



Desarrollar un plan de acción, adecuado a la Agencia Nacional del Espectro - ANE, para proteger sus Sistemas de Información Misionales

**Eduing Osvaldo Díaz Barbosa**

Trabajo de grado para optar al título profesional:  
**Maestría en Ciberseguridad y Ciberdefensa**

**Escuela Superior de Guerra “General Rafael Reyes Prieto”**  
Bogotá D.C., Colombia

2018

TACIBER 2018

009

EJ. 2

i

**MINISTERIO DE DEFENSA NACIONAL  
COMANDO GENERAL DE LAS FUERZAS MILITARES  
ESCUELA SUPERIOR DE GUERRA**



Fundada en 1909

**DESARROLLAR UN PLAN DE ACCIÓN, ADECUADO A LA  
AGENCIA NACIONAL DEL ESPECTRO – ANE, PARA PROTEGER SUS  
SISTEMAS DE INFORMACIÓN MISIONALES.**

**ALUMNO: EDUING OSVALDO DÍAZ BARBOSA**

**DIRECTOR: ING. CÉSAR I. RODRÍGUEZ**

**MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA**

**TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE MAGISTER  
EN CIBERSEGURIDAD Y CIBERDEFENSA**

**BOGOTÁ – COLOMBIA**

**2018**

106250



**MINISTERIO DE DEFENSA NACIONAL  
COMANDO GENERAL DE LAS FUERZAS MILITARES  
ESCUELA SUPERIOR DE GUERRA**



Fundada en 1909

**DESARROLLAR UN PLAN DE ACCIÓN, ADECUADO A LA AGENCIA  
NACIONAL DEL ESPECTRO – ANE, PARA PROTEGER SUS SISTEMAS  
DE INFORMACIÓN MISIONALES.**

**ALUMNO: EDUING OSVALDO DÍAZ BARBOSA**

**DIRECTOR: ING. CÉSAR I. RODRÍGUEZ**

**MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA**

**TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE MAGISTER EN  
CIBERSEGURIDAD Y CIBERDEFENSA**

**BOGOTÁ – COLOMBIA**

**2018**

## Agradecimiento

A Dios por darme la vida y ayudarme hacer posible la realización de este proyecto.

A mi asesor de tesis César Iván Rodríguez, por su gran ayuda y comprensión durante el desarrollo del proyecto.

A mis compañeros de clases con los que he compartido grandes momentos.

A mis profesores, por haberme dedicado el tiempo para enseñarme el conocimiento adquirido.

**A TODOS MUCHAS GRACIAS**

A LA MEMORIA

A mis padres Rafael Díaz y María Barrios que mientras estudiaba a mi lado me incentivaron el verdadero valor que tiene la vida.

GRACIAS A TODOS

## Dedicatoria

Con todo mi amor para mi esposa Yenes del Carmen Tirado Contreras por su paciencia y apoyo brindado para poder sacar adelante este proyecto.

A mis hijas Geraldine Díaz y Sara Sofía Díaz, por ser fuente de inspiración y motivación para poder superarme cada día más.

A mis hermanos y demás familiares, quienes con sus palabras de aliento no me dejan decaer en los momentos más adversos de mi vida.

A mis amigos y compañeros, que sin esperar nada a cambio compartieron sus conocimientos, tristezas y alegrías durante todo este tiempo que estuvieron a mi lado apoyándome para que este sueño se hiciera realidad.

## A LA MEMORIA

De mis padres Rafael Díaz y María Barbosa que mientras estuvieron a mi lado me inculcaron el verdadero valor que tiene la vida.

## GRACIAS A TODOS



## Abstract

This project was developed in the “National Agency of the Spectrum - NAS -”, entity of the Colombian State, attached to the Ministry of Information and Communications - MINTIC - this agency is responsible for planning, allocating, monitoring and control the Radio electric Spectrum in Colombia, as well as provides technical advice for the efficient management and promote its knowledge.

The problem that has been presented in the Entity is that in recent years its mission information systems have suffered several cyber-attacks, which have caused a series of problems that affect the fulfillment of the objectives, causing a great impact internally so as to the society in general, putting at risk the principles of availability, integrity and confidentiality of the information stored in these systems.

To mitigate these cyber-attacks, it is proposed to generate an action plan based on a risk analysis, to detect the cyber risks to which these systems are exposed and thus be able to recommend the best treatments for each of them, so they can be implemented in the future by the Agency, in order to avoid the loss or alteration of the information.

The risk analysis carried out on the mission information systems of the NAS was based on the ISO 27001 methodologies or standards, which is an international standard formulated by the ISO and describes how to manage information security in a company. Implemented in any type of company whether public or private, large, medium or small and provides a methodology for implementing information security management in an organization. In its Annex A, it lists in summary form the objectives of control and controls developed by ISO 27002: 2013, to be selected by organizations in the development of their SGS and ISO 27005 which provides general guidelines for risk management in information security. It is compatible with the general concepts specified in ISO / IEC 27001 and is designed to assist in the successful application of information security based on a risk management approach.

As a result of this project, all the proposed objectives were achieved, as well as obtaining an overview of each of the information assets of the Entity's mission information systems, additionally, it was possible to identify the risks that affect them, the existing controls, as well as the application of the controls and their effectiveness, which served as part of the necessary input for the generation of the SIM action plan.



## Tabla de Contenido

**Key words:** Cybersecurity, cyber-attack, cybersecurity risks, risk analysis, threat, vulnerability

|  |    |
|--|----|
| 2. OBJETIVOS.....  | 6  |
| 2.1 Objetivo general.....  | 6  |
| 2.2 Objetivos específicos.....   | 6  |
| 3. PROBLEMA DE INVESTIGACIÓN.....  | 7  |
| 3.1 Pregunta de investigación.....   | 8  |
| 4. MARCO DE REFERENCIA.....  | 9  |
| 4.1.  Ciberseguridad.....  | 9  |
| 4.1.2 Ciberdefensa.....  | 9  |
| 4.1.3 Seguridad informática.....   | 10 |
| 4.1.4 Seguridad de la información.....   | 11 |
| 4.1.5 Riesgos de los sistemas de información.....  | 12 |
| 4.1.5.1 Conceptos, Enfoques Sobre Análisis y Gestión Distribida del Riesgo SI.....               | 17 |
| 4.1.5.2 Análisis de riesgos en sistemas de información.....                                      | 12 |
| 4.1.5.3 Análisis y gestión del riesgo de la información en los SI de una entidad del estado..... | 13 |
| 4.1.5.4 Plan de recuperación.....  | 14 |
| 4.2 Metodologías de análisis de riesgo para sistemas de información.....                         | 15 |
| 4.2.1 Metodología MAGRID.....  | 15 |

## Tabla de Contenido

|         |   |    |
|---------|---|----|
| 1.      | INTRODUCCIÓN .....  | 4  |
| 2.      | OBJETIVOS .....   | 6  |
| 2.1     | Objetivo general .....  | 6  |
| 2.2     | Objetivos específicos.....  | 6  |
| 3.      | PROBLEMA DE INVESTIGACIÓN .....   | 7  |
| 3.1     | Pregunta de investigación.....  | 8  |
| 4.      | MARCO DE REFERENCIA .....   | 9  |
| 4.1.    | Ciberseguridad.....   | 9  |
| 4.1.2   | Ciberdefensa.....   | 9  |
| 4.1.3   | Seguridad Informática.....  | 10 |
| 4.1.4   | Seguridad de la Información .....   | 11 |
| 4.1.5   | Riesgos en los sistemas de información.....   | 12 |
| 4.1.5.1 | Conceptos, Enfoques Sobre Análisis y Gestión Dinámica del Riesgo SI.....                  | 12 |
| 4.1.5.2 | Análisis de riesgos en sistemas de información.....                                       | 12 |
| 4.1.5.3 | Análisis y gestión del riesgo de la información en los SIM de una entidad del estado..... | 13 |
| 4.1.5.4 | Plan de acción .....  | 14 |
| 4.2     | Metodologías de análisis de riesgo para sistemas de información.....                      | 15 |
| 4.2.1   | Metodología MAGERIT .....   | 15 |



|   |    |
|---|----|
| 4.2.1.1. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método. ....   | 16 |
| 4.2.1.2 MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos.....                                   | 16 |
| 4.2.1.3 MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas.....                                       | 16 |
| MAGERIT sigue una serie de fases antes de llegar a la elaboración e identificación de todos los riesgos de una organización. El proceso que sigue se muestra la figura No 1 ..... | 17 |
| 4.2.2 Metodología OCTAVE .....  | 17 |
| 4.2.3 Metodología MEHARI.....   | 18 |
| 4.3 Familia ISO/IEC 27000 La familia ISO 27000 .....  | 20 |
| 4.3.1 Norma Técnica NTC-ISO/IEC COLOMBIANA 27005.....   | 20 |
| 4.3.2 Norma Técnica Colombiana NTC- ISO- IEC 27001 .....  | 21 |
| 4.3.3 Norma Técnica Colombiana NTC- ISO- IEC 27002.....   | 24 |
| 4.4 Guía de gestión de riesgo No 7, Ministerio de las TIC.....  | 24 |
| 5. MARCO CONTEXTUAL .....   | 26 |
| 5.1 Agencia Nacional del Espectro (ANE). ....   | 26 |
| 5.1.1 Misión y Visión de la Agencia Nacional del Espectro .....   | 26 |
| 5.1.2 Organigrama de la ANE.....  | 27 |
| 5.1.3 Infraestructura tecnológica de la ANE.....  | 27 |
| 5.1.4 Red de comunicaciones de la ANE.....  | 28 |

|            |  |    |
|------------|--|----|
| 5.1.4.1    | Arquitectura del centro de cómputo – ANE.....  | 29 |
| 5.1.4.2    | Sistemas de información de la ANE .....  | 29 |
| 6.         | METODOLOGÍA .....  | 33 |
| 7.         | PLAN DE ACCIÓN PARA PROTEGER EL SISTEMAS DE INFORMACIÓN PARA LA AGENCIA NACIONAL DEL ESPECTRO (ANE)..... | 37 |
| 7.1        | Soporte de Coordinación y autorización .....   | 37 |
| 7.2.       | Definición del Alcance.....  | 38 |
| 7.2.1.     | Histórico de Cambios de los Sistemas de Información Misionales .....                                     | 38 |
| 7.2.2.     | Alcance e identificación de los Sistemas de Información Misionales de la ANE .....                       | 39 |
| 7.3.       | Evaluación de la Metodología para los Sistemas de Información ANE .....                                  | 42 |
| 7.4.       | Identificación de los Activos de Información. ....   | 46 |
| 7.5        | Identificación de las Amenazas.....  | 46 |
| 7.5.1.     | Identificación de controles existentes .....   | 47 |
| 7.5.2.     | Identificación de Vulnerabilidades .....   | 48 |
| 7.5.2.1.   | Análisis de Vulnerabilidades.....  | 49 |
| 7.5.2.2.   | Clasificación de Vulnerabilidades.....   | 49 |
| 7.5.2.2.1  | Análisis de vulnerabilidades con Acunetix y Nessus.....  | 50 |
| 7.5.2.2.2. | Escaneo de Vulnerabilidades - Wave control – SMRNI con Acunetix y Nessus .....                           | 51 |



|  |    |
|--|----|
| 7.5.2.2.3. Escaneo de Vulnerabilidades - Simulación en Línea - SpectrumE ..... | 52 |
| 7.5.2.2.4. Clasificación Vulnerabilidades SIM Wave control – SMRNI.....        | 54 |
| 7. 5.2.3 Clasificación Vulnerabilidades Spectrum E.....                        | 56 |
| 7.6 Metodología de Análisis y Evaluación de Riesgos .....                      | 59 |
| 7.6.1. Análisis de riesgo a los SIM de la ANE.....                             | 60 |
| 7.7 Identificación de los Riesgos .....  | 60 |
| 7.7.1 Estimación del Riesgo.....   | 62 |
| 7.7.2 Evaluación del Riesgo.....   | 63 |
| 7.7.3 Control del Riesgo .....   | 64 |
| 7.7.4 Valoración del Riesgo. ....  | 66 |
| 7.7.5. Tratamiento del Riesgo. ....  | 67 |
| 7.7.6 Informe del Análisis de riesgo .....                                     | 68 |
| 7.7.6.1 Caracterización del Sistema de Información.....                        | 69 |
| 7.7.6.2 Medición del Riesgo .....  | 69 |
| 7.7.7 Criterios de Aceptación del Riesgo.....                                  | 70 |
| 7.8 Identificación de impactos. ....   | 70 |
| 7.8.1 Criterios de Impacto.....  | 71 |
| 7.9. Criterios de Probabilidad.....  | 71 |
| 7.9.1 Matriz de riesgo.....  | 72 |
| 7.10. Elaboración del plan de acción .....                                     | 72 |

|  |    |
|--|----|
| 7. 10.1 Plan de acción o tratamiento de riesgos residuales de los SIM de la ANE...   | 73 |
| 7.11 Monitoreo.....  | 78 |
| 8. Conclusiones y Recomendaciones.....   | 79 |
| 9. REFERENCIAS BIBLIOGRÁFICAS.....   | 82 |
| Tabla 1. Resultados de la norma ISO 27001:2013                                       |    |
| Tabla 2. Sistema de Información ANE  |    |
| Tabla 3. Historial de cambios - Wave control   | 31 |
| Tabla 4. Historial de cambios - Spectrum E   | 39 |
| Tabla 5. Sistema de Información Misionales ANE                                       | 40 |
| Tabla 6. Sistema de Información Misionales ANE                                       | 41 |
| Tabla 7. Clasificación de activos de información                                     | 46 |
| Tabla 8. Resultados análisis de vulnerabilidades SIM                                 | 50 |
| Tabla 9. Identificación de vulnerabilidades SIM Wave control - SMRSI                 | 54 |
| Tabla 10. Clasificación Vulnerabilidades Spectrum E                                  | 56 |
| Tabla 11. Mapa de riesgo inherente   | 63 |
| Tabla 12. Mapa de riesgo residual  | 64 |
| Tabla 13. Nivel de exposición o severidad del riesgo                                 | 67 |
| Tabla 14. Criterios para la evaluación de controles                                  | 68 |
| Tabla 15. Políticas de administración o tratamiento del riesgo                       | 70 |
| Tabla 16. Impactos por materialización de amenazas                                   | 71 |
| Tabla 17. Probabilidad de materialización de sus amenazas                            | 72 |
| Tabla 18. Riesgos residuales identificados   | 73 |
| Tabla 19. Plan de acción o tratamiento de riesgos residuales de los SIM de la ANE... | 74 |



## LISTA DE TABLAS

|  |    |
|--|----|
| Tabla 1. Requisitos de la norma ISO-IEC 27001:2013. ....                               | 22 |
| Tabla 2. Sistemas de Información ANE.....  | 30 |
| Tabla 3. Historial de cambios-Wavecontrol.....   | 39 |
| Tabla 4. Historial de cambios SpectrumE.....   | 39 |
| Tabla 5. Sistema de Información Misionales ANE.....                                    | 40 |
| Tabla 6. Sistema de Información Misional ANE.....                                      | 41 |
| Tabla 7. Clasificación de activos de información .....                                 | 46 |
| Tabla 8. Resultados análisis de vulnerabilidades SIM.....                              | 50 |
| Tabla 9. Identificación de vulnerabilidades SIM Wave control – SMRNI.....              | 54 |
| Tabla 10. Clasificación Vulnerabilidades Spectrum E.....                               | 56 |
| Tabla 11. Mapa de riesgo inherente .....   | 63 |
| Tabla 12. Mapa de riesgo residual .....  | 64 |
| Tabla 13. Nivel de exposición o severidad del riesgo.....                              | 67 |
| Tabla 14. Criterios para la evaluación de controles .....                              | 68 |
| Tabla 15. Política de administración o tratamiento del riesgo .....                    | 70 |
| Tabla 16. Impactos por materialización de amenazas:.....                               | 71 |
| Tabla 17. Probabilidad de materialización de una amenaza .....                         | 72 |
| Tabla 18. Riesgos residuales identificados .....                                       | 73 |
| Tabla 19. Plan de acción o tratamiento de riesgos residuales de los SIM de la ANE..... | 74 |

**LISTA DE FIGURAS**

|   |    |
|---|----|
| Figura 1. Proceso de Análisis y evaluación de riesgos. ....                   | 15 |
| Figura 2. Organigrama de la ANE .....   | 27 |
| Figura 3. Diagrama de red LAN - ANE.....                                      | 28 |
| Figura 4. Diagrama LAN extendida ANE.....                                     | 29 |
| Figura 5. Arquitectura del centro de computo .....                            | 29 |
| Figura 6. Soporte de autorización .....                                       | 37 |
| Figura 7. Resumen porcentual de vulnerabilidades sobre los SIM de la ANE..... | 51 |
| Figura 8. Distribución de alertas internas con acunetix .....                 | 51 |
| Figura 9. Alertas internas con nessus .....                                   | 52 |
| Figura 10. Distribución de alertas externas acunetix .....                    | 52 |
| Figura 11. Alertas externa con nessus.....                                    | 52 |
| Figura 12. Distribución de alertas internas .....                             | 53 |
| Figura 13. Alertas internas con nessus.....                                   | 53 |
| Figura 14. Distribución de alertas externas acunetix .....                    | 53 |
| Figura 15. Alertas externas nessus .....                                      | 53 |
| Figura 16. Total, Vulnerabilidades red interna y externa.....                 | 54 |



### LISTA DE CUADROS

Cuadro 1. Matriz de Selección..... 43

## 1. INTRODUCCIÓN

El uso de las Tecnologías de Información y de las Comunicaciones (TIC'S) ha ganado protagonismo día a día en las actividades cotidianas, esto debido a que ha permitido el desarrollo de las organizaciones, bien sea grandes, pequeñas, públicas o privada, ya que les permite un mejor manejo de la información facilitando las operaciones internas e incentivando el crecimiento de las organizaciones. Sin embargo, el uso de las TIC'S dentro de las organizaciones también ha generado riesgos en cuanto a la seguridad de los datos resguardados.

Con el avance constante de las TIC'S las organizaciones van acumulando grandes volúmenes de información necesaria para la realización de las distintas operaciones internas, empleando entonces Sistemas de Información, donde todos los empleados tengan acceso de forma inmediata a la información necesaria para desarrollar su labor.

En términos de seguridad de información los riesgos más relevantes son: mala manipulación, accesos no autorizados, pérdida de la información, lo que puede ocasionar inconvenientes dentro de la organización afectando de manera significativa las operaciones internas.

Los Sistemas de Gestión de Seguridad (SIG) les permiten a las empresas mantener un control de la información compartida en sus sistemas de información, estos deben estar regidos bajo la normativa internacional ISO/IEC 27001 que establece las guías, procedimientos y procesos para gestionarla apropiadamente mediante un proceso de mejoramiento continuo.

De acuerdo a una encuesta realizada por la compañía de seguridad informática ESET-Latinoamérica en el año 2017 arrojó que el número de atacantes de las redes y de los sistemas de información en las organizaciones es cada vez mayor, siendo la amenaza que produce mayor preocupación dentro de las organizaciones la denominada "Ransomware" con un 57%, seguida por el robo de información con un 51% y la infección de los sistemas de información con código malicioso con un 45%.

Sin embargo, a la hora de hablar de incidentes de seguridad en las empresas, encontramos que por lo menos una de cada diez empresas encuestadas dijo haber sido víctima de incidentes que afectaron la disponibilidad de servicios críticos (10%) o de un acceso indebido a aplicaciones o bases datos (11%). Adicionalmente, en los últimos años, los porcentajes de empresas que dijeron ser víctimas de ataques de ingeniería social se han mantenido estables, con pequeñas diferencias a lo largo de 2017.



La Agencia Nacional del Espectro (ANE), es una Entidad del Estado Colombiano que se encarga de planear estratégicamente el uso del espectro radioeléctrico, así como su vigilancia y control en todo el territorio nacional, actualmente la ANE se encuentra en crecimiento lo que hace necesario involucrar en sus procesos internos el uso de buenas prácticas orientadas al resguardo y protección de la información.

Como cualquier organización que emplea el uso de las TIC'S para el desempeño de sus procesos internos, la ANE no está exenta a presentar ataques cibernéticos hacia sus sistemas de información, ocasionando problemas que afectan el normal funcionamiento de la organización.

Así mismo, estos ataques traen como consecuencia grietas de seguridad en los sistemas e infraestructura tecnológica que accidentalmente pueden ser utilizados por personas no autorizadas, afectando las operaciones internas de la entidad.

El manejo inadecuado de la información ocasiona una falla en la seguridad de la misma, bien sea por no tener el conocimiento básico de la información o de las aplicaciones que manejan dentro de la ANE diariamente; siendo la mayor consecuencia la pérdida de información valiosa tanto del usuario como de la entidad, así como también, retrasos en las actividades a desarrollar, uso incorrecto de los activos de información y cómputo, entre otras fallas que afecten el correcto desenvolvimiento de las actividades que pueden causar daños permanentes o temporales a la entidad.

Por consiguiente, aunque es un problema al que se enfrenta continuamente, los encargados de la seguridad del sistema de información misionales representan una preocupación para la ANE ya que pone en riesgo la integridad del sistema de información, así como también ponen en duda el rendimiento del mismo.

En este sentido y tomando en cuenta lo explicado anteriormente, la entidad decidió diagnosticar los factores de riesgos que amenazan con la integridad de los sistemas de información misionales, con el fin de conocer si se encuentran protegido contra amenazas y tomando en cuenta los controles adecuados y normalizados dentro de las políticas de seguridad informática, así como también facilitar el monitoreo continuo mediante procesos de auditorías y mejoras continuas.

De la situación planteada, se desprende el siguiente interrogante: ¿Cuáles serían los controles de seguridad informática adecuados a implementar en los sistemas de información misionales de la Agencia Nacional del Espectro (ANE) para mitigar el riesgo de ataques cibernéticos?

## 2. OBJETIVOS

### 2.1 Objetivo general

Desarrollar un plan de acción a través de estrategias de seguridad informática para la Agencia Nacional del Espectro (ANE) que permita proteger los Sistemas de Información Misionales de ciberataques.

### 2.2 Objetivos específicos

- Evaluar metodologías de estrategias de seguridad y riesgos informáticos con el propósito de establecer la más idónea para los sistemas de información misionales de la Agencia Nacional del Espectro (ANE).
- Determinar el estado actual de los sistemas de información misionales de la Agencia Nacional del Espectro (ANE), con el fin de conocer las políticas de seguridad informática de los mismos.
- Aplicar la metodología definida a los sistemas de información misionales de la Agencia Nacional del Espectro – ANE



### 3. PROBLEMA DE INVESTIGACIÓN

Las Tecnologías de Información (TIC'S) debido al gran auge que tienen hoy en día se han vuelto blanco de los ataques cibernéticos afectando al correcto desenvolvimiento de las diversas funciones de las organizaciones, estos ataques han generado gran preocupación para los responsables y proveedores de las TIC'S, razón por la cual tanto los gobiernos de los países como las instituciones públicas y privadas se ven obligados a resguardar sus sistemas de información.

Hechos como el ataque cibernético a la república de Estonia ocurrido en el año 2007 el cual afecto a sus sistemas de información ocasionando bloqueo de sus plataformas gubernamentales, militares y económicos, o el hecho cometido en el año 2009 al departamento de defensa de la casa blanca en donde se revelo información del desvió monitoreado del porta aviones más poderoso de la armada norteamericana: "Ronald Reagan" y los ataques a las centrifugadoras nucleares Iraníes por parte del ejército Israelí; con su potente "FLAME"<sup>1</sup>, motivan a los gobiernos a resguardar sus sistemas de información. El gobierno colombiano no escapa de esta realidad, dentro del mismo se proyectan escenarios de defensa y respuesta ante la presencia de ataques cibernéticos a sus sistemas de información, para esto emplean modelos que plantean acciones cibernéticas maliciosas a fin evaluar los riesgos potenciales en la seguridad y evitar la pérdida de información.

