. (2012). Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

MAGERIT – versión 3.0. (2012). Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WcsbOsjyjIU

Ardila, V. A. (2017). *Conceptos basicos en buenas practicas de TI y seguridad informatica.*

Areitio, J. (2008). *Seguridad de la Información.* España: Paraninfo S.A.

Barragán Sánchez, R., Mimbrero Mallado, C., & Pacheco González, R. (13 de 02 de 2016). *Revista Electrónica de Investigación y Docencia*. Obtenido de http://revistaselectronicas.ujaen.es/index.php/reid/article/view/989

Batalla, L. (2006). *Extreme Programming XP*.

Bernal, C. A. (2010). *Metodología de la Investigación.* Bogotá: Pearson.

Bernal, J. (2013). *El círculo de Deming de mejora continua*. Obtenido de https://www.pdcahome.com/5202/ciclo-pdca/

BORTNIK, S. (s.f.). *La serie de normas ISO 27000*. Obtenido de welivesecurity: http://www.welivesecurity.com/la-es/2010/04/16/la-serie-de-normas-iso-27000/

Canós, J. H., & Penadés, C. (2004). *Métodologías Ágiles para el desarrollo de software: eXtreme Programming (XP)*. Obtenido de ttp://www.willydev.net/descargas/prev/TodoAgil.Pdf

Caralt, J. (2010). *NTRODUCCION AL BUSINESS INTELLIGENCE.* Catalunya: UOC (UNIVERSITAT OBERTA DE CATALUNYA).

CONTENTO, M. J. (2015). *Implementación de un esquema de seguridad a los cuartos de cómputo, de una empresa que se dedica a la elaboración y comercialización de plásticos.*

Cortés, D., & Ardila, A. (2012). *METODOLOGIA PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO.* Obtenido de http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2

Davara, F. (2015). *El Blog de Fernando Davara*. Obtenido de http://fernandodavara.com/riesgos-vs-amenazas-de-que-se-trata-realmente/

Defaz Toapanta, V. E. (2015). *DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS INEN ISO/IEC27000 PARA EL MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS.*

Directory, T. I. (s.f.). *The ISO 27000 Directory*. Obtenido de http://www.27000.org/iso-27002.htm

Emelnorte. (2012). *Levantamiento de procesos de negocio.*

Emelnorte. (2014). *ACTUALIZACIÓN PLAN ESTRATÉGICO 2014 - 2017.*

Espinoza, P. (2015). *Sistema de gestión de seguridad de la Información*. Obtenido de http://pamela7913.wixsite.com/sgsi/implementacionsgsi

Fiallos, D. (2016). *Aplicación para Gestión de Procesos de Desarrollo de Software Basados en la Metodología Ágil XP Extreme Programming para Software de la*

Sierra S.A. Pontificia Universidad Católica del Ecuador. Ambato: Departamento de Investigación y Posgrados.

Fowler, M. (2003). *The New Methodology*. Obtenido de http://www.martinfowler.com/articles/newMethodology.html

Gestiopolis. (12 de 02 de 2016). *Gestiopolis*. Obtenido de http://www.gestiopolis.com/14-puntos-de-la-calidad-segun-edwards-deming/

González Viancha, J. F. (2014). *METODOLOGIAS DE EVALUACION DE RIESGOS INFORMATICOS*. Obtenido de http://riesgosunad.blogspot.com/

Grijalva, E. (2017). *DIAGRAMA ARQUITECTÓNICO*.

Gutiérrez, A. (2006). *Curso de Métodos de Investigación.* Quito.

INEN. (2011). Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001. Quito, Pichincha, Ecuador.

Institucio Nacional de Tecnologías de a Comunicación, G. d. (2017). Recuperado el 04 de 2017, de Implantación de un SGSI en la empresa: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

Instituto para la Calidad. (Miércoles 25 de Julio de 2012). *Universidad Católica del Perú*. Obtenido de http://calidad.pucp.edu.pe/el-asesor/sistemas-integrados-de-gestion-una-clara-definicion#sthash.t7d8rp5k.dpuf

ISO 27001 - Sistema de Gestión de Seguridad de la Información. (s.f.). Recuperado el 19 de 07 de 2017, de 2011: http://www.redser.com/servicios/iso-27001.asp

Jeffries, R. (2001). *What is Extreme Programming?* Obtenido de http://www.xprogramming.com/xpmag/whatisxp.htm

Kosutic, D. (2013). *27001 Academy*. Obtenido de http://advisera.com/27001academy/es/que-es-iso-27001/

Lanche Capa, D. S. (s.f.). *DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA.*

Leiva, F. (2010). *Nociones de Metodología de la Investigación Científica.* Quito.

López Rubio, J. M., & Callejón Piicón, F. (2014). *Tecnologías de la información y la Comunicación.* Málaga: Grupo Editorial Planeta Alvi.

Maldonado, J. (14 de 02 de 2016). *Eumed.net Enciclopedia Virtual.* Obtenido de http://www.eumed.net/libros-gratis/2011e/1084/indice.htm

MINTIC. (15 de 03 de 2016). *SEGURIDAD Y PRIVACIDAD DE LA INFORMACION*. Recuperado el 12 de 03 de 2017, de www.mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Najar Pacheco, J. C., & Suárez Suárez, N. E. (2015). La seguridad de la información: un activo valioso de la. *Vínculos*.

Prendas Espinosa, M. P., & Sánchez Vera, M. (13 de 02 de 2016). *Investigación Universidad de Sevilla*. Obtenido de https://idus.us.es/xmlui/handle/11441/22569

Rea, M. (2014). *DISEÑO DE LA ARQUITECTURA EMPRESARIAL DE APLICACIONES INFORMATICAS PARA LA EMPRESA EMELNORTE MEDIANTE ESTANDARES ABIERTOS Y SOFTWARE LIBRE.*

Sangil Martinez, J. (2012). CRM ¿Filosofía o Tecnología? . *Ipsos Investigación de Mercados S.A.* , 19.

Skarzynski, P., & Gibson, R. (2012). *Innovación en el ADN de la Organización.* México: Cosegraf.

Solutions, A. E. (2017). *27001 Academy*. Recuperado el 20 de 04 de 2017, de https://advisera.com/27001academy/es/que-es-iso-27001/

Tur Ferrer, G., & Urbina Ramírez, S. (13 de 02 de 2016). *Dialnet*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=5292191

Valhondo Solano, D. (2010). *Gestión del Conocimiento, del Mito a la Realidad.* Madrid: Ediciones Díaz de Santos.

Vega, A. (2007). *Las 10 mejores prácticas en seguridad*. Obtenido de https://seguinfo.wordpress.com/2007/07/05/las-10-mejores-practicas-en-seguridad/

Wells, D. (2003). *Extreme Programming: A gentle introduction.* Obtenido de http://www.extremeprogramming.org/

YourERPsoftware. (12 de 02 de 2016). *YourERPSoftware*. Obtenido de www.YourERPsoftware.com