La investigación se desarrolló dentro de la Agencia Nacional del Espectro (ANE), entidad perteneciente al Estado Colombiano que se encarga de realizar la planeación, atribución, vigilancia y control del Espectro Radioeléctrico dentro del territorio nacional, así como también de ofrecer asesoría técnica para la gestión eficiente del espectro y fomentar su conocimiento. La ANE se encuentra adscrita al Ministerio de la Información y la Comunicación (MINTIC).

La Agencia Nacional del Espectro (ANE), actualmente ha venido presentando problemas dentro de sus sistemas de información misionales producto de ataques cibernéticos que han comprometido el normal funcionamiento de la Entidad afectando el cumplimiento de los objetivos de la ANE, así como también causando impacto en la sociedad en general ya que dichos ataques también afectan los principios de disponibilidad, integridad y confidencialidad de la información almacenada en los sistemas de información misionales.

---

<sup>1</sup> Solución informática implementada por el ejército israelí para vulnerar las instalaciones iraníes. Disponible en: [https://es.wikipedia.org/wiki/Flame\\_\(malware\)](https://es.wikipedia.org/wiki/Flame_(malware))



De igual manera, el manejo inadecuado de la información almacenada en los sistemas de información misionales genera fallas en la seguridad, esto puede ser causado por no poseer el conocimiento básico del manejo de la información o de las aplicaciones empleadas dentro de la ANE, siendo la mayor consecuencia la pérdida de información de gran importancia tanto del usuario como de la entidad, retrasos en las actividades que se desarrollan, uso incorrecto de los activos de información y cómputo, poniendo en riesgo el correcto desenvolvimiento de sus actividades.

Con el propósito de mitigar los ataques cibernéticos anteriormente mencionados se propone el desarrollo de un plan de acción basado en estrategias de seguridad informática, sustentadas por la normativa internacional ISO/IEC 27001:2013, los cuales se aprecian en el anexo A, en donde se enlistan los objetivos de control propuestos por la norma, así como también se aprecian los puntos necesarios para que las organizaciones implemente sus SGS de acuerdo a lo planteado por ISO 27005 para el control de riesgos en la seguridad de la información; que permitan detectar los riesgos asociados a ataques cibernéticos con el fin de estimar los más adecuados para los sistemas de información misionales de la ANE y de esta manera se implementen.

**Key Word:** Ciberseguridad, ataque cibernético, riesgos de ciberseguridad, análisis de riesgo, amenaza, vulnerabilidad.

### 3.1 Pregunta de investigación

¿Cuáles serían los controles de seguridad informática adecuados a implementar en los sistemas de información misionales de la Agencia Nacional del Espectro (ANE) para mitigar el riesgo de ataques cibernéticos?

## 4. MARCO DE REFERENCIA

### 4.1. Ciberseguridad

El ciberespacio lo podemos interpretar como un entorno virtual no físico, el cual está conformado por computadores que unidos entre sí se pueden comunicar y que a través de él los operadores de estos computadores pueden interactuar de manera similar con el mundo real, como es enviar correos, realizar video llamadas, conectarse con sus amigos por redes sociales, realizar compras, entre otros.

Pero a través este ciberespacio se pueden cometer infinidad de ataques cibernéticos sobre todo a los sistemas de información y si no se toman las medidas necesarias con el fin de contrarrestarlos, es decir no se implementa la ciberseguridad en estos sistemas, la información contenida en ellos se podría ver afectada, vulnerando los principios de la información como son su integridad, disponibilidad y confiabilidad.

Según el autor define la ciberseguridad como:

La práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término es amplio y se aplica a numerosos elementos, desde seguridad informática hasta recuperación ante desastres y educación del usuario final (Karpesky, s.f.).

De igual forma la UIT ha definido la ciberseguridad como “el conjunto de políticas y acciones que se dirijan con el fin de proteger activos de una organización, y a la comunidad en general en el ciberespacio”. (UIT, s.f.) .

#### 4.1.2 Ciberdefensa

Debido a la creciente dependencia del ciberespacio, la seguridad de su infraestructura, componentes lógicos y las interacciones humanas que allí tienen lugar se ha constituido en una de las más importantes preocupaciones contemporáneas, y la gestión de dichos riesgos una prioridad a nivel global.



Infraestructuras críticas como los servicios básicos, transportes y diversas industrias como la financiera y del transporte, entre muchas otras, incluidas la administración del Estado y la Defensa Nacional, son susceptibles de ser atacadas en el ciberespacio, pudiendo amenazar la estabilidad, seguridad y soberanía de los países de múltiples formas.

Según el Conpes 3701, considera al ciberespacio como:

El ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Social, 2011, pág. 38).

#### 4.1.3 Seguridad Informática

Como afirma Ossa (2017) la seguridad informática se relaciona directamente con la seguridad de la información<sup>2</sup>. La seguridad informática se define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden obtener daños en la información, comprender su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (pág. 11)

La seguridad informática también abarca en asegurar los recursos del sistema de información de una organización, siendo que el acceso a la información sea posible a las personas que estén autorizadas y que se encuentren acreditadas. También se puede decir que es la disciplina de proteger y resguardar la información gestionada, administrada y operada en los dispositivos los cuales son: estaciones de trabajo, portátiles, PDA's y equipos de comunicación.

---

<sup>2</sup> Concepto de Seguridad Informática, Empresa Yumbo ESPY. Disponible en Internet: [http://www.espyumbo.com/portalespy/index.php?option=com\\_content&view=article&id=78:seg](http://www.espyumbo.com/portalespy/index.php?option=com_content&view=article&id=78:seg)

#### 4.1.4 Seguridad de la Información

Según el autor, define la seguridad de la información como:

Un estado específico de la misma sin importar su formato, que nos indica un nivel o un determinado grado de seguridad de información, por ejemplo, que está libre de peligro, daño o riesgo, o por el contrario que es vulnerable y puede ser objeto de materialización de una amenaza. Las vulnerabilidades, el peligro o el daño de esta es todo aquello que pueda afectar su funcionamiento directo y la esencia en sí de la información, o en su defecto los resultados que se obtienen de la consulta, administración o procesamiento de ella. (John Jairo Parafán, 2014, pág. 19)

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información mediante el establecimiento de un conjunto coherente de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan atentar contra la seguridad de la organización y la continuidad del negocio.

La ISO 27001 (2013) define la Seguridad de la Información como “La preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad” (pág. 3).

La información representa uno de los activos más valioso de las organizaciones, lo que implica que es indispensable asegurar su protección contra amenazas y eventos que puedan llegar comprometer su confidencialidad, integridad y disponibilidad. La información puede existir en diferentes medios tanto físicos como electrónicos, pero independientemente del medio, es necesario que las organizaciones garanticen y aseguren la debida protección de esta durante su recolección, almacenamiento, tratamiento y uso.

La seguridad de la información dentro de las organizaciones depende del nivel de protección y seguridad de sus activos de información, por lo tanto, es fundamental la implementación de medidas y controles de seguridad adecuados, y el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad.



#### **4.1.5 Riesgos en los sistemas de información.**

La información es uno de los elementos o activo más importantes que pueda tener una Entidad, por esta razón siempre es importante cuidar de esa información aplicando varios mecanismos de protección. La mayoría de esa información que tienen las Entidades públicas o privadas se encuentran almacenadas ya sea en carpetas, archivo, bases de datos, sistemas de información y otra en físico, pero hoy en día esa información siempre va a estar expuesta a muchos riesgos que puedan afectar la integridad, disponibilidad e integridad de esta.

Para mitigar o reducir los riesgos a los cuales se encuentra expuesta la información las Entidades deberán identificar, gestionar y darles el mejor tratamiento a esos riesgos con el fin de evitar su pérdida o alteración.

##### **4.1.5.1 Conceptos, Enfoques Sobre Análisis y Gestión Dinámica del Riesgo SI.**

Según (David Lopez, 2011) la aplicación de procesos de Análisis y Gestión de Riesgos en el ámbito de los Sistemas de Información es una práctica común que permite la planificación en un momento puntual de tiempo de las acciones preventivas frente al riesgo a corto, medio o largo plazo, pero con un considerable potencial actualmente desaprovechado, para facilitar la toma de decisiones en tiempo real frente a eventos o incidentes de seguridad.

La investigación hace un recorrido por las principales corrientes que buscan sacar partido a este potencial, englobadas principalmente bajo el concepto de Análisis de Riesgos Dinámico, que se permiten evidenciar ante las múltiples variaciones presentes en los sistemas de información misional de la agencia nacional del Espectro ANE, teniendo en cuenta períodos de tiempo que fueron realizados a partir de una retroalimentación continua de los datos, registrados en el historial de cambios de la entidad, cuyo principio es la actualización incesante de los parámetros que intervienen en el cálculo del riesgo para la optimización de su tratamiento posterior. Finalmente, se proponen las posibles tendencias futuras para la mejora en este ámbito.

##### **4.1.5.2 Análisis de riesgos en sistemas de información.**

Según el autor un ataque a un activo puede propagarse a través de la red y amenazar los activos más valiosos de una organización. Es necesario valorar todos los activos, las dependencias directas e indirectas de los activos, así como la probabilidad de amenazas y la consiguiente



degradación de los activos, sin embargo, los expertos encargados de asignar tales valores a menudo proporcionan sólo información vaga e incierta. La lógica difusa puede ser muy útil en tal situación, pero no está exenta de algunas dificultades, como la necesidad de una aritmética adecuada para el modelo considerado o el establecimiento de medidas de similitud apropiadas. (E. Vicente, 2013)

La anterior conferencia nos habla de que el ataque a un activo de una organización se puede propagar a todos los activos relacionados con el activo que se atacó siempre y cuando se encuentren conectados a una red, de igual forma nos habla de la necesidad de valorar todos y las dependencias directas e indirectas de ese activo, también de la probabilidad de las amenazas, dado que vienen siendo los principales involucrados en los riesgos de los SI, pero que sin embargo los expertos encargados de asignar estos valores y detectar las posibles amenazas a los SI proporcionan información vaga e incierta, lo cual constituye un riesgo para el análisis del riesgo de la información.

#### **4.1.5.3 Análisis y gestión del riesgo de la información en los SIM de una entidad del estado.**

En esta tesis el autor efectúa un análisis del riesgo trabajado con la metodología MAGERIT a una entidad del gobierno que no se nombra por motivos de seguridad para la Entidad, en donde se efectúa la valoración de los activos de información, la valoración de las amenazas que pueden afectar los activos, se realiza un análisis de salvaguardas y se realiza el análisis del riesgo efectivo.

Para hacer la valoración de las amenazas se utilizó como fuente de información las entrevistas que se realizaron a los administradores de la seguridad en la Entidad, los resultados del estudio de Ethical Hacking y los resultados de unas encuestas realizadas a todos los funcionarios con la finalidad de evaluar el buen uso de las tecnologías de información. Este análisis del riesgo dio como resultado: El riesgo efectivo en el que se encuentra la Entidad y también una propuesta de controles y recomendaciones con el objetivo de reducir los riesgos analizados y aumentar la fiabilidad, integridad y disponibilidad de la información. (ROBLES, 2015)

De igual forma en esta tesis se muestra la valorización de los activos que tiene la Entidad relacionados con los Sistema de Información Misional y se hace un estimado del impacto que causan en la empresa su daño o pérdida, así mismo nos muestra un estudio de los riesgos asociados a esos sistemas y a su entorno, como también nos lista las amenazas existentes sobre cada uno de los activos estudiados, permitiendo realizar la valoración del riesgo y haciendo una recomendación



de las medidas necesarias y la selección de controles para conocer, prevenir, impedir, reducir o controlar los riesgos estudiados.

También nos muestra la metodología que utilizaron los autores para poder llevar a cabo el desarrollo de este proyecto, como fue la “Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información de las Administraciones Públicas (MAGERIT), dado que es una metodología que está dirigida o enfocada a los medios electrónicos, informáticos y telemáticos y nos permite investigar los riesgos a los cuales se encuentran expuestos los Sistemas de Información, de igual forma nos permite realizar una serie de recomendaciones apropiadas que se deben adoptar para controlar o minimizar los riesgos asociados a los Sistemas de Información.

#### **4.1.5.4 Plan de acción**

Según Suarez (2002) los planes de acción son “documentos debidamente estructurados que forman parte del planeamiento estratégico de una investigación de carácter cualitativo, se busca materializar los objetivos estratégicos previamente establecidos, dotándose de un elemento cuantitativo y verificable a lo largo del proyecto” (Suarez 2002. p 20).

El plan de acción es un instrumento gerencial de programación y control de la ejecución anual de los proyectos y actividades que deben llevar a cabo las dependencias para dar cumplimiento a las estrategias y proyectos establecidos en el plan estratégico.

De igual manera, compromete el trabajo de una gran parte de los participantes e investigadores, estableciendo plazos y responsables y un sistema de seguimiento y monitoreo de todas las acciones diseñadas.

En general, los planes se estructuran principalmente mediante actividades estratégicas, sin embargo, el plan debe contener también, el desarrollo de las tareas específicas. La formulación de un plan de acción que priorice las iniciativas más relevantes para cumplir con los objetivos y métodos de gestión requiere estructurar adecuadamente su esquema de desarrollo y el enlace con los objetivos de la investigación.

Dichos planes son analizados a partir de la implementación del diseño de un control de riesgos identificados en los activos de los sistemas de información misionales de la entidad, que tienen en cuenta la asignación de responsabilidades según las dependencias adecuadas a sus necesidades y metas.



## 4.2 Metodologías de análisis de riesgo para sistemas de información.

Las metodologías para el análisis de riesgo a los sistemas de información permiten a las organizaciones identificar y gestionar los riesgos de tecnología de la información y tomar buenas decisiones de negocio, en lugar de invertir en controles y protección sin una comprensión clara de lo que se está realizando.

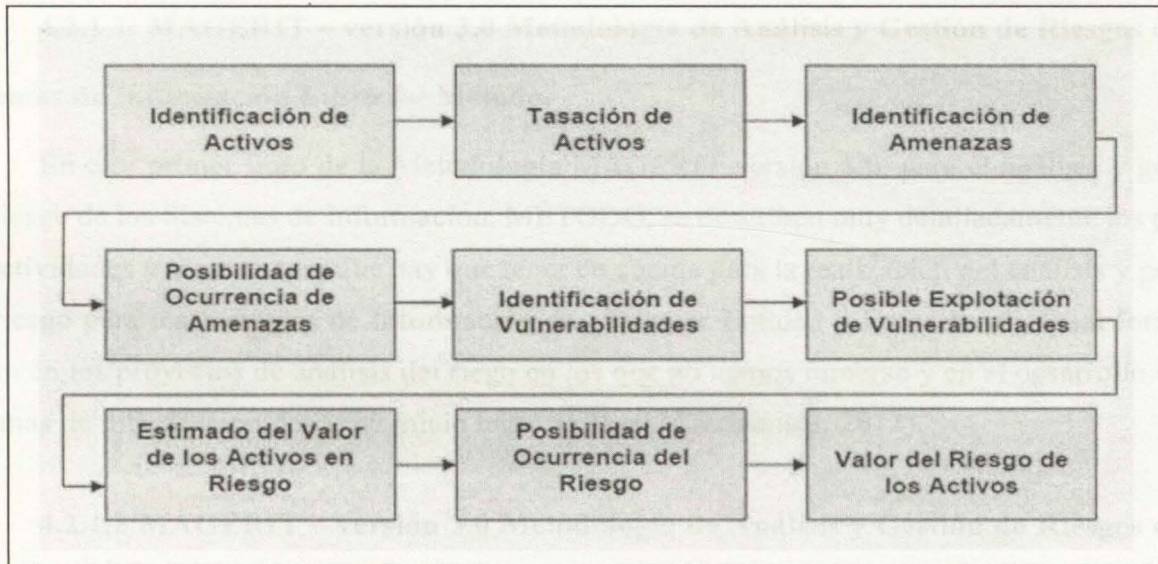


Figura 1. Proceso de Análisis y evaluación de riesgos. Fuente [www.centrum.pucp.edu.pe](http://www.centrum.pucp.edu.pe)

### 4.2.1 Metodología MAGERIT

Metodología de carácter público, pertenece al Ministerio de Administraciones Públicas de España.

Está dirigido a los medios electrónicos, informáticos y telemáticos, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que se deberían adaptar para el control de esos riesgos.

Permite un análisis completo tanto cualitativo como cuantitativo, posee un extenso archivo de inventarios, se le considera con un alcance completo tanto para el análisis como para la gestión del riesgo.

Es una metodología de análisis y gestión de riesgos de TI desarrollado por el Consejo Superior de Administración Electrónica y publicado por el Ministerio de Administraciones Públicas español, es un tipo de metodología que es una guía de referencia para realizar procesos



de análisis de riesgos al igual que provee lineamientos para la gestión de riesgos en sistemas informáticos y todos los aspectos que giran alrededor de ellos en las organizaciones para lograr muchas de las metas planteadas al interior de las mismas y buscando cumplir las políticas de buen gobierno, En la actualidad esta metodología se encuentra en la versión 3.0, publicada en el año 2005 y está compuesta por 3 libros como son:

#### **4.2.1.1. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método.**

En este primer libro de la Metodología MAGERIT versión 3.0, para el análisis y gestión del riesgo de los Sistemas de Información, MÉTODO, se describen muy detalladamente los pasos, las actividades y la estructura que hay que tener en cuenta para la realización del análisis y gestión del riesgo para los Sistemas de Información de cualquier Entidad o Empresa, de igual forma se centra en los proyectos de análisis del riesgo en los que no vemos inmerso y en el desarrollo de los sistemas de información desde su inicio hasta su final (Electronica, 2012).

#### **4.2.1.2 MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos.**

En este segundo libro de la Metodología MAGERIT versión 3.0, para el análisis y gestión del riesgo de los Sistemas de Información, CATALOGO DE ELEMENTOS, habla sobre una especie de inventario que puede utilizar cualquier empresa para enfocar su análisis de riesgo, de igual forma contiene una división de los activos de información que deben considerarse, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta para la realización del análisis y gestión del riesgo de los sistemas de información (Electrónica, 2012).

#### **4.2.1.3 MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas.**

En este tercer libro de la Metodología MAGERIT versión 3.0, para el análisis y gestión del riesgo de los Sistemas de Información, GUÍA DE TÉCNICAS, se describen diferentes técnicas



frecuentemente utilizadas en el análisis de riesgos y contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos de los sistemas de información (Electrónica, 2012).

Los objetivos principales de esta metodología son los siguientes:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y las comunicaciones.
- Ayudar a describir y planificar el tratamiento oportuno para mantener los riesgos bajo control
- Prepara a la organización para procesos de evaluación, auditoría, certificación.

Las principales desventajas de esta metodología es que su aplicación es realmente costosa debido a que se traducen todas las valoraciones a valores, de igual forma no involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir.

MAGERIT sigue una serie de fases antes de llegar a la elaboración e identificación de todos los riesgos de una organización. El proceso que sigue se muestra la figura No 1

#### 4.2.2 Metodología OCTAVE

Según describe el autor en el periódico el universo, el periódico de los universitarios, que Octave es:

Una metodología para el análisis de riesgos de TI. Se centra en el estudio de riesgos organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas). (Carmona, 2013, pág. 1)

Este periódico nos menciona que la metodología octave se centra en el estudio de riesgos organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas, de igual forma nos muestra que esta metodología estudia la infraestructura de información y más



importante aún, la manera como dicha infraestructura se usa y contempla para su implementación la conformación de un equipo mixto, compuesto de personas de las áreas de negocios y de TI.

Es una metodología de evaluación y gestión de los riesgos que garantiza la seguridad de los sistemas de información y que tiene como objetivo facilitar la gestión del riesgo en una organización. El estudio de riesgos organizacionales es su principal objetivo, la evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas).

Para su implementación involucra la conformación de un equipo mixto, compuesto de personas de diferentes áreas y de TI. Estudia o analiza la infraestructura de información, al igual que la manera como dicha infraestructura es usada en las empresas, con el fin de que una organización pueda cumplir sus objetivos trazados, los empleados de todos los niveles necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos y además identifica oportunamente riesgos importantes.

Presenta algunas desventajas como la no explicación en forma clara la definición y determinación de los activos de información, de igual forma se requiere tener conocimientos técnicos para su implementación y no tiene mucha compatibilidad con otras normas o estándares

El proceso de evaluación contemplado se divide en tres fases:

- Construcción de perfiles de amenazas basadas en activos.
- Identificación de vulnerabilidades en la infraestructura.
- Desarrollo de estrategias y planes de seguridad.

#### **4.2.3 Metodología MEHARI.**

Para el autor Mehari es un método armonizado de Análisis de Riesgos. Esta metodología fue propuesta y desarrollada por el Club Francés de la Seguridad de la Información CLUSIF en el año 1996; es de acceso público y para todo tipo de organizaciones. Se diseñó inicialmente y se actualiza continuamente para ayudar a los CISO (Chief Información Security Officers) en la



gestión de las actividades de la seguridad informática, pero también está concebida para auditores CIO o gestores de riesgos. Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo, evaluando cuantitativamente, de acuerdo con la situación de la organización, dónde se requiere el análisis. Castellanos 2014 p. 76.

Para las autoras de este artículo las diversas metodologías que se pueden aplicar para la seguridad de la información son diversas, cuyo principal objetivo son proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a las recomendaciones expuestas en la normas ISO/IEC 27005:2008<sup>3</sup>, y lo más importante es poder realizar una selección óptima teniendo en cuenta un análisis comparativo de las diferentes metodologías que exponen en donde se pueden ver sus ventajas y desventajas en cada una de ellas. (Alemán N., H 2015)

El principal objetivo es proporcionar un método para la evaluación y gestión de riesgos, teniendo en cuenta un conjunto de herramientas y elementos necesarios para su implementación, que permitan un análisis directo e individual de situaciones de riesgos descritas en los escenarios y un conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, mediano y largo plazo, así mismo se adapta a diferentes niveles de madurez y tipos de acciones.

Usa un modelo de análisis de riesgo cualitativo y cuantitativo, tiene la capacidad de evaluar y simular los niveles de riesgo derivados de medidas adicionales.

Las fases del desarrollo de la seguridad deben ser consistentes y cada resultado obtenido en una fase, debe poder ser reutilizado por otras herramientas o en otro lugar de la organización.

Al igual que las otras metodologías también tiene sus desventajas como es la estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos, de igual forma sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio.

---

<sup>3</sup> Directrices para la gestión del riesgo de seguridad de la información.



### **4.3 Familia ISO/IEC 27000 La familia ISO 27000**

Son un conjunto de normas, estándares, guías e informes técnicos desarrollados por la ISO (International Organization for Standardization) y por la IEC (International Electrotechnical Commission) que fueron creadas para facilitar la implantación de Sistemas de Gestión de Seguridad de la Información en las organizaciones y que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

- En 1999 se revisaron ambas normas BS 7799. En el año 2000 ISO adoptó, sin grandes cambios, la BS 7799-1 y la llamó ISO/IEC 17799.
- En 2002 se revisó la BS 7799-2 para adecuarse a la filosofía ISO de sistemas de gestión.
- En 2005, ISO publicó como estándar la ISO/IEC 27001, basada en la norma BS 7799-2. También se revisó y actualizó la ISO/IEC 17799.
- En el año 2007 la norma ISO/IEC 17799 pasó a denominarse ISO/IEC 27002:2005. En este año también se publicó la ISO/IEC 27006:2007.
- En 2008 se publicó la ISO/IEC 27005:2008.
- En 2009 se publicaron las ISO/IEC 27000:2009 y la ISO/IEC 27004:2009.
- En 2010 se publicó la ISO/IEC 27003.
- En 2013 se publican las nuevas versiones de las ISO/IEC 27001 e ISO/IEC 27002. (Iso27000, s.f.)

#### **4.3.1 Norma Técnica NTC-ISO/IEC COLOMBIANA 27005.**

Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información, de igual forma apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información, se integra perfectamente con otras metodologías de análisis de riesgo.

Permite identificar las necesidades de las organizaciones sobre los requisitos de seguridad de la información, sirve de base para crear el SGSI en las Entidades, Aborda los riesgos de manera eficaz y oportuna, donde y cuando es necesario.

Según el autor, esta norma:



Proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma NTC-ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial. Se puede utilizar una variedad de metodologías existentes bajo la estructura descrita en esta norma para implementar los requisitos de un sistema de gestión de seguridad de la información. Esta norma es pertinente para los directores y el personal involucrado en la gestión del riesgo en la seguridad de la información dentro de una organización y, cuando corresponda, para las partes externas que dan soporte a dichas actividades. (Espinosa, J. 2016)

Esta norma no facilita una metodología concreta para la realización del análisis de riesgos, sino que describe concretamente en cláusulas el proceso que se recomienda seguir para analizar el riesgo, en las cuales se incluyen las fases que lo conforman, además nos sirve para no tener dudas sobre los diferentes elementos que debe incluir toda la metodología de análisis de riesgos, por lo que si lo vemos desde este punto de vista se puede constituir como una metodología en sí misma.

Presenta algunas desventajas como la de no detallar la forma de valorar las amenazas, no es certificable, no posee herramientas, técnicas, ni comparativas de ayuda para su implementación, no recomienda una metodología concreta.

#### **4.3.2 Norma Técnica Colombiana NTC- ISO- IEC 27001**

La revisión de esta norma se dio el 25 de septiembre de 2013 y su publicación se dio el 15 de octubre del año 2005, contiene los requisitos del sistema de gestión de seguridad de la información, se basó en la norma BS 7799-2:2002, la cual ya fue anulada y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones, en el Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002.



Tabla 1. Requisitos de la norma ISO-IEC 27001:2013.

|                                    |   |
|------------------------------------|---|
| <b>CONTEXTO DE LA ORGANIZACIÓN</b> | La organización debe estar consciente de las cuestiones internas y externas que podrían influir en los resultados deseados de la seguridad de la información, así como determinar su alcance, límites y capacidad, garantizando que el SGSI cumpla los requerimientos de la norma.  |
| <b>LIDERAZGO</b>                   | La alta gerencia de la organización debe liderar el proceso del SGSI verificando que se cumplan los requerimientos de la norma, garantizando los recursos, documentando las políticas y objetivos de seguridad propuestos, asignando las responsabilidades para cada una de las actividades y promoviendo el mejoramiento continuo.   |
| <b>PLANIFICACIÓN</b>               | La organización debe escoger una metodología de clasificación, análisis y evaluación de riesgos, formando criterios para establecer los controles de seguridad y así mantener los niveles de riesgo a un nivel aceptable de acuerdo a las políticas y objetivos de seguridad.   |
| <b>SOPORTE</b>                     | La organización debe velar por comunicar las políticas de seguridad de la información a sus empleados y que éstos se comprometan al mejoramiento continuo del SGSI. A su vez, también se deben garantizar los recursos y la cualificación de las personas para llevar a cabo cada actividad. También se deben generar los documentos que exige la norma y que éstos tengan su nivel de clasificación. |
| <b>OPERACIÓN</b>                   | La organización debe documentar y planear los procesos para llevar a cabo las actividades, incluyendo las valoraciones de riesgos de la seguridad de la información y el plan de tratamiento de riesgos.  |
| <b>EVALUACIÓN DEL DESEMPEÑO</b>    | La organización debe velar el desempeño de la seguridad de la información y medir la eficacia del SGSI, mediante auditorías internas a intervalos planificados, con el fin de verificar si se están cumpliendo con los objetivos y políticas de seguridad, así como con la norma.   |
| <b>MEJORA</b>                      | La organización debe aplicar las acciones correctivas y promover un mejoramiento continuo.  |

**Fuente:** NTC-ISO-IEC 27001. Requisitos. Bogotá: ICONTEC. 2013. p. 9.

Según los objetivos y campos de aplicación de la norma NTC-ISO-IEC 27001 (2013), la presente norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. La presente norma incluye también los requisitos para la valoración y el tratamiento de los riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

Esta norma consiste en la creación de un sistema de gestión de seguridad de la información (en adelante: SGSI), nos describe cómo gestionar la seguridad de la información de una organización, proporciona una metodología para implementar la seguridad de la información en una organización y nos recomienda los controles de seguridad que debemos aplicar a toda la infraestructura tecnológica de esa organizaciones para proteges los activos de la información, de igual forma incluye los requisitos para la valoración y el tratamiento de los riesgos de seguridad de la información y tiene como objetivo principal establecer, implantar, mantener y mejorar de forma continua la seguridad de la información de la organización

Las empresas se pueden certificar con esta norma, lo cual las hace más competitivas, además permite el ahorro económico al prevenir sus sistemas informáticos de cualquier amenaza que se llegará a materializar, así mismo reduce el riesgo al implementar los controles y la toma de conciencia y compromiso en todos los niveles de

la empresa, no solo al implementarla, sino que será permanente al tratarse de un ciclo basada en un enfoque de gestión de riesgos.

Esta metodología permite ser aplicada en cualquier organización ya sea pública o privada, organizaciones sin ánimo de lucro, ONG o cualquier otra Entidad que desee implementar su SGSI y proteger todo lo que afecte la seguridad de la información.

De igual modo esta norma presenta también algunas desventajas como son que los requisitos pueden parecer difíciles de interpretar, ya que existen nuevos conceptos, no podemos encontrar una descripción detallada de la identificación de los riesgos, requiere esfuerzo continuo de toda la organización.



### **4.3.3 Norma Técnica Colombiana NTC- ISO- IEC 27002.**

Según la presente Norma Internacional NTC- ISO- IEC 27002 (2013), está diseñada para uso por parte de las organizaciones, como referencia para la selección de controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la información (SGSI) con base en la ISO/IEC 27001, o como un documento guía para organizaciones que implementan controles de seguridad de la información comúnmente aceptados. Esta norma está prevista para uso en el desarrollo de directrices de gestión de la seguridad de la información específicas para la industria y las organizaciones, teniendo en cuenta su(s) entorno(s) específico(s) de riesgo de seguridad de la información

Las organizaciones de cualquier tipo y tamaño (incluido el sector público y privado, comercial y sin ánimo de lucro) recolectan, procesan, almacenan y transmiten información en muchas formas, que incluyen los formatos electrónicos, físico y las comunicaciones verbales (por ejemplo, conversaciones y presentaciones).

Esta norma nos permite evaluar el desempeño de la ISO 27001, la cual es una guía de buenas prácticas que describe los objetivos de control y controles recomendable en cuanto a la seguridad de la información, establece un catálogo de buenas prácticas que determina, desde la experiencia, una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en relación con el tratamiento de los riesgos.

### **4.4 Guía de gestión de riesgo No 7, Ministerio de las TIC.**

Según el Ministerio de las Tecnologías de la Información y las Comunicaciones en la guía número 7 de 2016, la cual habla de la seguridad y la privacidad de la información describe que: La información que hace parte de una Entidad Pública es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad o de un Estado. (Comunicaciones, 2016, pág. 39)

A través de esta guía se busca orientar y apoyar a las Entidades a gestionar los riesgos de seguridad de la información basado en los criterios de seguridad y privacidad de la información

como son la confidencialidad, integridad y disponibilidad de esta, buscando la integración con la Metodología de riesgos del DAFP,

### 5.1 Agencia Nacional del Espectro (ANE)

La Agencia Nacional del Espectro (ANE), es una Entidad del Estado Colombiano, fue creada con la expedición de la Ley 1341 de 2007, como una Unidad Administrativa Especial del orden nacional adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones, cuyo objetivo es brindar el soporte técnico para la gestión y la planeación, la vigilancia y control del espectro radioeléctrico, en coordinación con las diferentes autoridades que tengan funciones e actividades relacionadas con el mismo.

Adicionalmente con la expedición del decreto 094 de 2010, se establece la planta de personal, y con el decreto 093 del 19 de enero de 2010, se adopta la estructura de la ANE, posteriormente con el Decreto 4189 de 2011, se modifica la naturaleza jurídica de la ANE a una Unidad Administrativa Especial del orden nacional, con personería jurídica, autonomía técnica, administrativa, financiera y patrimonial propia, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones.

Seguidamente con la expedición del decreto 1991 del 12 de septiembre de 2013, se incrementa la planta de personal en ochenta y dos (82) funcionarios.

#### 3.1.1 Misión y Visión de la Agencia Nacional del Espectro

La ANE en su página web describe la Misión como "analizar la planeación, gestión, vigilancia y control del Espectro Radioeléctrico en Colombia, así como brindar la asesoría técnica para la gestión eficiente del mismo." (Espectro, [www.ane.gov.co](http://www.ane.gov.co), 2016)

De igual forma describe la Visión de la siguiente forma:

En el 2018, la ANE será reconocida como una entidad especializada e innovadora para la consecución de espectro en banda ancha, la aplicación de nuevas tecnologías para un sistema moderno de gestión, vigilancia y control y la formación de la comunidad en temas de espectro. (Espectro, [www.ane.gov.co](http://www.ane.gov.co), 2016)



## 5. MARCO CONTEXTUAL

### 5.1 Agencia Nacional del Espectro (ANE).

La Agencia Nacional del Espectro (ANE), es una Entidad del Estado Colombiano, fue creada con la expedición de la Ley 1341 de 2009, como una Unidad Administrativa Especial del orden nacional adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones, cuyo objeto es brindar el soporte técnico para la gestión y la planeación, la vigilancia y control del espectro radioeléctrico, en coordinación con las diferentes autoridades que tengan funciones o actividades relacionadas con el mismo.

Adicionalmente con la expedición del decreto 094 de 2010, se establece la planta de personal, y con el decreto 093 del 19 de enero de 2010, se adopta la estructura de la ANE, posteriormente con el Decreto 4169 de 2011, se modifica la naturaleza jurídica de la ANE a una Unidad Administrativa Especial del orden nacional, con personería jurídica, autonomía técnica, administrativa, financiera y patrimonio propio, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones.

Seguidamente con la expedición del decreto 1991 del 12 de septiembre de 2013, se incrementa la planta de personal en ochenta y dos (82) funcionarios.

#### 5.1.1 Misión y Visión de la Agencia Nacional del Espectro

La ANE en su página web describe la Misión como “realizar la planeación, atribución, vigilancia y control del Espectro Radioeléctrico en Colombia, así como brindar la asesoría técnica para la gestión eficiente del mismo y fomentar su conocimiento”. (Espectro, [www.ane.gov.co](http://www.ane.gov.co), 2016)

De igual forma describe la Visión de la siguiente forma:

En el 2018, la ANE será reconocida como una entidad especializada e innovadora para la consecución de espectro en banda ancha, la aplicación de nuevas tecnologías para un sistema moderno de gestión, vigilancia y control y la formación de la comunidad en temas de espectro. (Espectro, [www.ane.gov.co](http://www.ane.gov.co), 2016)

### 5.1.2 Organigrama de la ANE

La Ane actualmente está compuesta estructuralmente por un consejo directivo, una dirección general, un comité de coordinación del sistema de control interno, una comisión de personal y tres subdirecciones como son la subdirección de gestión y planeación técnica del espectro, la subdirección de vigilancia y control y la subdirección de soporte institucional, como se muestra en la Figura 2.

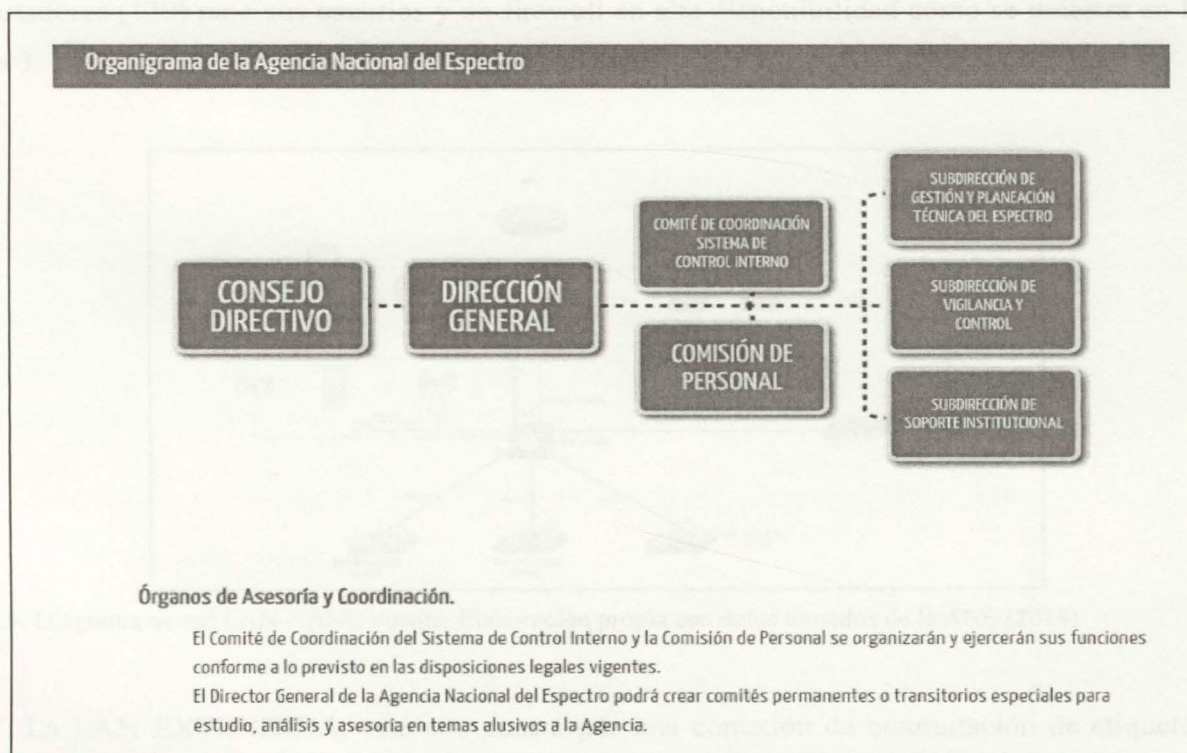


Figura 2. Organigrama de la ANE Fuente: (Espectro, [www.ane.gov.co](http://www.ane.gov.co), 2016)

### 5.1.3 Infraestructura tecnológica de la ANE

La infraestructura tecnológica de la entidad está conformada por su red de comunicaciones, arquitectura hardware y sus sistemas de información.





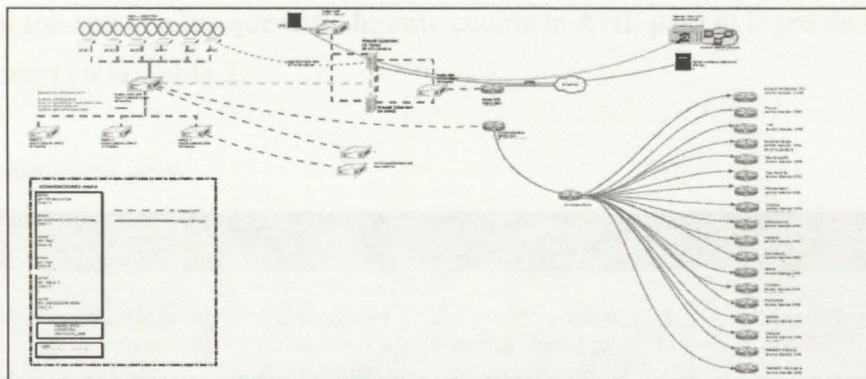


Figura 4. Diagrama LAN extendida ANE Fuente: Elaboración propia a partir de datos tomados de la ANE (2018)

#### 5.1.4.1 Arquitectura del centro de cómputo – ANE

El centro de cómputo de la ANE está conformado por dos (2) rack de comunicaciones, donde se encuentran alojados los servidores físicos, un sistema de alimentación ininterrumpida (en adelante: UPS) de 30 kva, con 15 minutos de autonomía de sus baterías, dos (2) aires acondicionados de 18 Btu, que enfrían el centro de cómputo, una planta telefónica, pisos falsos, extintores, sistema de regío como se muestra en la Figura 5.

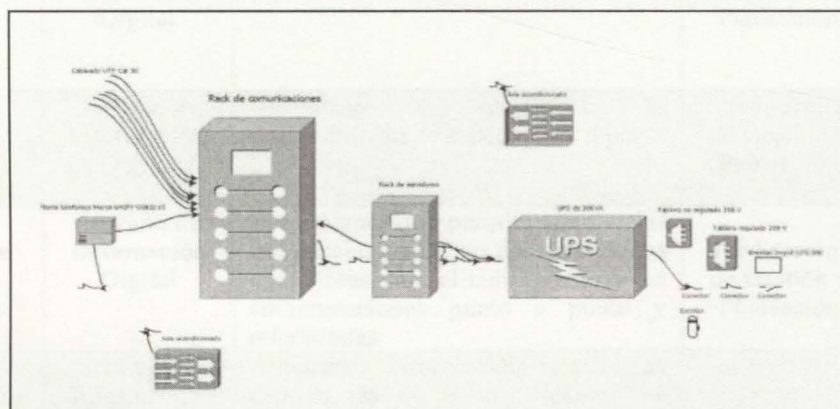


Figura 5. Arquitectura del centro de cómputo Fuente: Elaboración propia, datos tomados de la ANE (2018)

#### 5.1.4.2 Sistemas de información de la ANE

Actualmente los sistemas de información con que cuenta la Entidad están divididos en sistemas de información misionales y sistemas de información no misionales, los siguientes



sistemas de información son con los que actualmente cuenta la ANE para el logro de sus objetivos, los cuales se relacionan en la Tabla 2.

Tabla 2: Sistemas de Información ANE

| Ítem | Nombre del sistema  | Servicio o componente           | Objetivo del sistema  | Áreas usuarias  | Estado        |
|------|---|---------------------------------|---|---|---------------|
| 1    | <b>Portal Institucional Agencia Nacional del Espectro (Página Web)</b>                  | Servicio de Información Digital | Publicación de contenidos y comunicaciones de la entidad a la comunidad y sector en general.  | Todas las áreas   | En Producción |
| 2    | <b>Cuadro Nacional de Atribuciones de Banda de Frecuencia - CNABF</b>                   | Servicio de Información Digital | Muestra la totalidad de los servicios de radiocomunicación del país y su compatibilidad con la descripción de servicios del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT) de la cual forma parte la administración de Colombia. | Subdirección de Gestión y Planeación<br>Subdirección de Vigilancia y Control del Espectro | En producción |
| 3    | <b>Sistema de Monitoreo de Campos RNI - Wavecontrol</b>                                 | Servicio de Información Digital | Herramienta para monitorear en línea los niveles de campos electromagnéticos producidos por las antenas de telecomunicaciones a lo largo del territorio nacional.   | Subdirección de Vigilancia y Control  | En producción |
| 4    | <b>Indicadores de eficiencia del Uso del Espectro - INDEFI</b>                          | Servicio de Información Digital | Evaluar la eficiencia en el uso del espectro.   | Subdirección de Gestión y Planeación  | En producción |
| 5    | <b>Consulta de Espectro en Línea – CONALESPEC</b>                                       | Servicio de Información Digital | Visualizar y consultar la disponibilidad de espectro en el país.  | Subdirección de Gestión y Planeación  | En producción |
| 6    | <b>Sistema de simulación en línea - SpectrumE</b>                                       | Servicio de Información Digital | Herramienta que permite simular las frecuencias a solicitar por parte de los operadores para el cubrimiento y las comunicaciones punto a punto y microondas.  | Subdirección de Gestión y Planeación  | En producción |
| 7    | <b>Base de datos de visitas -DB Visitas</b>   | Servicio de Información Digital | Almacenar información relacionada con visitas de control técnico de espectro y PQRSD del uso clandestino de espectro (Mejorar el objetivo, validar con el SIS-INFO VISITAS)   | Subdirección de Vigilancia y Control  | En producción |
| 8    | <b>Formularios de registro de visitas Grupo Control Técnico del Espectro – TES Avit</b> | Servicio de Información Digital | Herramienta de registro de información referente a las verificaciones de control técnico del espectro radioeléctrico In Situ  | Subdirección de Vigilancia y Control  | En producción |



|    |  |                                 |   |                                       |               |
|----|--|---------------------------------|---|---------------------------------------|---------------|
| 9  | <b>Consulta de expediente en línea - EXPEDIENTES</b>                     | Servicio de Información Digital | Herramienta para realizar la consulta pública de los expedientes y el estado de las investigaciones.  | Subdirección de Vigilancia y Control  | En producción |
| 10 | <b>Actisoft</b>  | Servicio de Tecnología          | Software para el control de activos fijos, con el desde su incorporación hasta depreciación, traslados, mantenimientos, pólizas. En cualquier momento usted puede consultar de manera inmediata su inventario de act por cualquier: clasificación, ubicación, responsable, estado, factura, marca, ciudad, sucursal, unidad de negocio.   | Subdirección de Soporte Institucional | En producción |
| 11 | <b>Integra32</b>   | Servicio de Tecnología          | Gestionar el control del acceso de los funcionarios de la ANE   | Todas las áreas                       | En producción |
| 12 | <b>ARGUS</b>   | Servicio de Tecnología          | Software de gestión de las estaciones remotas de monitoreo de espectro a nivel nacional.  | Subdirección de Vigilancia y Control  | En producción |
| 13 | <b>OCS Manager</b>   | Servicio de Tecnología          | Realizar el inventario de los activos de hardware y software de TI.   | Todas las áreas                       | En producción |
| 14 | <b>Sistema de Gestión de Procesos de Negocios - ProcessMaker - Horus</b> | Servicio de Tecnología          | Permite diseñar, modelar, automatizar e implementar los procesos del negocio.   | Todas las áreas                       | En producción |
| 15 | <b>Intranet</b>  | Servicio de información digital | Publicación de contenidos y comunicaciones de la entidad al interior de esta  | Todas las áreas                       | En desarrollo |
| 16 | <b>Proyecto SCEM - SIRCE</b>   | Servicio de tecnología          | Plataforma por medio del cual la Agencia Nacional del Espectro (ANE), así como los proveedores de redes y servicios de telecomunicaciones, los operadores de televisión abierta radiodifundida y todos aquellos agentes que tengan la posesión, tenencia o que bajo cualquier título ostenten el control sobre la infraestructura activa para la prestación del servicio de telecomunicaciones, televisión y radiodifusión sonora, que tengan estaciones que generen campos electromagnéticos, así como a las empresas o personas naturales que estén interesadas en realizar mediciones de campos electromagnéticos, puedan agilizar la cantidad de estudios y trámites que se manejan para el cumplimiento a la resolución 754 de 2016. | Subdirección de Vigilancia y Control  | En desarrollo |
| 17 | <b>Sistema Nacional de Vigilancia del</b>                                | Servicio de tecnología          | Herramienta a través de la cual se pueden enviar ordenes de medición a  |                                       |               |



|    |  |                        |   |                                      |                     |
|----|--|------------------------|---|--------------------------------------|---------------------|
|    | <b>Espectro Radioelectrico-Spectrum-E2 - Centro de Monitoreo de Espectro - CME</b> |                        | una estación de monitoreo de Rohde Schwarz de forma automática a través del módulo ORM  | Subdirección de Vigilancia y Control | En producción       |
| 18 | <b>Monitoreo de variables</b>  | Servicio de tecnología | Medición en línea de las variables de temperatura, humedad, voltaje a UPS y apertura y cierre de rack, para 17 estaciones de monitoreo de espectro radioeléctrico.  | Subdirección de Vigilancia y Control | En producción       |
| 19 | <b>ERP</b>   | Servicio de tecnología | Sistema para gestionar y controlar de la mejor manera posible los recursos, procesos y operaciones de la Entidad.   | Todas las áreas                      | En desarrollo       |
| 20 | <b>SGDEA</b>   | Servicio de tecnología | Un grupo de sistemas de información destinados a gestionar documentos electrónicos y mantener los flujos de trabajo en entornos digitales logrando reducir el consumo de papel y mejorando la eficiencia en la institución. | Todas las áreas                      | En desarrollo       |
| 21 | <b>ESCORPÍO</b>  | Servicio de tecnología | Monitorear el espectro radioeléctrico a nivel nacional  | Subdirección de Vigilancia y Control | Fuera de producción |
| 22 | <b>TES MONITOR</b>   | Servicio de tecnología | Realizar la programación de las mediciones de espectro de acuerdo al Plan Anual de Espectro.  | Subdirección de Vigilancia y Control | Fuera de producción |
| 23 | <b>BSC – Sistema de Gestión Integrado</b>  | Servicio de tecnología | Herramienta de Balance Scorecard para medir los indicadores de proceso de la entidad  | Todas las áreas                      | Fuera de producción |
| 24 | <b>Viper - Automatización de Procesos</b>  | Servicio de tecnología | Herramienta de gestión y modelamiento de procesos, por medio del organigrama de la entidad, formularios y línea de tiempo.  | Todas las áreas                      | Fuera de producción |

Fuente: Elaboración propia, a partir de datos tomados de la ANE (2018)



## 6. METODOLOGÍA

La metodología es un procedimiento destinado a describir y analizar a fondo el problema planteado, está constituido por diferentes técnicas de investigación tales como la observación y recolección de datos, las cuales se manifiestan agregando operatividad y validez al caso estudio. El autor Blanco (2008) escribe que el marco metodológico “es el ‘cómo’ se realizará la investigación y está conformado en si por las estrategias, métodos, y los procedimientos necesarios para alcanzar los objetivos planteados”.

De acuerdo a lo planteado se describe entonces lo referente a la metodología aplicada a la investigación, abordando aspectos como tipo de investigación, enfoque y nivel. Así mismo se plantea el procedimiento que se implementó para el desarrollo del plan de acción.

### **Tipos de Investigación**

#### **Estudio Descriptivo**

Según el autor Galán (2012)<sup>4</sup> la investigación descriptiva es una de las más efectivas ya que permite observar, describir, predecir y controlar datos reales con el fin de entenderlos de mejor manera, además indica que “la finalidad de está radica en formular nuevos planteamientos y profundizar en los hechos existentes, e incrementar los supuestos teóricos de los fenómenos de la realidad observada”.

De igual manera, el autor Shuttleworth (2008), define el estudio descriptivo como “un método científico que implica observar y describir el comportamiento de un sujeto sin influir sobre él de ninguna manera”. Además, señala que los resultados no son necesariamente una respuesta definitiva a la investigación, sin embargo, esta arroja datos muy específicos que pueden ser analizados en el entorno en el que se desarrolla debido a que este es natural e invariable para los implicados; así pues, se obtiene un panorama general del objeto estudio de modo que pueda ser evaluado posteriormente, se puede decir que este tipo de investigación busca conocer las situaciones que se desarrollan en un ambiente de trabajo a través del estudio de las actividades, procesos y personas involucradas. Asimismo, su meta no se limita a la recolección de datos, sino a la predicción e identificación futuras necesidades.

---

<sup>4</sup> Galán A., M. (2012). *Investigación Descriptiva*. Disponible en: [http://manuelgalan.blogspot.com/2012\\_08\\_26\\_archive.html](http://manuelgalan.blogspot.com/2012_08_26_archive.html)



La presente investigación se ajusta al tipo descriptivo debido a que su desarrollo lleva a cabo el análisis de procesos relacionados con la seguridad de los sistemas de información misionales de la Agencia Nacional del Espectro (ANE), así como también controlar la información obtenida con el propósito de documentar el estudio.

### **Estudio de Campo**

En lo que respecta al estudio de campo el autor, Arias (2012) indica que “consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variables algunas”. (Arias 2012 p.31)

Mientras tanto Palella y Martins (2012) señalan que en el proceso de esta:

No se formulan hipótesis”, con referencia a esto podemos concluir que esta investigación no se basta por sí sola para la evaluación de datos y la generación de posibles soluciones, es por ello que intervienen los estudios anteriores, ya que unos complementan a los otros, debido a que todos se basan en distintas etapas de la investigación.

Tomando en cuenta lo anteriormente descrito, la investigación se suscribe a un estudio de campo debido que se realiza una recolección de la información de forma directa sin manipular o controlar alguna variable involucrada en los procesos de la Agencia Nacional del Espectro (ANE).

### **Diseño de la investigación**

La investigación por esta suscrita al tipo descriptivo emplearan técnicas de recolección de la información tales como: la revisión de documentos que proporcionen información acerca de las distintas metodologías que existen para la realización de análisis de riesgo de sistemas de información y efectuar un comparativo entre ellas con el fin de escoger la que más se adecue a la Agencia Nacional del Espectro (ANE); así mismo se identificarán los sistemas de información misionales existentes en la Entidad con el propósito de poder realizarles un análisis de riesgo a dichos sistemas, donde se detecten las amenazas y las vulnerabilidades que los azotan, con el propósito de poder estimar el impacto que puedan causar la falta de estos sistemas a la Entidad y posteriormente generar un plan de acción donde se recomienden o se listen los controles más adecuados que puedan contrarrestar dichos riesgos para contribuir con la mejor toma de decisión en el tratamiento de los mismos, ya sea para eliminarlos, controlarlos, aceptarlos, transferirlos o



mitigarlos y así de esta forma asegurar la integridad, confidencialidad y disponibilidad de la información que se encuentra alojada en dichos sistemas de información.

A continuación, se detallan los procedimientos que se desarrollaran:

- **Obtener el soporte de coordinación.** Organizar una reunión con el Coordinador TI de la Agencia Nacional del Espectro – ANE, para plantear el proyecto de investigación que se pretende, cuáles son los objetivos y cuáles son los beneficios en base al estándar ISO/IEC 27001:2013 y así obtener su aprobación y soporte durante todo el proceso.

Este proceso generó el documento requerido por el estándar ISO/IEC 27001:2013 de *Soporte y Aprobación por la Coordinación de TI*.

- **Definir el Alcance.** Determinar el departamento, servicios y procesos sobre los cuáles aplicará el correspondiente plan de riesgos es decir corresponde a la identificación de los Sistemas de Información Misionales de la ANE.
- **Definir la Metodología de Análisis y Evaluación de Riesgos.** Definir la Metodología de Evaluación de Riesgos y realizar el Análisis de Riesgos de los activos de información inventariados e identificar las vulnerabilidades y amenazas para así determinar el impacto de cada uno de ellos con el fin de establecer el nivel de riesgo existente. A su vez, se deben definir los criterios para aceptar los riesgos y establecer los controles de seguridad en base a los recursos disponibles.

Este proceso generó el documento requerido por el estándar ISO/IEC 27001:2013 de *Metodología de Análisis y Evaluación de Riesgos* y el *Reporte de Evaluación de Riesgos*, a continuación, se listan cada uno de los procesos desarrollados teniendo en cuenta la metodología seleccionada.

- **Identificación de Activos, Amenazas, controles y vulnerabilidades de Información.** Realizar el levantamiento de la información que serán abarcados por los Sistemas de Información Misionales, identificando los responsables, la clasificación (*hardware, software, infraestructura, servicios, aplicaciones, etc.*) y su valoración de acuerdo a su impacto y relevancia, con el fin de efectuar el *Análisis de Riesgos* en base a ellos.



- **Determinación de probabilidad de amenazas.** Se realizará teniendo en cuenta las diferentes probabilidades de ocurrencia, el grado de impacto ocurrido en los sistemas de información misional y a partir de la política de riesgos de la ANE.
- **Tratamiento de Riesgos.** Definir la forma en cómo se tratarán los riesgos (*mitigarlos, asumirlos, transferirlos a terceros o eliminarlos*) de acuerdo a los criterios seleccionados y justificar las razones de la implementación o no de los controles de seguridad en cada uno de los objetivos de control.

Este proceso generó los documentos requeridos por el estándar ISO/IEC 27001:2013 de *Declaración de Aplicabilidad y Plan de Tratamiento de Riesgos*.

Finalmente se generó el correspondiente Plan de Acción correspondiente a los sistemas de información misionales de la entidad.

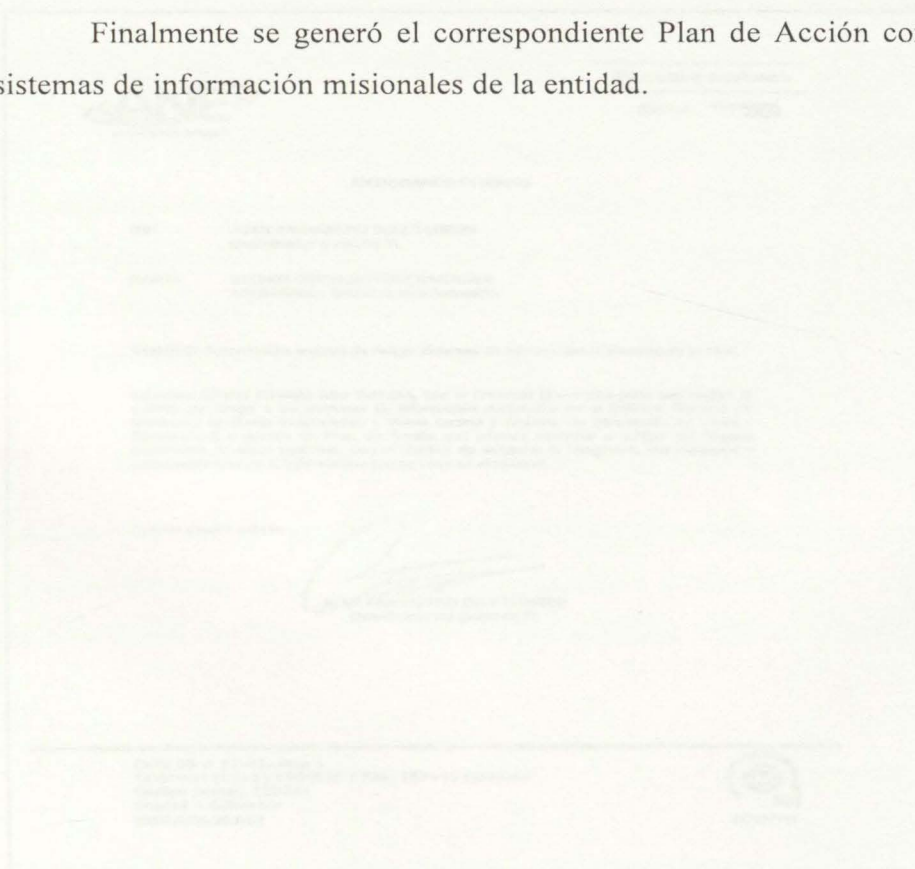


Figura 4. Registro de información

## 7. PLAN DE ACCIÓN PARA PROTEGER EL SISTEMAS DE INFORMACIÓN PARA LA AGENCIA NACIONAL DEL ESPECTRO (ANE)

### 7.1 Soporte de Coordinación y autorización

Como primera actividad se realizó una reunión con el Coordinador TI de la Agencia Nacional del Espectro (ANE), para plantear el proyecto de investigación, indicando lo que se pretende, cuáles son los objetivos planteados, así como también cuáles son los beneficios que ofrecerá el plan de acción basado en la normativa internacional ISO/IEC 27001:2013.

De igual manera se llevaron a cabo reuniones con el Administrador de servidores, Administrador de redes LAN y WAN, Administrador de base de datos, Administración de sistemas de información y oficial de seguridad, lo cual permitió llevar a cabo el desarrollo del proyecto.


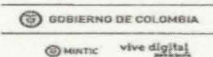


|  |  |
|--|--|
|   |  |
| <b>MEMORANDO INTERNO</b>   |  |
| <b>DE:</b>   | <b>JUAN FRANCISCO DIAZ TORRES</b><br>Coordinador grupo de TI                       |
| <b>PARA:</b>   | <b>EDUING OSVALDO DIAZ BARBOSA</b><br>Administrador Sistemas de Información        |
| <b>ASUNTO:</b> Autorización análisis de riesgo sistemas de información misionales de la ANE  |  |
| <p>Ingeniero Eduing Osvaldo Diaz Barbosa, con el presente lo autorizo para que realice el análisis de riesgo a los sistemas de información misionales de la Entidad, Sistema de Monitoreo de Radio Frecuencias – Wave control y Sistema de Simulación en Línea - Espectrum-E y genere un Plan de Acción que permita controlar o mitigar los riesgos detectados en estos sistemas, con el objetivo de asegurar la integridad, disponibilidad y confidencialidad de la información que en ellos se almacena.</p> |  |
| Con un cordial saludo,   |  |
| <br><b>JUAN FRANCISCO DIAZ TORRES</b><br>Coordinador del grupo de TI  |  |
| <hr/> Calle 93 # 17-45, Piso 4<br>Teléfono: (57+1) 6000030 / Fax: (57+1) 6000090<br>Código postal: 110221<br>Bogotá - Colombia<br><a href="http://www.ane.gov.co">www.ane.gov.co</a>   |  |
| <br>CO16/7161  |  |

Figura 6. Soporte de autorización



Una vez realizada la reunión con el Coordinador TI de la Agencia Nacional del Espectro (ANE) se obtuvo la autorización en donde se le permite al investigador observar los procesos de seguridad existentes dentro de la ANE, así como también genera el plan de acción acorde a los sistemas de información misionales.

Seguidamente y contando con la aprobación del Coordinador TI de la Agencia Nacional del Espectro (ANE) se establecieron las fases basadas en la normativa ISO/IEC 27001:2013 en las que se desarrollaría la investigación:

- **Definición del Alcance.**
- **Definición de la Metodología de Análisis y Evaluación de Riesgos.**
- **Identificación de Activos, Amenazas, controles y vulnerabilidades de Información.**
- **Determinación de probabilidad de amenazas.**
- **Tratamiento de Riesgos.**

## **7.2. Definición del Alcance**

En esta fase se busca determinar el alcance del plan de acción, tomando como objeto de estudio el departamento, los servicios y los procesos de los Sistemas de Información Misionales de la ANE. De este modo se podrá desarrollar un plan de acción a seguir para solventar la situación. Para cumplir con el objetivo de esta fase se muestran el histórico de cambios que ha sufrido los Sistemas de Información Misionales

### **7.2.1. Histórico de Cambios de los Sistemas de Información Misionales**

A continuación, en las tablas 3 y 4 se evidencian el historial de cambios en los diferentes ajustes y actualizaciones que han realizado en cuanto a la identificación de riesgos a la fecha por la Agencia Nacional del Espectro – ANE, en sus sistemas misionales de información.

## Wavecontrol

Tabla 3. Historial de cambios-Wavecontrol

| Histórico de Cambios- Wavecontrol |         |  |   |
|-----------------------------------|---------|--|---|
| FECHA                             | VERSIÓN | CREADO POR                               | VERSIÓN DEL CAMBIO                                  |
| 20/09/2012                        | 1,0     | Nelson Hernández -<br>Álvaro Casallas    | Inicial   |
| 15/12/2016                        | 1,1     | Nelson Hernández -<br>Luis Carlos Galvis | Ampliación Para Conectar<br>Mas Sondas De Monitoreo |
| 12/01/2018                        | 1,2     | Nelson Hernández -<br>Eduing Díaz        | Mejorar Presentación                                |

Fuente: Elaboración propia, a partir de datos tomados de la ANE (2018)

## Espectrum E

Tabla 4.: Historial de cambios- Espectrum E

| Histórico de Cambios- Espectrum E |         |  |  |
|-----------------------------------|---------|--|--|
| FECHA                             | VERSIÓN | CREADO POR                                       | VERSIÓN DEL CAMBIO                             |
| 30/10/2014                        | 1       | Johanna Cruz -<br>Carolina Daza                  | Inicial  |
| 22/12/2016                        | 1,1     | Johanna Cruz -<br>Carolina Daza - Eduing<br>Díaz | Extensión Del Sistema -<br>Mejorar El Servicio |
| 12/01/2018                        | 1,2     | Johanna Cruz -<br>Carolina Daza - Eduing<br>Díaz | Incluir Servicio De<br>Televisión              |

Fuente: Elaboración propia, a partir de datos tomados de la ANE (2018)

### 7.2.2. Alcance e identificación de los Sistemas de Información Misionales de la ANE

Para soportar los procesos misionales y de apoyo en una organización es importante contar con sistemas de información que se conviertan en fuentes únicas de datos útiles para apoyar o argumentar las decisiones que se tomen en las Entidades.

La ANE cuenta con sistemas de información que soportan tanto procesos misionales como los no misionales, los cuales además de garantizar la calidad de la información, la consulta para el público de interés y las transacciones desde los procesos que las generen, deberán contar con los mecanismos de seguridad para la integridad, disponibilidad y confidencialidad de la información que en ellos se almacena.



Ahora bien, dado que el objetivo de la ANE es: “Brindar soporte técnico para la gestión y planeación, la vigilancia y el control del espectro radioeléctrico, en coordinación con las diferentes autoridades que tengan funciones o actividades relacionadas con el mismo” (Ley 1341, Artículo 25, Inciso 2, 2009) y que los sistemas de información misionales son aquellos que sirven de apoyo a las Entidades para ayudar al cumplimiento de los objetivos propuestos y que además inciden directamente a la misión de la Entidad.

Para el diseño, desarrollo e implementación de los sistemas de información misionales Wave control y Spectrum-E contrató una organización externa, esto con el propósito de apoyar el cumplimiento de los mismos. En las tablas 5 y se 6 se evidencian la información a los sistemas misionales de la Agencia Nacional del Espectro (ANE)

Tabla 5. Sistema de Información Misionales ANE

|                                |   |  |
|--------------------------------|---|--|
| <b>Nombre del Sistema</b>      | Sistema de Monitoreo de Radio Frecuencias – Wave control  |  |
| <b>Servicio o componente</b>   | Servicio de tecnología  |  |
| <b>Categoría</b>               | Apoyo, Misional de gestión, Servicio de Información Digital   |  |
| <b>Objetivo del sistema</b>    | Herramienta para monitorear en línea los niveles de exposición de campos electromagnéticos producidos por las antenas de telecomunicaciones en varios (70) puntos a lo largo del territorio nacional, a través de instrumentos especializados ubicados en lugares estratégicos en cercanías a Centros Educativos, Hospitales, Hogares Infantiles y Geriátricos, de las principales ciudades del país. |  |
| <b>Tipo</b>                    | Web con base de datos central   |  |
| <b>Áreas usuarias</b>          | Subdirección de Vigilancia y Control  |  |
| <b>Líder Funcional</b>         | Profesional de Vigilancia y Control   |  |
| <b>Líder TI</b>                | Profesional Área TI   |  |
| <b>Funcionalidad detallada</b> | Captura de datos (Niveles de exposición a campos electromagnéticos) a través de la comunicación con las 70 sondas desplegadas a nivel nacional por parte de la ANE, procesamiento y graficación de los mismos.  |  |
| <b>Módulos</b>                 | <b>Módulos</b>  | <b>Descripción</b>   |
|                                | Sitios  | Modulo encargado de la información de todos los sitios registrados en la herramienta   |
|                                | Equipos   | Modulo encargado de la información de todas las sondas MonitEM registradas en el sitio |
|                                | Usuarios  | Modulo encargado de la gestión de usuarios y trazabilidad de estos                     |
|                                | Informas  | Modulo para la generación de informes de sitio   |
|                                | Configuración   | Modulo para configurar idioma, plantilla e interlocutores de la herramienta            |
| <b>URL</b>                     | <a href="http://smrni.ane.gov.co/">http://smrni.ane.gov.co/</a>   |  |
| <b>Proveedor</b>               | Tes América   |  |
| <b>Estado</b>                  | En producción   |  |
| <b>Número de licencias</b>     | N/A   |  |



|   |   |                          |   |                            |                                    |
|---|---|--------------------------|---|----------------------------|------------------------------------|
| <b>Tipo de licencias</b>                      | Licenciamiento ilimitado                            |                          |   |                            |                                    |
| <b>Modalidad implementación</b>               | On premises (Instalado en los servidores de la ANE) |                          |   |                            |                                    |
| <b>Plataforma de presentación</b>             | PHP   |                          |   |                            |                                    |
| <b>Ubicación del servidor de presentación</b> | <b>Ambiente</b>                                     | <b>Sistema Operativo</b> | <b>Centro de Datos</b>                        | <b>Nombre del Servidor</b> | <b>IP Pública/Privada</b>          |
|   | Producción  | XXXXXXXXXX               | Datacenter<br>Calle 93 No.<br>17-45<br>Piso 5 | XXXXXXXXXXXXXX             | 192.XXXXXX /<br>190.XXXXXX         |
| <b>Ubicación del servidor de aplicaciones</b> | <b>Ambiente</b>                                     | <b>Sistema Operativo</b> | <b>Centro de Datos</b>                        | <b>Nombre del Servidor</b> | <b>IP Pública/Privada</b>          |
|   | Producción  | XXXXXXXXXX               | Datacenter<br>Calle 93 No.<br>17-45<br>Piso 5 | XXXXXXXXXXXXXX             | 192.XXXXXXXXXX /<br>190.XXXXXXXXXX |
| <b>Plataforma de base de datos</b>            | SQL Server  |                          |   |                            |                                    |
| <b>Ubicación de base de datos</b>             | <b>Ambiente</b>                                     | <b>Sistema Operativo</b> | <b>Centro de Datos</b>                        | <b>Nombre del Servidor</b> | <b>IP Pública/Privada</b>          |
|   | Producción  | XXXXXXXXXX               | Datacenter<br>Calle 93 No.<br>17-45<br>Piso 5 | XXXXXXXXXXXXXX             | 192.XXXXXXXXXX /<br>190.XXXXXXXXXX |

Fuente: Elaboración propia, a partir de datos tomados de la ANE (2018)

Tabla 6. Sistema de Información Misional ANE

|                                |   |  |
|--------------------------------|---|--|
| <b>Nombre del Sistema</b>      | Sistema de simulación en línea - Espectrum-E  |  |
| <b>Servicio o componente</b>   | Servicio de tecnología  |  |
| <b>Categoría</b>               | Apoyo, Servicio de información digital, Misional de gestión   |  |
| <b>Objetivo del sistema</b>    | Herramienta que permite simular las frecuencias a solicitar por parte de los operadores para las frecuencias de cobertura y las frecuencias de comunicaciones pto a pto microondas.             |  |
| <b>Tipo</b>                    | Web con base de datos central   |  |
| <b>Áreas usuarias</b>          | Subdirección de Gestión y Planeación  |  |
| <b>Líder Funcional</b>         | Profesional de Gestión y Planeación   |  |
| <b>Líder TI</b>                | Profesional Área TI   |  |
| <b>Funcionalidad detallada</b> | Esta herramienta permite simular vía web cargando modelos de propagación estándar e importando la información del espectro asignado desde el sistema de gestión de espectro del Ministerio TIC. |  |
| <b>Módulos</b>                 | <b>Módulos</b>  | <b>Descripción</b>   |
|                                | Simulaciones  | Permite ver y consultar las simulaciones actuales y existentes en la plataforma de conformidad con los parámetros seleccionados. |
|                                | Opciones de Visualización   | Modificar los parámetros de visualización de los resultados.   |



|  |   |   |   |                     |                            |
|--|---|---|---|---------------------|----------------------------|
|  | Opciones Vectoriales  | Administrar y cargar vectores a la herramienta de acuerdo a los parámetros establecidos, archivo en formato vectorial Shapefile (shp+shx+dbf) o KMLs. |   |                     |                            |
|  | Imprimir Mapa   | Imprimir los reportes obtenidos en el mapa de acuerdo a los parámetros establecidos.  |   |                     |                            |
|  | Red   | Adicionar/Ver/Editar Objetos; importar enlaces, calcular viabilidades.  |   |                     |                            |
| URL                                    | <a href="http://simulacion.ane.gov.co:8088/se/portal/ane/login.php">http://simulacion.ane.gov.co:8088/se/portal/ane/login.php</a> |   |   |                     |                            |
| Proveedor                              | Tes América   |   |   |                     |                            |
| Estado                                 | En producción   |   |   |                     |                            |
| Número de licencias                    | 20  |   |   |                     |                            |
| Tipo de licencias                      | Por usuario nombrado  |   |   |                     |                            |
| Modalidad implementación               | On premises (Instalado en los servidores de la ANE)   |   |   |                     |                            |
| Plataforma de presentación             | PHP   |   |   |                     |                            |
| Ubicación del servidor de presentación | Ambiente  | Sistema Operativo   | Centro de Datos                               | Nombre del Servidor | IP Pública/Privada         |
|  | Producción  | XXXXXXXXXX  | Datacenter<br>Calle 93<br>No. 17-45<br>Piso 5 | XXXXXXXXXXXX        | 190.XXXXXX /<br>192.XXXXXX |
| Ubicación del servidor de aplicaciones | Ambiente  | Sistema Operativo   | Centro de Datos                               | Nombre del Servidor | IP Pública/Privada         |
|  | Producción  | XXXXXXXXXX  | Datacenter<br>Calle 93<br>No. 17-45<br>Piso 5 | XXXXXXXXXXXX        | 190.XXXXXX /<br>192.XXXXXX |
| Plataforma de base de datos            | SQL Server  |   |   |                     |                            |
| Ubicación de base de datos             | Ambiente  | Sistema Operativo   | Centro de Datos                               | Nombre del Servidor | IP Pública/Privada         |
|  | Producción  | XXXXXXXXXX  | Datacenter<br>Calle 93<br>No. 17-45<br>Piso 5 | XXXXXXXXXXXX        | 172.23.XX.XXX              |

Fuente: Elaboración propia, a partir de datos tomados de la ANE (2018)

### 7.3. Evaluación de la Metodología para los Sistemas de Información ANE

Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención contra peligros potenciales o reducir su impacto.



Ciertamente no existe una única metodología para evaluar los riesgos, lo ideal de realizar una selección de metodologías combinando las mejores técnicas según el tipo de negocio o de proyecto. De tal manera, a la hora de escoger una metodología, se debe tener en cuenta que algunas de estas herramientas son idóneas para evaluar las causas de un problema, mientras que otras son adecuadas para valorar las consecuencias.

El análisis de riesgos es el primer punto de la gestión de la seguridad de la información de una organización, y es necesario para la toma de decisiones.

En el caso de la Agencia Nacional del Espectro (ANE) el proceso para determinar la metodología adecuada comenzó con la investigación y el estudio pormenorizado de las principales técnicas existentes en el mercado para el análisis de los riesgos informáticos, con el fin de evaluarlas y conocer de forma detallada las ventajas y desventajas de cada una de ellas, así como también, su funcionamiento y las fases para el desarrollo de estas.

Las metodologías evaluadas en la investigación fueron:

- Octave.
- Magerit.
- Mehari.
- ISO 27001, 27002, 27005 e ISO 31000.

Para seleccionar la metodología más idónea para la Agencia Nacional del Espectro (ANE) se realizó una matriz de evaluación.

Cuadro N° 1. Matriz de Selección.

|                                    |                                     | Criterios              |                        |                        |                        |            |
|------------------------------------|-------------------------------------|------------------------|------------------------|------------------------|------------------------|------------|
|                                    |                                     | F. I. (25%)            | C. I. (25%)            | T. I. (25%)            | C. S. I. M. (25%)      | TOTAL 100% |
| Metodologías de Análisis de Riesgo | Octave                              | $3 \times 0.25 = 0.75$ | $2 \times 0.25 = 0.5$  | $3 \times 0.25 = 0.75$ | $2 \times 0.25 = 0.5$  | 2.5        |
|                                    | Magerit                             | $3 \times 0.25 = 0.75$ | $3 \times 0.25 = 0.75$ | $2 \times 0.25 = 0.5$  | $2 \times 0.25 = 0.5$  | 2.5        |
|                                    | Mehari                              | $2 \times 0.25 = 0.5$  | $2 \times 0.25 = 0.5$  | $3 \times 0.25 = 0.75$ | $3 \times 0.25 = 0.75$ | 2.5        |
|                                    | ISO 27001, 27002, 27005 e ISO 31000 | $4 \times 0.25 = 1$    | $4 \times 0.25 = 1$    | $4 \times 0.25 = 1$    | $4 \times 0.25 = 1$    | 4          |

Fuente: Elaboración propia (2018)

#### Leyenda

F. I.: Facilidad de Implementación.

C. I.: Costo de Implementación.

T. I.: Tiempo de Implementación.

#### Escala

1 = Muy deficiente.

2 = Deficiente.

3 = Regular.



C. S. I. M.: Compatibilidad con los 4 = Bueno.  
Sistemas de Información Misionales. 5 = Excelente.

Una vez realizada la herramienta Matriz de Selección se evidenció que la metodología más acorde para la Agencia Nacional del Espectro (ANE) es la **ISO 27001, 27002, ISO 27005, e ISO 31000**

Para el autor Lewis (2018) las características correspondientes a la última actualización de la norma ISO 27000/IEC 2018 publicadas en el mes de febrero de 2018 (Quinta Edición), proporcionan una descripción general de los sistemas de gestión de la seguridad de la información (ISMS), entre las cuales se describen a continuación:

- **ISO / IEC 27005: 2018** Este documento proporciona directrices para la gestión de riesgos de seguridad de la información.
- **ISO / IEC 27034-3: 2018** Este documento proporciona una descripción detallada y una guía de implementación para el proceso de administración de seguridad de la aplicación.
- **ISO / IEC TR 27103:2018** proporciona una guía sobre cómo aprovechar los estándares existentes en un marco de ciberseguridad.
- **ISO / IEC 27000: 2018** proporciona una descripción general de los sistemas de gestión de la seguridad de la información (ISMS). También proporciona términos y definiciones comúnmente utilizados en la familia de estándares ISMS.
- **NTC-ISO/IEC 27001:2013 (Norma Técnica Colombiana (ICONTEC)-Tecnología de la Información-Técnicas de Seguridad- Sistemas de Gestión de la Seguridad de la Información- Requerimientos).**

Finalmente, tomando en cuenta que la versión publicada en febrero de 2018 es reciente y el proyecto se había iniciado por cronograma se seleccionó la metodología ISO/IEC 27001:2013, para lograr los objetivos propuestos y generar la documentación respectiva. De igual manera, para el análisis de riesgos se consideraron las metodologías ISO/IEC 27005 y MAGERIT.

A continuación, se detallan los aspectos positivos tenidos en cuenta para la selección de la

metodología más adecuada a ser implementada para el cumplimiento de los objetivos propuestos.

- Metodologías reconocidas por ENISA (European Network and Information Security Agency)
- Compatibles con todas aquellas empresas que trabajan con sistemas informáticos y digitales
- Cumplen con la Estrategia de Gobierno en Línea, en el marco de la arquitectura de TI, exigidos por el Estado Colombiano a la Entidades del Gobierno Nacional, para lo cual les sugieren que tomen como base la metodología del Departamento Administrativo de la Función Pública (en adelante DAFP)<sup>4</sup> la cual se basó en las metodologías escogidas ISO/IEC 27001 e ISO/IEC 27005.
- Integran perfectamente con otras metodologías de análisis de riesgo.
- Las empresas pueden certificarse con esta norma, lo cual las hace más competitivas.
- Permiten el ahorro económico al prevenir sus sistemas informáticos de cualquier amenaza que se llegara a materializar.
- Metodologías fáciles de utilizar y evalúan todos los componentes que se requieren para llevar a cabo el desarrollo del análisis de riesgo en los sistemas de información misionales de la Entidad
- Se centran en aspectos cualitativos y cuantitativos del riesgo (Escala de medición)
- Sirve de base para crear el SGSI en la Entidades
- Hecha esencialmente para apoyar la tarea de análisis y gestión del riesgo en el marco de un SGSI.
- Permite identificar las necesidades de las organizaciones sobre los requisitos de seguridad de la información.
- Permiten realizar la identificación de activos, identificación de amenazas, identificación de controles existentes, identificación de vulnerabilidades y la estimación del riesgo



#### 7.4. Identificación de los Activos de Información.

Para los Sistemas de Información Misionales de la ANE existen unos activos necesarios, los cuales se evidencian en la tabla 7, los mismos fueron identificados y discriminados por el tipo de activo de acuerdo a la metodología utilizada.

Tabla 7. Clasificación de activos de información

| Tipo de Activo                | Activos Identificados  |
|-------------------------------|--|
| Software – SW                 | Base de datos, Aplicaciones (SIM), Servidores, Sistema Operativo de Servidores |
| Hardware – HW                 | Servidores, PCs de los usuarios  |
| Servicios Internos – SI       | Directorio Activo, Gestión documental, Web Service - Medición Antena           |
| Servicios Subcontratados – SE | Contrato de mantenimiento y desarrollo   |
| Datos / Información – D       | Información Interna de los Procesos Misionales.                                |
| Personal – P                  | Usuarios de los SIM, Servidores ANE  |
| Instalaciones Físicas – L     | Instalaciones de la ANE, Data Center   |

Fuente: Elaboración propia, a partir de datos tomados de la ANE (2018) e ISO/IEC 27005

#### 7.5 Identificación de las Amenazas

Siguiendo la secuencia de la metodología el siguiente paso consistió en realizar la identificación de las amenazas a los activos de los sistemas de información misionales de la Entidad, como afirma la norma ISO/IEC 27001 (2013) “Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrán ser accidentales o deliberadas”: (pág. 13)

Para este proyecto se identificaron las amenazas más relevantes de los sistemas de información misionales, caracterizándolas por el tipo de activo, además se utilizó como referencia el catálogo de amenazas de la metodología Magerit v3, y fueron segregadas en los siguientes grupos:

- Ataques [A]
- Errores humanos [E]
- De origen industrial [I]
- De origen natural [N]

### 7.5.1. Identificación de controles existentes

Los Sistema de Información Misionales, apoyan integralmente las funciones misionales de la gestión, planeación, vigilancia y control del espectro radioeléctrico de la ANE. Los sistemas cuentan con una parte técnica y funcional que maneja la oficina de sistemas de la entidad y la parte de garantía y soporte, que es manejada por un tercero.

Para la verificación o identificación de los controles existentes de seguridad de estos sistemas misionales, se realizó a través de una lista de chequeo, la cual se encuentra estructurada y definida bajo la norma ISO 27001 del 2013, agrupando la calificación en los 14 dominios de la norma:

- Política de Seguridad de la Información.
- Organización de la seguridad de la información.
- Seguridad de los Recursos Humanos.
- Gestión de Activos.
- Control de Acceso.
- Criptografía.
- Seguridad Física y del Entorno.
- Seguridad de Operaciones.
- Seguridad de las Comunicaciones.
- Adquisición, desarrollo y Mantenimiento de Sistemas.
  - Relaciones con los Proveedores.
  - Gestión de incidentes de la seguridad informática.
  - Aspectos de seguridad de la información de la gestión de continuidad del negocio.
  - Cumplimiento.

La lista de chequeo se realizó a los administradores de BD, Administradores de Servidores, Administrador de redes LAN y WAN, Oficial de seguridad técnicos y Sistemas de información, es decir a los dueños de cada proceso buscando con ello analizar el estado actual de seguridad existente de estos sistemas de información, como se muestran en el anexo A.

Con la información obtenida de la lista de chequeo, se pudo obtener una visión general del estado de seguridad de los sistemas de información misionales de la Entidad, la cual sirvió como



parte fundamental del insumo necesario para la generación del plan de acción. Dentro de la información obtenida por la lista de chequeo se obtuvo lo siguiente:

- La Entidad cuenta con un documento de políticas de seguridad de la información, pero este no ha sido dado a conocer por completo a los administradores, técnicos y funcionarios de los diferentes sistemas de información, aunque el documento fue aprobado por la alta dirección.
- Se debe definir un conjunto de políticas para la seguridad de la información propias para los sistemas de información misionales que posteriormente puede ser extendido a los demás sistemas de información de la entidad. Dicho documento debe ser aprobado por la entidad, publicado y comunicado a los empleados y a las partes externas pertinentes.
- Se deben definir procedimientos para el manejo de información sensible, teniendo en cuenta la confidencialidad, integridad y el no repudio.
- No existe un procedimiento establecido para que se elimine o cambie los derechos de acceso al sistema después de que se le notifica de un retiro o cambio de funciones de los funcionarios.
- Se debe definir una matriz de roles y perfiles que se maneje para dar acceso a las diferentes funcionalidades de los sistemas, puesto al parecer se están dando privilegios a usuarios que no corresponden. Adicionalmente se debe incluir dentro de la matriz las funcionalidades de consultas y reportes que genera la aplicación.

### **7.5.2. Identificación de Vulnerabilidades**

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.



### 7.5.2.1. Análisis de Vulnerabilidades

Después de haber realizado el escaneo de vulnerabilidades sobre los sistemas de información misionales (SIM), y que se identificó un total de 143 vulnerabilidades, clasificadas según su criticidad de impacto sobre los sistemas; Críticas, Altas, Medias, Bajas e Informativas, como se muestra en la figura 7, para el análisis y clasificación de las mismas no se tuvieron en cuenta todas las vulnerabilidades encontradas, si no solamente las que causaran mayor impacto en estos sistemas de información si se llegaran a materializar.

### 7.5.2.2. Clasificación de Vulnerabilidades

Las vulnerabilidades encontradas en los sistemas de información misionales de la ANE fueron clasificadas de acuerdo al nivel de criticidad para ambos sistemas, tomando en cuenta las que probablemente causarán mayor impacto de llegarse a materializar, mencionadas anteriormente.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla, el objetivo es identificar las vulnerabilidades de los activos empleados en los sistemas de información misionales que puedan convertirse en una potencial amenaza.

La presente investigación evidencia los resultados del análisis de vulnerabilidades realizadas sobre los Sistemas de Información Misional de la ANE, ofreciendo una visión global sobre las posibles vulnerabilidades en esos sistemas. De igual manera se pretende concientizar a la entidad y a los dueños de los activos involucrados sobre la importancia de los escaneos en los sistemas para detectar y minimizar los riesgos generados por las vulnerabilidades, adicionalmente se determinaron los posibles vectores de ataque dentro de la red de la entidad que ponen en riesgo la disponibilidad, integridad y disponibilidad de la información.

Para la ejecución del análisis de vulnerabilidad a los sistemas de información se utilizaron las herramientas Acunetix y Nessus, no se escaneo el código fuente de estos sistemas de información misionales dado que son sistemas tercerizados y la Entidad no cuenta o no contrato la entrega de estos códigos fuentes

**ACUNETIX**, Es una herramienta que permite escanear sitios web en busca de posibles fallas de seguridad y que puedan poner en peligro la integridad de una página publicada en Internet.



Esta aplicación ejecuta una serie de pruebas, totalmente configurables por el usuario, para identificar las vulnerabilidades tanto en la programación de la página como en la configuración del servidor web.

**NESSUS**, Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos, host y red, en operación normal, Nessus comienza escaneando los puertos con mapa o con su propio escaneo de puertos para buscar puertos abiertos, permitiendo así la definición de determinadas opciones para acceder a un escaneo mucho más preciso con el uso de filtros por puertos, máquinas, segmentos de red o protocolos.

#### 7.5.2.2.1 Análisis de vulnerabilidades con Acunetix y Nessus

Después de realizar el escaneo de vulnerabilidades a los sistemas de información misionales de la ANE, se obtuvo información a los cuales están expuesto estos sistemas en un posible ataque de alguna de las vulnerabilidades identificadas.

Como resultado del análisis de vulnerabilidades realizado a los sistemas de información misionales de la ANE, según su criticidad de impacto se identificaron en total 143 vulnerabilidades distribuidas en:

- 0 vulnerabilidades críticas (0%)
- 1 vulnerabilidad alta (1%)
- 17 medias (13%),
- 38 bajas (25%)
- 87 informativas (61%)

En la tabla 8 y la figura 7 se evidencian de forma general las vulnerabilidades presentes en los Sistemas de Información Misionales de la ANE.

Tabla 8. Resultados análisis de vulnerabilidades SIM

| Resultados | Vulnerabilidades encontradas |       |        |       |              |
|------------|------------------------------|-------|--------|-------|--------------|
|            | Criticas                     | Altas | Medias | Bajas | Informativas |
| Total      | 0                            | 1     | 17     | 38    | 87           |

Fuente: Elaboración propia

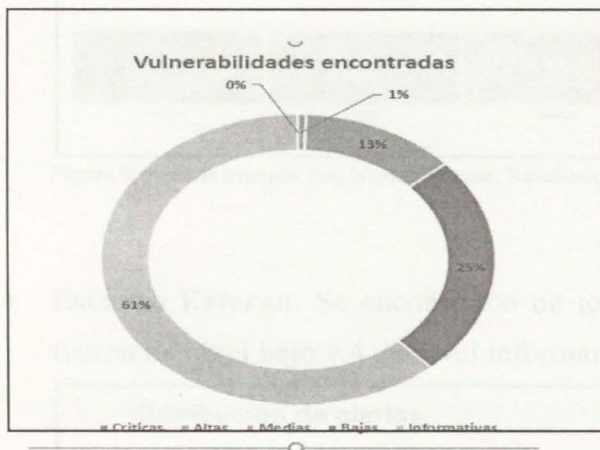


Figura 7. Resumen porcentual de vulnerabilidades sobre los SIM de la ANE. Fuente: Elaboración propia

**7.5.2.2.2. Escaneo de Vulnerabilidades - Wave control – SMRNI con Acunetix y**

**Nessus**

El objetivo de este escaneo fue identificar o detectar las vulnerabilidades que se están presente en este sistema de información misional de la Agencia Nacional del Espectro (ANE).

El escaneo realizado tuvo como alcance la Red Interna y Externa de la Entidad como se presenta a continuación.

- **Escaneo Interno:** Se encontraron un total de 40 vulnerabilidades, de las cuales 2 fueron de nivel medio, 11 de nivel bajo y 27 de nivel informativo como se muestra en la figura 8 y 9.

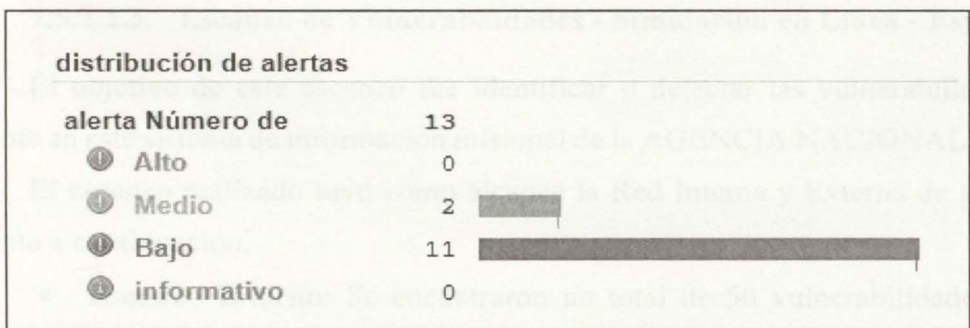


Figura 8. Distribución de alertas internas con Acunetix Fuente: Resultado del escaneo con la herramienta Acunetix (2018)



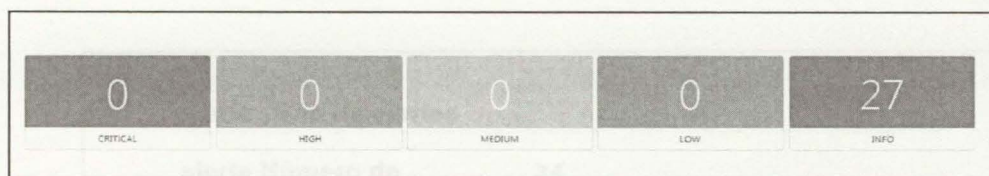


Figura 9. Alertas internas con Nessus Fuente: Resultado del escaneo con la herramienta Nessus (2018)

- **Escaneo Externo:** Se encontraron un total de 16 vulnerabilidades, de las cuales 12 fueron de nivel bajo y 4 de nivel informativo como se muestra en las figuras 10 y 11.

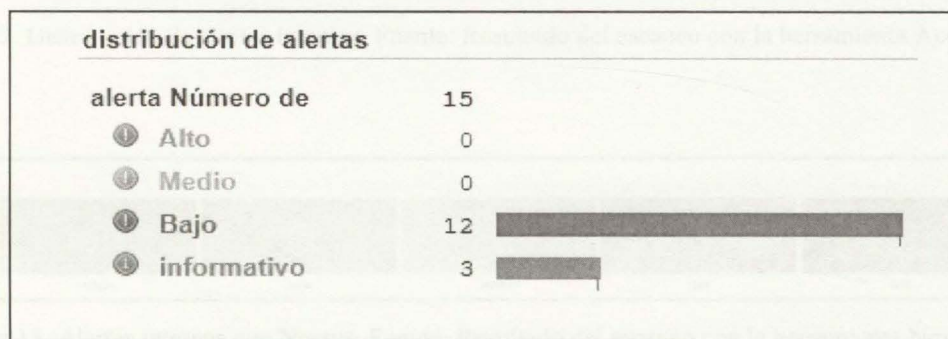


Figura 10. Distribución de alertas externas Acunetix Fuente: Resultado del escaneo con la herramienta Acunetix (2018)

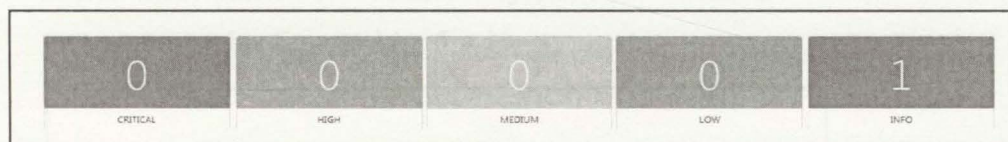


Figura 11, Alertas externa con Nessus. Fuente: Resultado del escaneo con la herramienta Nessus (2018)

### 7.5.2.2.3. Escaneo de Vulnerabilidades - Simulación en Línea - EspectrumE

El objetivo de este escaneo fue identificar o detectar las vulnerabilidades que se están presente en este sistema de información misional de la AGENCIA NACIONAL DEL ESPECTRO.

El escaneo realizado tuvo como alcance la Red Interna y Externa de la Entidad como se presenta a continuación.

- **Escaneo Interno:** Se encontraron un total de 50 vulnerabilidades, de las cuales 9 fueron de nivel medio, 8 de nivel bajo y 33 de nivel informativo como se muestra en las figuras 12 y 13.

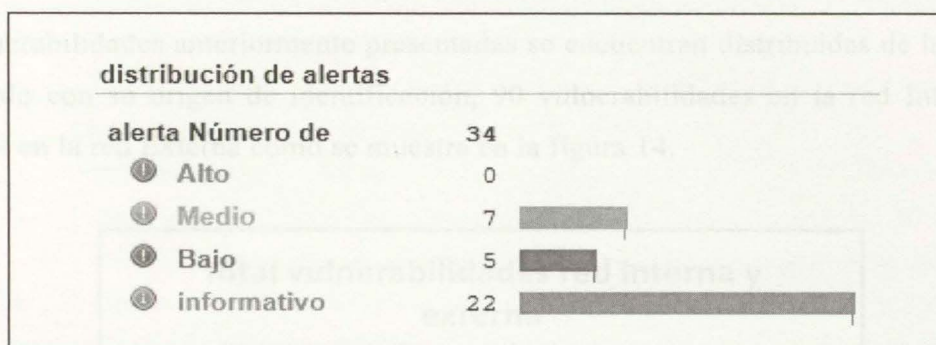


Figura 12. Distribución de alertas internas. Fuente: Resultado del escaneo con la herramienta Acunetix (2018)

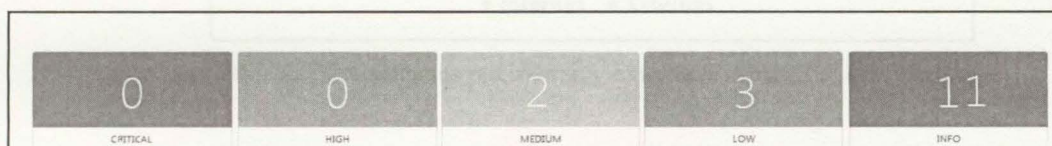


Figura 13. Alertas internas con Nessus. Fuente: Resultado del escaneo con la herramienta Nessus (2018)

- **Escaneo Externo:** Se encontraron un total de 37 vulnerabilidades, de las cuales 6 fueron de nivel medio, 7 de nivel bajo, 23 de nivel informativo y 1 de nivel alto como se muestra en las figuras 14, 15 y 16.

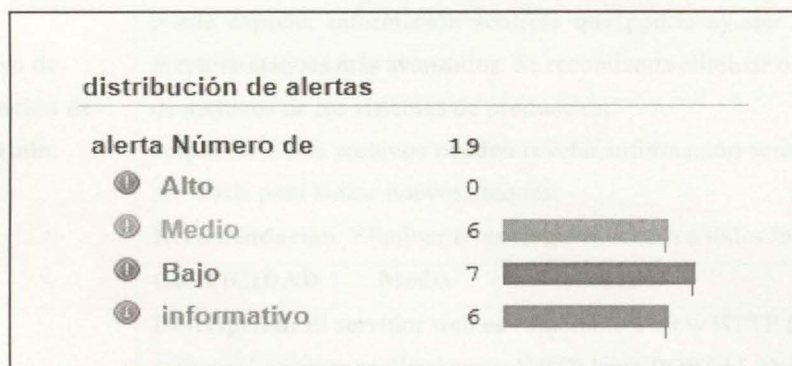


Figura 14. Distribución de alertas externas Acunetix. Fuente: Resultado del escaneo con la herramienta Acunetix (2018)

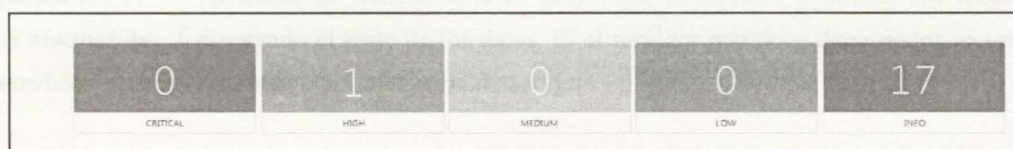




Figura 15. Alertas externas Nessus. Fuente: Resultado del escaneo con la herramienta Nessus (2018)

Las vulnerabilidades anteriormente presentadas se encuentran distribuidas de la siguiente forma de acuerdo con su origen de identificación, 90 vulnerabilidades en la red Interna y 53 vulnerabilidades en la red Externa como se muestra en la figura 14.

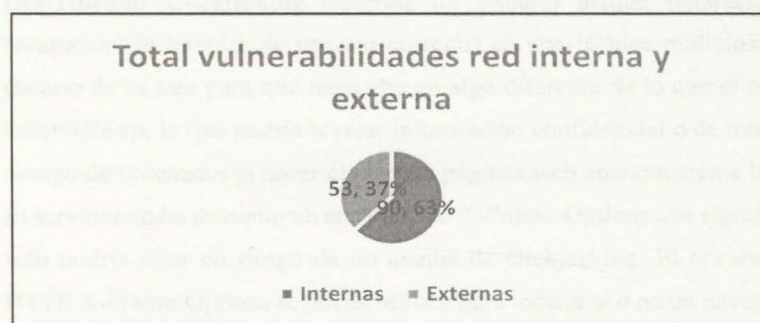


Figura 16. Total, Vulnerabilidades red interna y externa. Fuente: Elaboración propia

#### 7.5.2.2.4. Clasificación Vulnerabilidades SIM Wave control – SMRNI

Tabla 9. Identificación de vulnerabilidades SIM Wave control – SMRNI

| VULNERABILIDAD                                | DESCRIPCIÓN GENERAL   |            |               |      |               |  |  |  |
|---|---|------------|---------------|------|---------------|--|--|--|
| Archivo de configuración de desarrollo.       | <p><b>Descripción:</b> Un archivo de configuración se encuentra en este directorio. Este archivo puede exponer información sensible que podría ayudar a un usuario malicioso para preparar ataques más avanzados. Se recomienda eliminar o restringir el acceso a este tipo de archivos de los sistemas de producción.</p> <p><b>Impacto:</b> Estos archivos pueden revelar información sensible. Esta información puede ser usada para lanzar nuevos ataques.</p> <p><b>Recomendación:</b> Eliminar o restringir el acceso a todos los archivos de configuración</p>             |            |               |      |               |  |  |  |
|   | <table border="1"> <thead> <tr> <th>CRITICIDAD</th> <th>Media</th> <th>TIPO</th> <th>Configuración</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>   | CRITICIDAD | Media         | TIPO | Configuración |  |  |  |
| CRITICIDAD                                    | Media   | TIPO       | Configuración |      |               |  |  |  |
|   |   |            |               |      |               |  |  |  |
| La negación HTTP lenta de ataques de servicio | <p><b>Descripción:</b> El servidor web es vulnerable a Slow HTTP DoS (Denegación de Servicio) ataques. Los ataques Slowloris y HTTP lenta POSTAL DoS se basan en el hecho de que el protocolo HTTP, por diseño, requiere solicitudes para ser completamente recibidos por el servidor antes de ser procesadas. Si una solicitud HTTP no está completa, o si la velocidad de transferencia es muy baja, el servidor mantiene sus recursos ocupados esperando el resto de los datos. Si el servidor mantiene demasiados recursos ocupados, esto crea una denegación de servicio</p> |            |               |      |               |  |  |  |

|  | <p><b>Impacto:</b> Una sola máquina puede acabar con el servidor Web de otra máquina con un mínimo de efectos secundarios en ancho de banda y servicios no relacionados y los puertos.</p> <p><b>Recomendación:</b> Consultar las referencias Web para obtener información sobre cómo proteger su servidor web contra este tipo de ataque.</p>   |            |               |      |               |
|--|--|------------|---------------|------|---------------|
|  | <table border="1"> <thead> <tr> <th>CRITICIDAD</th> <th>Media</th> <th>TIPO</th> <th>Configuración</th> </tr> </thead> </table>  | CRITICIDAD | Media         | TIPO | Configuración |
| CRITICIDAD   | Media  | TIPO       | Configuración |      |               |
| <p><b>Clickjacking: X-Frame-opciones de la cabecera falta.</b></p> | <p><b>Descripción:</b> Clickjacking (Interfaz de Usuario ataque reparación, IU ataque de reparación, la interfaz de usuario corregir) es una técnica maliciosa de engañar a un usuario de la web para que haga clic en algo diferente de lo que el usuario percibe que hacen clic en, lo que podría revelar información confidencial o de tomar el control de su tiempo de ordenador al hacer clic en las páginas web aparentemente inocuos.</p> <p>El servidor no ha devuelto un encabezado X-Frame-Options que significa que esta página web podría estar en riesgo de un ataque de clickjacking. El encabezado de respuesta HTTP X-Frame-Options se puede utilizar para indicar si o no un navegador debe permitir que presentar una página dentro de un marco o iframe. Los sitios pueden usar esto para evitar los ataques de clickjacking, asegurando que su contenido no está incrustado en otros sitios.</p> <p><b>Impacto:</b> El impacto depende de la aplicación Web afectado.</p> <p><b>Recomendación:</b> Configurar el servidor web para incluir una cabecera X-Frame-Options. Consultar las referencias Web para obtener más información sobre los valores posibles para esta cabecera.</p> |            |               |      |               |
|  | <table border="1"> <thead> <tr> <th>CRITICIDAD</th> <th>Baja</th> <th>TIPO</th> <th>Configuración</th> </tr> </thead> </table>   | CRITICIDAD | Baja          | TIPO | Configuración |
| CRITICIDAD   | Baja   | TIPO       | Configuración |      |               |
| <p><b>Posibles directorios sensibles</b></p>                       | <p><b>Descripción:</b> Un directorio sensible posible se ha encontrado. Este directorio no está directamente vinculada a la comprobación website. Se buscan los recursos sensibles comunes, como los directorios de copia de seguridad de base de datos, vertederos, páginas de administración, directorios temporales. Cada uno de estos directorios puede ayudar a un atacante para aprender más acerca de su objetivo.</p> <p><b>Impacto:</b> Este directorio puede exponer información sensible que podría ayudar a un usuario malicioso para preparar ataques más avanzados.</p> <p><b>Recomendación:</b> Restringir el acceso a este directorio o eliminarlo de la página web.</p>   |            |               |      |               |
| <p><b>I</b></p>  | <table border="1"> <thead> <tr> <th>CRITICIDAD</th> <th>Baja</th> <th>TIPO</th> <th>Validación</th> </tr> </thead> </table>  | CRITICIDAD | Baja          | TIPO | Validación    |
| CRITICIDAD   | Baja   | TIPO       | Validación    |      |               |
| <p><b>Posibles archivos confidenciales</b></p>                     | <p><b>Descripción:</b> Un archivo sensible posible se ha encontrado. Este archivo no está directamente vinculado desde el sitio web. Esta comprobación busca recursos sensibles comunes, como archivos de contraseñas, archivos de configuración, archivos de registro, archivos de inclusión de datos de estadísticas, bases de datos volcados. Cada uno de estos archivos puede ayudar a un atacante para aprender más acerca de su objetivo.</p>  |            |               |      |               |



|                                   |  |                   |                    |             |                    |
|-----------------------------------|--|-------------------|--------------------|-------------|--------------------|
|                                   | <p><b>Impacto:</b> Este archivo puede exponer información sensible que podría ayudar a un usuario malicioso para preparar ataques más avanzados.</p> <p><b>Recomendación:</b> Restringir el acceso a este archivo o eliminarlo de la página web</p>  |                   |                    |             |                    |
|                                   | <table border="1"> <tr> <td><b>CRITICIDAD</b></td> <td><b>Baja</b></td> <td><b>TIPO</b></td> <td><b>Validación</b></td> </tr> </table>   | <b>CRITICIDAD</b> | <b>Baja</b>        | <b>TIPO</b> | <b>Validación</b>  |
| <b>CRITICIDAD</b>                 | <b>Baja</b>  | <b>TIPO</b>       | <b>Validación</b>  |             |                    |
| <b>Tiempo de respuesta lenta.</b> | <p><b>Descripción:</b> Esta página tuvo un tiempo de respuesta lento. Este tipo de archivos se pueden orientar en ataques de denegación de servicio. Un atacante puede solicitar esta página repetidamente desde varios equipos hasta que el servidor se sobre cargue</p> <p><b>Impacto:</b> Posible denegación de servicio.</p> <p><b>Recomendación:</b> Investigar si es posible reducir el tiempo de respuesta para esta página</p> |                   |                    |             |                    |
|                                   | <table border="1"> <tr> <td><b>CRITICIDAD</b></td> <td><b>Baja</b></td> <td><b>TIPO</b></td> <td><b>Informativo</b></td> </tr> </table>  | <b>CRITICIDAD</b> | <b>Baja</b>        | <b>TIPO</b> | <b>Informativo</b> |
| <b>CRITICIDAD</b>                 | <b>Baja</b>  | <b>TIPO</b>       | <b>Informativo</b> |             |                    |
| <b>Enlaces rotos.</b>             | <p><b>Descripción:</b> Un enlace roto se refiere a cualquier enlace que debería tomar a un documento, imagen o página web, que en realidad se traduce en un error. Esta página fue ligada en el sitio web, pero es inaccesible</p> <p><b>Impacto:</b> Problemas para navegar el sitio</p> <p><b>Recomendación:</b> Eliminar los enlaces a este archivo o hacerlo accesible.</p>  |                   |                    |             |                    |
|                                   | <table border="1"> <tr> <td><b>CRITICIDAD</b></td> <td><b>Baja</b></td> <td><b>TIPO</b></td> <td><b>Informativo</b></td> </tr> </table>  | <b>CRITICIDAD</b> | <b>Baja</b>        | <b>TIPO</b> | <b>Informativo</b> |
| <b>CRITICIDAD</b>                 | <b>Baja</b>  | <b>TIPO</b>       | <b>Informativo</b> |             |                    |

### 7. 5.2.3 Clasificación Vulnerabilidades Spectrum E

Tabla 10 Clasificación Vulnerabilidades Spectrum E

| VULNERABILIDAD                              | DESCRIPCIÓN GENERAL   |
|---|---|
| <b>Formulario HTML sin protección CSRF.</b> | <p><b>Descripción:</b> Esta alerta puede ser necesaria una confirmación manual de falsos positivos.</p> <p>Entre sitios de falsificación de petición, también conocido como un ataque o sección de manejo de un solo clic y abreviado como CSRF o XSRF, es un tipo de explotación maliciosa de un sitio web mediante el cual los comandos no autorizadas se transmiten de un usuario que confía el sitio web.</p> <p>Acunetix WVS encontró un formulario HTML sin aparente protección CSRF implementado.</p> <p><b>Impacto:</b> Un atacante puede forzar a los usuarios de una aplicación web para ejecutar acciones de comprometer los datos de usuario final y la operación en caso de usuario normal. Si el usuario final apuntado es la cuenta de administrador, esto puede comprometer toda la aplicación web.</p> <p><b>Recomendación:</b> Compruebe si esta forma requiere protección CSRF e implementar contramedidas CSRF si es necesario.</p> |

|   | CRITICIDAD  | Media | TIPO | Información   |
|---|---|-------|------|---------------|
| <b>La negación HTTP lenta de ataques de servicio</b>  | <p><b>Descripción:</b> Su servidor web es vulnerable a Slow HTTP DoS (Denegación de Servicio) ataques. Slowloris y HTTP lenta POSTAL DoS se basan en el hecho de que el protocolo HTTP, por diseño, requiere solicitudes para ser completamente recibidos por el servidor antes de ser procesadas. Si una solicitud HTTP no está completa, o si la velocidad de transferencia es muy baja, el servidor mantiene sus recursos ocupados esperando el resto de los datos. Si el servidor mantiene demasiados recursos ocupados, esto crea una denegación de servicio.</p> <p><b>Impacto:</b> Una sola máquina puede acabar con el servidor Web de otra máquina con un mínimo de efectos secundarios en ancho de banda y servicios no relacionados y los puertos.</p> <p><b>Recomendación:</b> Consultar las referencias Web para obtener información sobre cómo proteger su servidor web contra este tipo de ataque.</p>   |       |      |               |
|   | CRITICIDAD  | Media | TIPO | Configuración |
| <b>La versión de PHP que se ejecuta en el servidor web remoto se ve afectada por varias vulnerabilidades de denegación de servicio.</b> | <p><b>Descripción:</b> Según su banner, la versión de PHP que se ejecuta en el servidor web remoto es 5.6.x anterior a 5.6.30. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:</p> <p><b>Impacto:</b> Un atacante puede forzar a los usuarios de una aplicación web para ejecutar acciones de comprometer los datos de usuario final y la operación en caso de usuario normal. Si el usuario final apuntado es la cuenta de administrador, esto puede comprometer toda la aplicación web.</p> <p><b>Recomendación:</b> Actualice a PHP versión 5.6.30 o posterior.</p>  |       |      |               |
|   | CRITICIDAD  | Alta  | TIPO | Configuración |
| <b>Clickjacking: X-Frame-opciones de la cabecera falta</b>  | <p><b>Descripción:</b> Clickjacking (Interfaz de Usuario ataque reparación, IU ataque de reparación, la interfaz de usuario corregir) es una técnica maliciosa de engañar a un usuario de la web para que haga clic en algo diferente de lo que el usuario percibe que hacen clic en, lo que podría revelar información confidencial o de tomar el control de su tiempo de ordenador al hacer clic en las páginas web aparentemente inocuos.</p> <p>El servidor no ha devuelto un encabezado X-Frame-Options que significa que esta página web podría estar en riesgo de un ataque de clickjacking. El encabezado de respuesta HTTP X-Frame-Options se puede utilizar para indicar si o no un navegador debe permitir que presentar una página dentro de un marco o iframe. Los sitios pueden usar esto para evitar los ataques de clickjacking, asegurando que su contenido no está incrustado en otros sitios.</p> <p><b>Impacto:</b> El impacto depende de la aplicación Web afectado.</p> |       |      |               |
|   |   |       |      |               |



|  | <b>Recomendación:</b> Configurar el servidor web para incluir una cabecera X-Frame-Options. Consultar las referencias Web para obtener más información sobre los valores posibles para esta cabecera.   |            |               |      |               |
|--|---|------------|---------------|------|---------------|
|  | <table border="1"> <tr> <th>CRITICIDAD</th> <td>Baja</td> <th>TIPO</th> <td>Configuración</td> </tr> </table>   | CRITICIDAD | Baja          | TIPO | Configuración |
| CRITICIDAD   | Baja  | TIPO       | Configuración |      |               |
| <b>Cookies y sin HttpOnly conjunto del indicador</b>               | <p><b>Descripción:</b> Esta cookie no tiene establecido el indicador de HTTPOnly. Cuando una cookie se establece con la bandera HTTP, indica al navegador que la cookie sólo se puede acceder por el servidor y no por las secuencias de comandos del lado del cliente. Se trata de una protección de seguridad importante para las cookies de sesión.</p> <p><b>Impacto:</b> Ninguna.</p> <p><b>Recomendación:</b> Si es posible, se debe establecer el indicador HTTP</p>   |            |               |      |               |
|  | <table border="1"> <tr> <th>CRITICIDAD</th> <td>Baja</td> <th>TIPO</th> <td>Informativo</td> </tr> </table>   | CRITICIDAD | Baja          | TIPO | Informativo   |
| CRITICIDAD   | Baja  | TIPO       | Informativo   |      |               |
| <b>Cookies y sin pabellón conjunto Secure.</b>                     | <p><b>Descripción:</b> Esta cookie no tiene establecido el indicador de seguro. Cuando una cookie se establece con la bandera seguro, indica al navegador que la cookie sólo se puede acceder a través de canales SSL seguras. Se trata de una protección de seguridad importante para las cookies de sesión.</p> <p><b>Impacto:</b> Ninguna.</p> <p><b>Recomendación:</b> Si es posible, se debe establecer el indicador seguro para esta cookie.</p>  |            |               |      |               |
|  | <table border="1"> <tr> <th>CRITICIDAD</th> <td>Baja</td> <th>TIPO</th> <td>Informativo</td> </tr> </table>   | CRITICIDAD | Baja          | TIPO | Informativo   |
| CRITICIDAD   | Baja  | TIPO       | Informativo   |      |               |
| <b>Formulario de entrada oculta precio de llamada se encontró.</b> | <p><b>Descripción:</b> Se encontró una entrada de formulario oculto llamado precio. No es recomendable para ocultar información confidencial en los campos de formulario ocultos.</p> <p><b>Impacto:</b> El usuario puede cambiar la información de precios antes de enviar el formulario.</p> <p><b>Recomendación:</b> Compruebe si las entradas de secuencias de comandos están validadas adecuadamente.</p>  |            |               |      |               |
|  | <table border="1"> <tr> <th>CRITICIDAD</th> <td>Baja</td> <th>TIPO</th> <td>Informativo</td> </tr> </table>   | CRITICIDAD | Baja          | TIPO | Informativo   |
| CRITICIDAD   | Baja  | TIPO       | Informativo   |      |               |
| <b>Método TRACE está activado</b>                                  | <p><b>Descripción:</b> Método HTTP TRACE está habilitado en este servidor web. En presencia de otras vulnerabilidades entre dominios en los navegadores web, información de cabecera sensible se puede leer desde cualquier dominio que apoyan el método TRACE HTTP.</p> <p><b>Impacto:</b> Los atacantes pueden abusar funcionalidad TRACE HTTP para tener acceso a la información en las cabeceras HTTP como cookies y datos de autenticación.</p> <p><b>Recomendación:</b> Desactivar método trace en el servidor web.</p> |            |               |      |               |
|  | <table border="1"> <tr> <th>CRITICIDAD</th> <td>Baja</td> <th>TIPO</th> <td>Validación</td> </tr> </table>  | CRITICIDAD | Baja          | TIPO | Validación    |
| CRITICIDAD   | Baja  | TIPO       | Validación    |      |               |
| <b>Enlaces rotos</b>   | <p><b>Descripción:</b> Un enlace roto se refiere a cualquier enlace que debería tomar a un documento, imagen o página web, que en realidad se traduce en un error. Esta página fue ligada en el sitio web, pero es inaccesible.</p>   |            |               |      |               |

|   |  |  |             |                    |
|---|--|--|-------------|--------------------|
|   | <p><b>Impacto:</b> Problemas para navegar el sitio.</p> <p><b>Recomendación:</b> Eliminar los enlaces a este archivo o hacerlo accesible.</p>  |  |             |                    |
|   | <b>CRITICIDAD</b>  | <b>Baja</b>  | <b>TIPO</b> | <b>Informático</b> |
| <p><b>Contraseña de entrada de tipo de autocompletar habilitado</b></p> | <p><b>Descripción:</b> Cuando se introduce un nuevo nombre y contraseña en un formulario y se envía el formulario, el navegador le pregunta si la contraseña debe ser salvada cuando se muestra el formulario, el nombre y la contraseña se rellenan automáticamente o se hayan completado como se introduce el nombre. Un atacante con acceso local podría obtener la contraseña sin cifrar desde la caché del navegador.</p> <p><b>Impacto:</b> Posible divulgación de información sensible.</p> <p><b>Recomendación:</b> La contraseña de la función de autocompletar debe desactivarse en aplicaciones sensibles.</p> <p>Para desactivar el autocompletado, se puede usar un código similar al siguiente: <code>&lt;INPUT TYPE = "contraseña" auto-complete = "off"&gt;</code>. Luego de realizar el escaneo de vulnerabilidades, se obtuvo información importante que brinda el conocimiento al cual están expuestos los sistemas de información misionales en un posible ataque por explotación de alguna de las vulnerabilidades identificadas. Teniendo en cuenta el análisis se debe adelantar una evaluación detallada y profunda de los componentes de infraestructura para solucionar las vulnerabilidades identificadas, comenzando por aquellos de mayor vulnerabilidad para determinar las áreas específicas en que se requiere asistencia.</p> |  |             |                    |
|   | <b>CRITICIDAD</b>  | <b>Baja</b>  | <b>TIPO</b> | <b>Informativo</b> |
|   | <p><b>Un servicio que se ejecuta en el host remoto se ve afectado por múltiples vulnerabilidades</b></p>   | <p><b>Descripción:</b> Según su banner, la versión de OpenSSL que se ejecuta en el host remoto es 1.0.x anterior a la 1.0.2n. Por lo tanto, se ve afectado por múltiples vulnerabilidades que permiten la recuperación potencial de la información de la clave privada o la falla en el cifrado de datos.</p> <p><b>Recomendación:</b> Actualice a OpenSSL versión 1.0.2n o posterior.</p> |             |                    |
|   | <b>CRITICIDAD</b>  | <b>Baja</b>  | <b>TIPO</b> | <b>Informativo</b> |

## 7.6 Metodología de Análisis y Evaluación de Riesgos

Corresponde al análisis e implementación de la Metodología de Evaluación de Riesgos y realizar el Análisis de Riesgos de los activos de información inventariados de igual forma se describen las vulnerabilidades y amenazas para así determinar el impacto de cada uno de ellos con el fin de establecer el nivel de riesgo existente.



### 7.6.1. Análisis de riesgo a los SIM de la ANE

Basados en las metodologías seleccionadas ISO/IEC 27001 e ISO/IEC 27005, se identificaron los riesgos, las amenazas y las vulnerabilidades de los sistemas de información misionales de la Entidad, y se determinó la probabilidad y el impacto de ocurrencia los mismos.

Para ello, junto con los dueños de cada proceso de los sistemas de información misionales, se identificaron las amenazas, vulnerabilidades y riesgos asociados a cada uno de los activos de los sistemas de información, y se generó un plan de acción para los riesgos residuales de nivel ALTO mitigando o reduciendo el nivel de impacto y probabilidad de ocurrencia o materialización de los riesgos identificados, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Las metodologías empleadas para el análisis de riesgos en los sistemas misionales de la ANE fueron la metodología ISO/IEC 27005, y el anexo A de la metodología ISO/IEC 27001, por ser las que mejor se adaptaban a los objetivos planteados.

## 7.7 Identificación de los Riesgos

Tomando en cuenta las amenazas y vulnerabilidades identificadas en conjunto con los dueños de los procesos y el escaneo de los sistemas de información misionales de la Entidad, se determinó el riesgo de seguridad de la información para los mismos. Así mismo, se identifican las fallas de seguridad con mayor probabilidad de ser afectadas por el incumplimiento de los objetivos de materializarse las amenazas sobre dichos activos.

Estas probabilidades se utilizan para valorar las consecuencias de la materialización de una amenaza y la medida del perjuicio para la entidad si el activo se ve afectado por determinada falla de seguridad.

Para identificar los riesgos y las amenazas asociadas a las vulnerabilidades detectadas con el escaneo a los SIM, fueron identificadas con las herramientas ACUNETIX y NESSUS, así mismo, se tomó como base la matriz que se utilizó para identificar los riesgos de los activos más críticos empleados para los sistemas de información misionales, como se muestra en el anexo B7 y B8.



De igual manera, para la identificación de la forma de relacionamiento mediante una matriz de riesgos de vulnerabilidades en sistemas de información se contactó de forma presencial y telefónicas empresas nacionales, tales como **Password Consulting Services Sas, Sonda, NewNet S.A.**, dedicadas al resguardo de la seguridad de la información, a las cuales se les realizó la siguiente interrogante: **¿cuál sería la mejor forma de relacionar en una matriz de riesgo las vulnerabilidades identificadas con una herramienta de escaneo de vulnerabilidades a sistemas de información?**, obteniendo las siguientes respuestas por parte de las citadas empresas:

**Password Consulting Services Sas, (1991).** Es una empresa colombiana, que ofrece Servicios de consultoría en Seguridad de la Información, con experiencia de más de 10 años, conocimiento e innovación desarrollado de productos sólidos y confiables para asegurar su información.

Expertos en apoyar y acompañar a las organizaciones en su proyecto de implementación del Sistema de la Gestión de la Seguridad de la Información (SGSI), basado en la norma ISO 27001 y propenden por la seguridad de los activos de información de las empresas de nuestro País.

Password es líder en prestación de servicios de Seguridad de la Información, implementando soluciones de seguridad en empresas públicas y privadas. Recuperado de: <https://www.password.co/es/>

**SONDA. (1974)** La mayor multinacional latinoamericana de servicios de Tecnologías de la Información (TI), ubicada en la Av. Cra 45 Autopista Norte No 118 – 68. la cual se caracteriza por una profunda vocación de servicio, una amplia oferta de soluciones y una sólida posición financiera. Nuestra misión es agregar valor a los clientes, mediante el mejor uso de las Tecnologías de la Información. Nuestro sello ha estado marcado por un fuerte compromiso con cada uno de nuestros clientes, procurando establecer relaciones de largo plazo, lo cual nos exige entregar de manera consistente servicios y productos de calidad. Recuperado de: <https://www.sonda.com/es/co/>

**NewNet S.A – Consultoría, Software GRC y Servicios Administrados. (1996)** Cuenta con más de 20 años de experiencia en servicios y soluciones relacionados con tecnologías de la información y comunicaciones, en donde se ha caracterizado por sus valores y principios. Desde



su comienzo la empresa se ha dedicado a clientes corporativos, su estrategia es el conocimiento profundo de los mismos, buscando siempre las soluciones que sean acorde a sus necesidades.

Ahora **NewNet S.A** Hace parte del selecto grupo de empresas pioneras que representan al sector de Tecnologías de la Información (TI) de Colombia, ubicado en la Sede Norte. Autopista Norte # 103-34, en que lleva con orgullo la marca Colombia TI, posicionándonos como un aliado estratégico en el crecimiento económico de Colombia y como embajadores de una industria nacional pujante y madura, capaz de competir con empresas de talla mundial con un portafolio completo y diverso. Recuperado de: <http://www.newnetsa.com/>

Las anteriores empresas coincidieron en que la mejor forma de relacionar en la matriz de riesgo las vulnerabilidades encontradas con las herramientas de escaneo ACUNETIX y NESSUS en los sistemas de información misional de la Entidad, es teniendo en cuenta los datos arrojados en cada una de las vulnerabilidades detectadas de los sistemas de información escaneados y partiendo del análisis de esos mismos datos, en conjunto con el responsable de cada uno de los procesos en donde se ubica la respectiva vulnerabilidad, establecer claramente cuáles serían las posibles amenazas para esas vulnerabilidades, la probabilidad de materialización de las mismas y el impacto que puedan llegar a causar (Operacional, Reputacional o Legal), para así poder estimar los niveles de riesgos a los que se encuentran expuestos estos sistemas de información en caso de que se llegaran a materializar.

Lo anterior se pudo llevar a cabo con cada dueño de cada proceso o activos afectados tal como lo recomendaron las empresas consultadas, y se ve reflejado en las matrices de riesgos del anexo B7 y B8.

### **7.7.1 Estimación del Riesgo**

Para realizar la estimación del riesgo, la metodología utilizada contempla los siguientes ítems:

Inicialmente se debe dar una calificación a la probabilidad de materialización de la amenaza, en una escala de uno (1) a cinco (5).

- Se califica cada uno de los impactos (reputacional, legal y operativo) como se plantea en la tabla 16, a continuación, se realiza un promedio entre los mismos para determinar el valor único de impacto generado por la materialización de una amenaza utilizando la siguiente fórmula:

$$I_{total} = (Operacional + Reputacional + Legal) / 3$$

- Se calcula el nivel del riesgo inherente concatenando la probabilidad de ocurrencia de la amenaza y el total del impacto, luego es ubicado el riesgo inherente en el mapa de calor de la tabla 11. Una vez identificado el riesgo inherente, se deben ejecutar los controles requeridos en los criterios de aceptación del riesgo definidos para los sistemas de información misionales.

Tabla 11. Mapa de riesgo inherente

| Probabilidad   | Mapa de Riesgo Inherente |         |            |          |                | Impacto |
|----------------|--------------------------|---------|------------|----------|----------------|---------|
| 5- Casi seguro |                          |         | D-2, P-1   | S-1      |                |         |
| 4- Probable    |                          | D-4     | S-5        |          |                |         |
| 3- Posible     |                          | S-3, P2 | P-3, W1    |          |                |         |
| 2- Improbable  |                          | D-7     | D-1, E1    | S-2, P-6 |                |         |
| 1- Raro        |                          | S-7     |            |          |                |         |
|                | 1-Insignificante         | 2-Leve  | 3-Moderado | 4-Severo | 5-Catastrofico |         |

Fuente: Elaboración propia, a partir de datos tomados de la Guía para la Administración del Riesgo DAFP (2014)

### 7.7.2 Evaluación del Riesgo

Una vez identificado el riesgo inherente se debe realizar una comparación con criterios de evaluación de los riesgos. Los criterios determinan el riesgo en la seguridad de una organización, sin embargo, este proyecto se basa en los sistemas de información misionales en donde se tuvo en cuenta los siguientes aspectos:

Los sistemas de información misionales tienen un valor estratégico para la Agencia Nacional del Espectro, por lo tanto, cualquier riesgo identificado con nivel Alto o Extremo se le debe dar mayor prioridad en el tratamiento.



### 7.7.3 Control del Riesgo

En esta etapa se identifican los controles que actualmente se tienen para mitigar los riesgos, con el fin de evaluar su efectividad en la implementación de los controles y la reducción del impacto en caso de que el riesgo se materialice. El resultado final de esta etapa es la generación del mapa de riesgos residual el cual se obtiene de la medición de la efectividad de los controles existentes, que buscan minimizar el grado de severidad y el nivel de riesgo de los riesgos inherentes como se muestra en la tabla 12.

Tabla 12. Mapa de riesgo residual

| Probabilidad   | Mapa de Riesgo Residual |          |                    |          |                | Impacto |
|----------------|-------------------------|----------|--------------------|----------|----------------|---------|
| 5- Casi seguro |                         |          |                    |          |                |         |
| 4- Probable    |                         |          |                    |          |                |         |
| 3- Posible     | S-3, P-2                |          | P-3                |          |                |         |
| 2- Improbable  |                         | S-2      | S-5, D4            | S-1      |                |         |
| 1- Raro        |                         | S-7, D-7 | D-1, D-2, P-1, P-6 | S-10     |                |         |
|                | 1-Insignificante        | 2-Leve   | 3-Moderado         | 4-Severo | 5-Catastrofico |         |

Fuente: Elaboración propia, a partir de datos tomados de la Guía para la Administración del Riesgo DAFP (2014)

Luego de identificar y clasificar los riesgos inherentes se identificaron los controles que actualmente se tienen para mitigar los riesgos, con el fin de evaluar su efectividad y la reducción del impacto en caso de que el riesgo se materialice los cuales se ubicaron en la matriz de calor de riesgos residuales.

Finalmente, después de clasificarlos en riesgos residuales, los mismos quedaron tipificados en los niveles **EXTREMO** y **ALTO**, para los cuales se gestionará su tratamiento a través del diseño de planes de seguridad o plan de acción.

En la fase de medición, se identificaron en total veintisiete (27) riesgos inherentes; en la actualidad el 85,19 % de estos tienen aplicación de controles para tratar de mitigarlos; dichos controles son evaluados por cada uno de los riesgos para determinar su efectividad.



Una vez realizada la evaluación de efectividad de los riesgos por cada uno de los activos se determinó lo siguiente:

- **Software [SW]:** Para este activo se identificaron 11 riesgos y disminuyeron aquellos riesgos tipificados en el nivel EXTREMO, pasando de 3 a 0 y los riesgos tipificados en el nivel ALTO disminuyeron de 6 a 3.

El control “Contrato de Mantenimiento y Desarrollo”, es el que presenta mayor efectividad, reduciendo la probabilidad de materialización de la amenaza y pasando de un nivel del riesgo “Posible falta de integridad en el ingreso de la información al sistema” de extremo a medio.

El 25 % de los controles que son aplicados a este activo corresponden a un tipo de control preventivo.

La amenaza “Errores de mantenimiento / actualización de programas”, cuyo riesgo paso de nivel alto a nivel medio, esto gracias al control que actualmente se aplica para mitigarlo. Pero para dicho riesgo sino se realiza un adecuado monitoreo puede llegar a generar nuevas amenazas y vulnerabilidades puesto que los sistemas operativos de los servidores del SIM caducaron.

- **Datos / Información [D]:** Para este activo se identificaron un total de 8 riesgos, siendo el segundo activo junto con el de personas el de menor número de riesgos identificados.

Junto con el activo de persona, los datos fueron los de menor identificación de riesgos inherentes con el 16,6 %, pero luego de aplicar los controles correspondientes para cada uno de ellos se logró mitigar su probabilidad de ocurrencia, reduciendo sus niveles de alto y medio.

Dentro de todos los activos, el riesgo “Posible fuga de la información sensible”, fue el que presento la mayor calificación de probabilidad de ocurrencia de la amenaza (Casi Seguro). Luego de aplicar los controles se logró reducir su probabilidad a (Raro), es decir este riesgo quedo categorizado en el nivel MEDIO, porque aun si se llegase a presentar, su impacto está catalogado en nivel 3, pudiendo afectar algunas operaciones de los sistemas de información misionales de la Entidad.

- **Personas [P]:** Se logró identificar 8 riesgos inherentes para este activo, clasificados en los niveles Extremo, Alto y Medio, en donde el 62,5 % del total de los riesgos corresponden al nivel Alto y Extremo, porcentaje relativamente alto teniendo en cuenta la importancia de dicho activo para desempeño del sistema.



Luego de la ejecución de los controles, se logró reducir el nivel de los riesgos Extremos y Altos, a niveles aceptables para los SIM.

Aun cuando el riesgo “Posible fallo en las operaciones del sistema por indisponibilidad de personal”, que inicialmente se encontró en un nivel Extremo, luego de los controles fue catalogado en nivel Medio; sin embargo se debe realizar un monitoreo continuo sobre este ya que se están modificando el manual de funciones de la entidad impactando directamente las operaciones de los funcionarios en los SIM.

Los riesgos que formaron parte del proceso de tratamiento a través del diseño del plan de acción se muestran a continuación:

- Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios. [SW].
- Posible suplantación de usuarios por falta de protección de contraseñas. [SW].
- Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario. [SW].
- Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración. [SW].
- Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de estas en el sistema de información. [SW].
- Posible afectación de la confidencialidad de la información. [D].

#### 7.7.4 Valoración del Riesgo.

Basados en la etapa de estimación del riesgo, donde se identifica el riesgo inherente, tomando en cuenta la calificación numérica del impacto, probabilidad y la descripción de los riesgos, así como también, los controles para cada una de las vulnerabilidades identificadas. La valoración del riesgo se refleja en la severidad, que es el resultado de cruzar el impacto y la probabilidad, mide la intensidad en que un riesgo está presente lo que permite asignarle un valor y un nivel de riesgo de acuerdo a los colores correspondientes:

**Rojo** = Extremo. **Naranja** = Alto. **Amarillo** = Moderado o Medio. **Verde** = Bajo.

En la tabla 13 se muestra los criterios para la Valoración del riesgo con sus respectivos controles.

Tabla 13. Nivel de exposición o severidad del riesgo

| Nivel de exposición o severidad del riesgo |   |
|--|---|
| Riesgo                                     | Descripción   |
| <b>Extremo</b>                             | Se requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la alta dirección. INACEPTABLE   |
| <b>Alto</b>                                | Se requiere atención de la alta dirección. Planes de tratamiento requeridos, implementados y reportados a los jefes delegados, Oficina, Divisiones, etc. IMPORTANTE |
| <b>Moderado</b>                            | Aceptable, debe ser administrado con procedimientos normales de control. TOLERABLE  |
| <b>Bajo</b>                                | Menores efectos que pueden ser fácilmente remediados. Se administra con procedimientos rutinarios. No se requiere de ninguna acción. ACEPTABLE.                     |

Fuente: Elaboración propia, a partir de datos tomados de la política de riesgos ANE (2018)

#### 7.7.5. Tratamiento del Riesgo.

Durante esta etapa se definió la forma cómo se tratarán los riesgos (mitigarlos, asumirlos, transferirlos a terceros o eliminarlos) de acuerdo a los criterios seleccionados, así mismo se justifican las razones de la implementación o no, de los controles de seguridad en cada uno de los objetivos de control.

De igual manera, se analizó los riesgos inherentes identificados y se toman decisiones sobre su tratamiento, para lo cual se aplican los controles que actualmente tiene la entidad para dar cumplimiento al objetivo de control y por consiguiente mitigar los riesgos, algunas actividades pueden ser sencillas, mientras que otras alcanzarán el suficiente nivel de complejidad y costo como para que su ejecución se convierta en un proyecto para la entidad.

Para realizar una adecuada ejecución de los controles, se determinó asignar criterios cualitativos para la evaluación de controles como se muestra en la tabla 14.



Tabla 14. Criterios para la evaluación de controles

| Características del control       | Descripción  |
|-----------------------------------|--|
| Tipo de control                   | Especifica el tipo de control que será implementado (Preventivo, Detectivos o Correctivo). |
| Frecuencia                        | Periodicidad con que se utiliza el control   |
| Ejecución                         | Forma de implementar el control  |
| Complejidad                       | Grado de dificultad para ejecutar el control   |
| Documentación                     | Especifica el grado de identificación del control  |
| Evidencia                         | Registro del uso del control   |
| Recursos para ejecutar el control | Cantidad de recursos con que cuenta el área / subprocesos para ejecutar el control         |

Fuente: Elaboración propia

El resultado final de esta etapa es el valor del riesgo residual, este se da concatenando el valor de la probabilidad residual y el valor del impacto residual, para finalmente ubicarlo el riesgo residual en el mapa de calor, luego para los que se tipifique en los niveles **EXTREMO** y **ALTO**, se deberá gestionar su tratamiento a través del diseño del plan de acción o plan de seguridad.

#### 7.7.6 Informe del Análisis de riesgo

El presente informe, evidencia el resultado del análisis y gestión de riesgos aplicados a los sistemas de información misionales de la ANE. Para lo cual se tomaron como referencia las metodologías seleccionadas anteriormente, de igual manera se tuvieron en cuenta los lineamientos de la estrategia GEL del Ministerios de las TIC.

Para realizar el análisis se tuvieron en cuenta las siguientes fases:

- Caracterización del sistema de información
- Medición del riesgo
- Control del riesgo

En cada fase se identificaron una serie de características y criterios permitiendo hallar posibles fallas de seguridad que se verían afectadas para el incumplimiento de los objetivos y de esta manera comprometiendo a la Confidencialidad, Integridad y Disponibilidad de la información de los SIM de la Entidad



### 7.7.6.1 Caracterización del Sistema de Información

Para esta primera fase se tomaron como referencia los tres (3) activos de información identificados anteriormente como los más críticos para la ejecución de las tareas diarias de los sistemas, permitiendo con ello identificar para cada uno los riesgos.

### 7.7.6.2 Medición del Riesgo

Esta fase se evaluaron los riesgos identificados, sobre los cuales se determinaron la probabilidad y el impacto de estos. Para ello, el dueño del proceso identifica las amenazas, vulnerabilidades y riesgos de cada uno de los activos de información, con el fin de generar el plan de implementación o de acción de los controles que aseguren un ambiente informático seguro.

Dentro de los tres (3) activos definidos se identificaron un total de 27 riesgos, dada la calificación de probabilidad e impacto se clasificaron de acuerdo a su severidad.

Teniendo en cuenta la política de tratamiento de los riesgos para los sistemas de información misionales, a continuación, se relacionan los 17 riesgos inherentes que se identificaron en esta etapa y que por su calificación presentan la mayor severidad quedando tipificados en los niveles **EXTREMO** y **ALTO**.

Con el 40.8% el activo “Software” es el de mayor número de riesgos identificados, de igual manera es el que presenta el mayor número de riesgos extremos con un total de 3, al igual que el activo “Datos/ Información”.

Luego de la calificación de los riesgos inherentes el riesgo con mayor nivel de severidad **EXTREMO** correspondiente a “posible afectación de la integridad y disponibilidad de la información por abuso de privilegios”, del activo software.

Para cada riesgo identificado se determinó una amenaza, siendo las de tipo “Datos” y “Personas” las de menor presencia con el 29,6 % para cada una de ellas y en conjunto llegan al 59,2 % del total de las amenazas.

El riesgo con mayor número de vulnerabilidades identificadas corresponde a “Posible error humano en la protección de la Información debido al insuficiente conocimiento y aceptación de las responsabilidades con la seguridad informática.”, con un total de 5 y se encuentra bajo el activo personas.

Se identificaron un total de 51 vulnerabilidades para los 27 riesgos identificados, presentando un promedio 1,88 %. vulnerabilidades por cada riesgo identificado.



### 7.7.7 Criterios de Aceptación del Riesgo

Estos criterios permiten establecer los lineamientos orientados en la toma de decisiones respecto del tratamiento de los riesgos, con el fin de identificar las opciones para tratar y manejar los riesgos y tomar decisiones basadas en la valoración de estos.

En la tabla 15. Políticas de administración del riesgo, muestra los criterios para la evaluación de riesgo en la ANE.

Tabla 15. Política de administración o tratamiento del riesgo

| TRATAMIENTO DEL RIESGO  |
|---|
| Evitar el riesgo: Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.   |
| Reducir el riesgo: Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.   |
| Compartir o Transferir el riesgo: reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización. |
| Asumir un riesgo: Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.   |

Fuente: Elaboración propia, a partir de datos tomados de la política de riesgos ANE (2018)

### 7.8 Identificación de impactos.

Dado que este proyecto se basó en metodologías para gestionar riesgos tecnológicos cuya base fueron los estándares ISO/IEC 27001 e ISO/IEC 27005 para la identificación y el tratamiento de los mismos y que la Entidad para administrar y gestionar sus riesgos, definiendo criterios de impacto, criterios de probabilidad y criterios de aceptación basados en el estándar ISO/IEC 31000, el cual hace parte al igual que los dos estándares nombrados anteriormente de la familia ISO, fue posible establecer una alineación mucho más compatible entre estos tres estándares y ajustarlos a la metodología aplicada para el desarrollo de este proyecto.

Por consiguiente, se tomaron dichos criterios establecidos por la Entidad para determinar el impacto de afectación ya sea en lo operacional, reputacional o legal y la probabilidad de



ocurrencia de los riesgos identificados en caso de que se llagaran a materializar antes y después de aplicarle los contrales.

### 7.8.1 Criterios de Impacto

En los criterios de impacto se especificaron en términos de daño para la Entidad causados por un evento de seguridad, con una calificación que va de uno (1) a cinco (5) siendo uno (1) el impacto más bajo y cinco (5) el más alto como se muestra en la tabla 16:

- Operaciones deterioradas
- Daños a la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Tabla 16. Impactos por materialización de amenazas:

| Categoría             | Valor    | Operacional  | Reputacional   | Legal  |
|-----------------------|----------|--|--|--|
| <b>Catastrófico</b>   | <b>5</b> | Afecta la operación total de la ANE  | Se afecta gravemente la imagen de la ANE hay pérdida de credibilidad y opinión pública negativa. Hay divulgación en medios de comunicación | Incumplimiento de la normatividad legal vigente establecida en Colombia (Constitución, leyes, decretos). |
| <b>Severo</b>         | <b>4</b> | Afecta a todas las actividades de los SIM.                                     | Se afecta la imagen de la ANE por pérdida de credibilidad y opinión pública negativa.  | Incumplimiento de la normatividad exigida por los entes de control.                                      |
| <b>Moderado</b>       | <b>3</b> | Afecta la operación de algunas actividades del SIM.                            | Puede generarse una opinión pública negativa sobre la prestación del servicio.   | Incumplimiento de las Políticas internas de Seguridad de la Información, organizacionales                |
| <b>Leve</b>           | <b>2</b> | Genera reprocesos en las actividades, pero no afecta significativamente el SIM | La afectación de la Imagen de los SIM es Leve y resolver este tema implica recursos y puede durar buen tiempo.                             | Incumplimiento a los procedimientos y prácticas definidas para la operación adecuada.                    |
| <b>Insignificante</b> | <b>1</b> | No se afecta la operación del SIM  | La afectación de la Imagen del SIM es insignificante y fácil de resolver.  | No genera afectación legal.  |

Fuente: Elaboración propia, a partir de datos tomados de la política de riesgos ANE (2018)

### 7.9. Criterios de Probabilidad.

En los criterios de probabilidad se especificaron en términos de materialización de ocurrencia de una amenaza, con una calificación que va de uno (1) a cinco (5) siendo uno (1) la probabilidad más baja de materialización y cinco (5) la probabilidad más alta de materialización de las amenazas como se muestra en la tabla 17.



Tabla 17. Probabilidad de materialización de una amenaza

| Categoría             | Valor    | Descripción  |
|-----------------------|----------|--|
| <b>5- Casi seguro</b> | <b>5</b> | La materialización de la amenaza ocurre diariamente.                     |
| <b>4- Probable</b>    | <b>4</b> | La materialización de la amenaza ocurre una vez al mes.                  |
| <b>3- Posible</b>     | <b>3</b> | La materialización de la amenaza ocurre una vez al año.                  |
| <b>2- Improbable</b>  | <b>2</b> | La materialización de la amenaza ocurre en periodo de 2 a 5 años.        |
| <b>1-Raro</b>         | <b>1</b> | Nunca se ha materializado la amenaza, pero no se descarta su ocurrencia. |

Fuente: Elaboración propia, a partir de datos tomados de la política de riesgos ANE (2018)

### 7.9.1 Matriz de riesgo

A través de esta matriz se puede identificar o determinar objetivamente cuáles son los riesgos más relevantes de los sistemas de información misionales que enfrenta la Agencia Nacional del Espectro, como se refleja en los anexos B.

Para el llenado de esta matriz se tomaron como referencia los activos más críticos identificados para los sistemas de información misionales de la Entidad y las vulnerabilidades detectadas en el escaneo de estos sistemas con las herramientas ya mencionadas como fueron son:

- Software (SW)
- Datos / Información (D)
- Personal (P)
- Escaneo de vulnerabilidades a los SIM de la ANE

### 7.10. Elaboración del plan de acción

A continuación, se presenta el plan de reducción de brechas o plan de acción, el cual permite que la Agencia Nacional del Espectro (ANE) pueda garantizar la correcta implementación de las actividades de remediación sobre los riesgos residuales identificados, dichas actividades se basan en las mejores prácticas de gestión de riesgos de acuerdo con la metodología utilizada en el presente análisis.

El plan de acción es un conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos. Teniendo en cuenta esta premisa, se contará con un conjunto de decisiones necesarias para realizar los planes de acción para la seguridad de los sistemas de información misionales, de igual manera servirá como insumo para cualquier otro sistema de información de la Entidad.

Luego de la identificación de riesgos, amenazas y vulnerabilidades tanto en la matriz de riesgo como en el escaneo de los Sistemas de Información Misionales de la Entidad, se pudo determinar un conjunto de actividades que son importantes que sean realizadas por la Entidad, las cuales permitirán alinear las medidas de seguridad existentes con las exigidas y la reducción de los riesgos identificados.

Las actividades se agrupan en un plan de acción e implementación, el cual contiene el riesgo tratado identificado, activos afectados, plan de tratamiento, afectación, descripción de actividades, tiempo de implementación y responsable de la implementación.

De acuerdo con los criterios de aceptación de riesgos definidos en la metodología, los riesgos residuales a los cuales se les realiza un plan de acción o seguridad informática son los siguientes, como se muestra en la tabla 18.

Tabla 18. Riesgos residuales identificados

| Nº | Riesgos identificados   | Código | Categoría residual |
|----|---|--------|--------------------|
| 1  | Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios   | S-1    | ALTO               |
| 2  | Posible suplantación de usuarios por falta de protección de contraseñas.  | S-4    | ALTO               |
| 3  | Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario  | S-9    | ALTO               |
| 4  | Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración.                                     | S-10   | ALTO               |
| 5  | Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de estas en los sistemas de información. | S-6    | ALTO               |
| 6  | Posible afectación de la confidencialidad de la información   | D-5    | ALTO               |

Fuente: Elaboración propia

### 7. 10.1 Plan de acción o tratamiento de riesgos residuales de los SIM de la ANE

Se recomienda que todo el proceso de plan de acción sea supervisado por el área de Seguridad Informática, esto con el fin de mantener un control dual sobre las actividades realizadas a la infraestructura que corrijan las vulnerabilidades identificadas,

A continuación, se describen las recomendaciones a implementar de acuerdo con el plan de acción dentro de Agencia Nacional del Espectro.



- Cada uno de los riesgos presentados y descritos en el presente documento, debe ser revisado en detalle con el fin de tener un entendimiento de la afectación de cada riesgo hacia la infraestructura y el negocio.
- Contemplar la construcción de un plan de parches y migración de aplicaciones en sus últimas versiones. Lo anterior, en caso de no existir. Esto permite que los sistemas de información cuenten con un número mínimo de vulnerabilidades que no sean de dominios públicos o fáciles de explotar.
- Restringir el uso de aplicaciones que utilicen protocolos no seguros como http, FTP, Telnet, entre otros. Lo anterior con el fin de cerrar cualquier tipo de brechas que puedan afectar la infraestructura a través de este tipo de servicios.
- Así mismo, es importante tener en cuenta que el plan de acción se plantea por nivel de severidad de los riesgos, a los cuales se encuentran expuestos estos sistemas para así poder recomendar los mejores tratamientos para cada uno de ellos para que a futuro sean implementados por la entidad con el objetivo de poder evitar la pérdida o alteración de la información que en ellos se almacena a partir de la implementación de la norma internacional ISO/IEC 27001.

Tabla 19. Plan de acción o tratamiento de riesgos residuales de los SIM de la ANE

| Riesgos  | Activos afectados   | Riesgo Residual    | Plan de Tratamiento | Afecta |   |   | Descripción plan de acción   | Responsable               |
|--|---|--------------------|---------------------|--------|---|---|--|---------------------------|
|  |   |                    |                     | D      | I | C |  |                           |
| D-5. Posible afectación de la confidencialidad | Información en Bases de Datos, Servidores de Administración, sistemas de información, correos, carpetas | <b>Riesgo Alto</b> | Reducir el riesgo   |        |   | C | Establecer procedimiento de autenticación de usuario y control de acceso, tanto para la visualización como para el tratamiento de los datos; | Oficina de Tecnología     |
|  |   |                    |                     |        |   |   | Realizar permanentemente campañas de seguridad   | Oficina de Comunicaciones |
|  |   |                    |                     |        |   |   | Asegurar que solo es posible acceder a los sistemas tras un proceso de   | Oficina de Tecnología     |

|   |   |             |  |  |           |   |                                 |
|---|---|-------------|--|--|-----------|---|---------------------------------|
| de la información   |   |             |  |  |           | autenticación SEGURO  |                                 |
|   |   |             |  |  |           | Realizar copias de respaldo de la información   | Oficina de Tecnología           |
|   |   |             |  |  |           | Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios | Oficina de Tecnología           |
|   |   |             |  |  | PLAZO     | 2 MESES   |                                 |
| S-6. Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de estas en los sistemas de información | Bases de datos, Directorio Activo, Red LAN, Red WAN, Servidores de Producción, sistemas de información, bases de datos, correos | Riesgo Alto | Reducir el riesgo                          |  | D         | Monitorear periódica los Logs de eventos de seguridad.  | Oficina de Tecnología           |
|   |   |             |  |  |           | Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios | Oficina de Tecnología           |
|   |   |             |  |  |           | Garantizar capacitación en seguridad a los funcionarios de la oficina de tecnología           | Oficina de Personal             |
|   |   |             |  |  |           | Asegurar que solo es posible acceder a los sistemas tras un proceso de autenticación SEGURO   | Oficina de Tecnología           |
|   |   |             |  |  |           | Garantizar la debida ejecución de las pruebas de contingencia de TI                           | Coordinador plan de continuidad |
|   |   |             |  |  | PLAZO MAX | 1 MES   |                                 |
| S-10. Posible afectación en la disponibilidad e integridad de los sistemas por la manipulación de la configuración                                | Bases de datos, Directorio Activo, Servidores de Administración, Servidores de bases de datos. Servidores de                    | Riesgo Alto | Medidas preventivas para reducir el riesgo |  | D         | Monitorear periódicamente los Logs de eventos de seguridad.                                   | Oficial de Seguridad            |
|   |   |             |  |  |           | Garantizar que todo cambio que se realizan en   | Oficina de Tecnología           |



|   |  |                    |  |  |   |   |  |
|---|--|--------------------|--|--|---|---|--|
|   | aplicaciones, de producción, Correos   |                    |  |  |   | producción es aprobado por el comité de cambios                                     |  |
|   |  |                    |  |  |   | Revisar periódicamente el estado de los usuarios, roles y permisos en los sistemas. | Oficial de Seguridad   |
|   |  |                    |  |  |   | PLAZO MAX   | 1 MES  |
| S-9. Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario | Bases de datos, Directorio Activo, Servidores de Administración, Servidores de bases de datos de producción, sistemas de información, Correo, carpetas | <b>Riesgo Alto</b> | Medidas preventivas para reducir el riesgo |  | I | C   | Monitorear periódica los Logs de eventos de seguridad.<br>Oficial de Seguridad<br>Revisar periódicamente el estado de los usuarios, roles y permisos los sistemas.<br>Oficial de Seguridad<br>Implementar mecanismo de cifrado de disco duro de los dispositivos móviles y portátiles de la entidad<br>Oficina de Tecnología<br>Capacitación de usuarios en materia de uso y manejo de usuario y contraseñas<br>Oficina de Tecnología<br>Garantizar que se implementen políticas de usuario y contraseñas seguras, para usuarios internos y externos<br>Oficial de Seguridad |
|   |  |                    |  |  |   | PLAZO MAX   | INMEDIATO  |
| S-4. Posible suplantación   |  | <b>Riesgo Alto</b> | Medidas preventivas                        |  | I | C   | Monitorear periódica los Logs<br>Oficina de Tecnología   |

|  |  |             |                        |           |           |  |   |   |
|--|--|-------------|------------------------|-----------|-----------|--|---|---|
| de usuarios por falta de protección de contraseñas   | Directorio Activo, sistemas de información, bases de datos, Correos, carpetas  |             | para reducir el riesgo |           |           |  | de eventos de seguridad.  |   |
|  |  |             |                        |           |           |  | Revisar periódicamente el estado de los usuarios, roles y permisos en los sistemas, directorio activo, bases de datos y aplicaciones                    | Oficial de Seguridad                          |
|  |  |             |                        |           |           |  | Capacitación de usuarios en materia de uso y manejo contraseñas   | Oficina de Tecnología                         |
|  |  |             |                        |           |           |  | Garantizar que este implementada las políticas de contraseña segura y bloqueo automático de pantallas.  | Oficial de Seguridad<br>Oficina de Tecnología |
|  |  |             |                        |           |           |  | Realizar permanentemente campañas de seguridad  | Oficial de Seguridad                          |
|  |  |             |                        | PLAZO MAX | INMEDIATO |  |   |   |
| S-1. Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios | Bases de datos, Directorio Activo, Equipos de seguridad perimetral, Servidores de Administración, Servidores de bases de datos de producción, Servidores de aplicaciones de producción, Plataforma de Correo | Riesgo Alto | Reducir el riesgo      | D         | I         |  | Monitorear de manera periódica los Logs de eventos de seguridad y las actividades que realizan los administradores                                      | Oficial de Seguridad                          |
|  |  |             |                        |           |           |  | Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones | Oficial de Seguridad                          |



|  |  |  |  |           |  |   |
|--|--|--|--|-----------|--|---|
|  |  |  |  |           | Eliminar (si es posible) o bloquear las cuentas de súper administradores. En caso de bloqueo la contraseña de esta deberá ser administrado por el oficial de seguridad | Oficial de Seguridad<br>Oficina de Tecnología |
|  |  |  |  |           | Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios  | Oficina de Tecnología                         |
|  |  |  |  | PLAZO MAX | 1 MES  |   |

Fuente: Elaboración propia, a partir de datos tomados de la política de riesgos ANE (2018)

### 7.11 Monitoreo y Control.

Corresponde a la última fase del proceso de análisis de riesgos, la cual consiste en hacer seguimiento y control, al cumplimiento de los planes de acción definidos para los riesgos identificados con severidad extrema y alta.

Si el valor del riesgo residual es despreciable, los controles implementados son los adecuados, esto no quiere decir que se debe descuidar el riesgo, simplemente hay gestión efectiva del sistema de seguridad de la información.

Es importante entender que un valor residual es sólo un valor, el riesgo residual es un indicador, su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer para mitigar este riesgo, lo cual se involucra en el plan de tratamiento de riesgos acompañado de un monitoreo constante evaluando continuamente los controles y su efectividad.

## 8. Conclusiones y Recomendaciones

### Conclusiones

Cumpliendo con los objetivos planteados en la investigación, se pueden exponer las conclusiones obtenidas a partir de un análisis exhaustivo de la problemática establecida dentro de la Agencia Nacional del Espectro (ANE). El determinar el estado actual de los sistemas de información misionales permitió conocer las falencias en el manejo de la seguridad en los mismos, los cuales son de vital importancia para el desarrollo de los procesos internos de la ANE. Tomando como base los resultados obtenidos, se concluye lo siguiente:

El poder conocer y evaluar varias metodologías para la realización del análisis de riesgo en los sistemas de información misionales de la ANE nos permitió conocer para cada una de ellas sus funcionalidades, ventajas, desventaja, campos de aplicación, entre otras características y además se pudo decidir las que más se alineaban con los objetivos misionales de la Entidad y las que le permitían ayudar con al cumplimiento de varios requisitos exigidos por el Gobierno colombiano en materia de la seguridad informática y de la información.

Toda organización bien se pública o privada, debe contar con políticas de seguridad para los sistemas de información, así mismo se debe poseer una serie de medidas de contingencia en cuanto a ataques que vulneren la seguridad de los sistemas de información.

En el caso de la Agencia Nacional del Espectro (ANE) existía falencias en cuanto a los protocolos de seguridad de los sistemas de información misionales, afectando las operaciones internas de la entidad, ocasionando pérdida de información relevante, lentitud en los procesos.

Así mismo, la optimización de la seguridad de los sistemas de información misionales es un proceso que busca la mejora continua de los procesos que se realizan dentro de la ANE. En lo que respecta al mundo de la informática, al momento de implementar políticas de seguridad en un sistema de información, se busca siempre resguardar la información almacenada en ellos a fin de que hagan posible el correcto desenvolvimiento de las actividades de la organización. Los conceptos anteriormente explicados fueron los que dieron paso al diseño de la solución para la problemática del caso estudio.



Es importante para un plan de acción, la seguridad de los sistemas de información misionales que se establezca cuáles son los requerimientos estrictamente necesarios, así mismo, el encargado de implementar el plan de acción es quien le indica a la organización como se pueden manejar los requerimientos, todo ello se hace mediante un correcto levantamiento de información de modo que ambas partes comprendan como se debe desarrollar el plan de acción de seguridad para ataques cibernéticos a fin de que se adapte a las necesidades de la entidad, aplicando a su vez, métodos y técnicas eficientes que perduren a través del tiempo.

Se recalca el establecimiento de los requerimientos ya que además de contribuir a que la seguridad de los sistemas de información misionales perdure en el tiempo, este sirve como fundamento para la implementación del mismo.

Finalmente, el uso de plan de acción de seguridad para ataques cibernéticos representa un aspecto de gran relevancia para la ANE, debido a que se evitara la perdida de información así como también mejorara el desenvolvimiento de los procesos que se llevan a cabo dentro de la entidad.

### **Recomendaciones**

Es importante para la Agencia Nacional del Espectro (ANE) crecer en cuanto a políticas de seguridad para todos los sistemas de información de la entidad, no solo en los sistemas de información misionales, ya que esto permitirá que la entidad ofrezca un servicio especializado a sus clientes, reduciendo los riesgos de pérdida de información producto de ataques cibernéticos, es por ello que se recomienda:

En primer lugar, se recomienda a la Agencia Nacional del Espectro (ANE) evaluar la propuesta del plan de acción, esto con el propósito de resguardar la información almacenada en los sistemas de información misionales. De igual manera, se recomienda evaluar periódicamente la obsolescencia de los equipos.

Así mismo se recomienda implementar el plan de acción dentro de la Agencia Nacional del Espectro (ANE), ya que mejoraría los procesos de la entidad, permitiéndoles resguardar la información almacenada en los sistemas de información misionales.

Igualmente, se recomienda adiestrar al personal encargado de los procesos acerca de los procesos de seguridad existentes dentro de la entidad, esto con el propósito de mejorar constantemente los protocolos de seguridad en los sistemas de información misionales de la entidad.

Para concluir, a próximos investigadores se les recomienda, mejorar el plan de acción propuesto a la Agencia Nacional del Espectro (ANE), esto con el fin de no solo implementarlo a los sistemas de información misionales sino también a los demás sistemas de información existentes dentro de la entidad.



## 9. REFERENCIAS BIBLIOGRÁFICAS

- (INCIBE), E. I. (2017). Los diez mayores ataques informáticos de 2016. *EDeconomiaDigital*, 3. *Agencia Nacional del Espectro*. (s.f.). Obtenido de Agencia Nacional del Espectro.
- Andalucía, J. d. (s.f.). *Junta de Andalucía*. Obtenido de Junta de Andalucía: <http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/656>
- Antonio, E. V. (2015). Safeguard selection for risk management in information systems: a fuzzy approach/Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. *Revista Iberica de Sistemas e Tecnologías de Informacao*, 8 edición.
- Arias, F. (2012). *El Proyecto de Investigación: Introducción a la metodología científica*. 6ta Edición. Caracas: Episteme
- CARDER, A. (2016). *Reglamento General de Protección de Datos (RGPD) de la UE*. IT Governance Publishing.
- CARDER, A. (2017). *ISO27001/ISO27002: Una guía de bolsillo*. IT Governance Publishing.
- Carmona, E. J. (23 de Septiembre de 2013). OCTAVE, metodología para el análisis de riesgos de TI. *OCTAVE, metodología para el análisis de riesgos de TI*, pág. 1.
- Castellanos, F. U. (2014). Metodologías Para el Análisis de Riesgos en los SGSi. *Revista Especializada en Ingeniería*, 76.
- Certificación, I. I. (19 de 08 de 2009). NORMA TECNICA COLOMBIANA NTC-ISO/IEC 27005. *TECNICAS DE SEGURIDAD. GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION*. BOGOTA, COLOMBIA: ICONTEC.
- Comunicaciones, M. d. (07 de 2009). [www.ane.gov.co](http://www.ane.gov.co). Obtenido de [www.ane.gov.co](http://www.ane.gov.co): <http://www.ane.gov.co/index.php/2015-12-08-19-09-22/normas-generales>
- Comunicaciones, M. d. (2016). Seguridad y Privacidad de la Información. *Guia No 7*, 39.

David Lopez, O. P. (2011). Conceptos y enfoques sobre el análisis y la gestión dinámica del riesgo en sistemas de información.

Definición, & de. (2009). <https://definicion.de/>. Obtenido de <https://definicion.de/>: <https://definicion.de/>

E. Vicente, A. M. (2013). Risk analysis in information systems: A Fuzzy approach. *Information Systems and Technologies (CISTI), 2013 8th Iberian Conference on* (pág. 7). Lisboa, Portugal: IEEE.

Electronica, C. S. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid, España: Ministerio de Hacienda y Administraciones Publicas.

Electrónica, C. S. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Espectro, A. N. (2016). [www.ane.gov.co](http://www.ane.gov.co). Obtenido de [www.ane.gov.co](http://www.ane.gov.co): <http://www.ane.gov.co/index.php/about-us/mision-y-vision>

Espectro, A. N. (s.f.). [www.ane.gov.co](http://www.ane.gov.co). Obtenido de [www.ane.gov.co](http://www.ane.gov.co): <http://www.ane.gov.co/index.php/about-us/organigrama>

Galan A., M. (2012). *Investigación Descriptiva*. Obtenido de en: [http://manuelgalan.blogspot.com/2012\\_08\\_26\\_archive.html](http://manuelgalan.blogspot.com/2012_08_26_archive.html)

Helena Alemán Novoa, C. R. (2015). Metodologías Para el Análisis de Riesgos en los SGSi. *Revista especializada en ingeniería*.

ICONTEC. (19 de 08 de 2013). NTC-ISO/IEC 27001. *TECNICAS DE SEGURIDAD. GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN*. Bogotá: ICONTEC.

INCIBE, I. N. (12 de 05 de 2015). *INCIBE*. Obtenido de INCIBE: [HTTPS://WWW.INCIBE.ES](https://www.incibe.es)



- Iso27000. (s.f.). Obtenido de [http://www.iso27000.es/download/doc\\_iso27000\\_all.pdf](http://www.iso27000.es/download/doc_iso27000_all.pdf)
- John Jairo Parafán, M. C. (2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución universidad colegio mayor del cauca*. Popayan.
- Juan Betancurt, R. G. (2016). SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS TRES.
- Juan Esponisa, R. G. (2016). *TESIS DE GRADO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS TRES*.
- Karpesky. (s.f.). *KARPESKY LAB*. Obtenido de <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- LEON, J. G. (2002). *Introduccion al analisis de riesgo*. Mexico D.F: LUMISA S.A.
- Lewis, B. (2018). El estándar internacional clave para la seguridad de la información ISO / IEC 27000. *Organización Internacional para la Estandarización*.
- López, J. L. (Septiembre de 2009). *Análisis forense de sistemas de información*. Barcelona: Eureka Media, SL.
- Lopez, J. R. (Junio 2009). *Desarrollo de un esquema de analisis de vulnerabilidades y pruebas de penetración en sistemas operativos para una organización de la administración publica federal*. Mexico: Instituto Politecnico Nacional.
- MINDEFENSA. (s.f.). *Ministario de defensa nacional de Chile*. Obtenido de Ministerio de defensa nacional de Chile: <http://www.defensa.cl/temas-de-contenido/ciberdefensa/>
- MINTIC. (15 de Marzo de 2016). <http://www.mintic.gov.co>. Obtenido de <http://www.mintic.gov.co>: [http://www.mintic.gov.co/gestionti/615/articulos-5482\\_G5\\_Gestion\\_Clasificacion.pdf](http://www.mintic.gov.co/gestionti/615/articulos-5482_G5_Gestion_Clasificacion.pdf)
- Palella, S. y Martins, F. (2012). *Metodología de la Investigación Cuantitativa*. Caracas: FEDUPEL.

- Ossa, J. W. (2007). *GÓMEZ VIEITES, Álvaro. Enciclopedia de la seguridad informática. México. Alfaomega, 2007. Pág. 11.* Obtenido de GÓMEZ VIEITES, Álvaro. Enciclopedia de la seguridad informática. México. Alfaomega, 2007. Pág. 11: <http://networkingsignora.pbworks.com/f/Unidad%201%20-%20Introduccion%20Seguridad%20Redes.pdf>
- ROBLES, H. L. (2015). *Universidad Nacional Abierta y a Distancia.* Obtenido de Universidad Nacional Abierta y a Distancia: <http://repository.unad.edu.co/handle/10596/3423>
- Ruiz, J. J. (2014). *Universidad Nacional Abierta y a Distancia.* Obtenido de Universidad Nacional Abierta y a Distancia: <https://www.unad.edu.co/>
- Sosa, J. (27 de 01 de 2012). *Análisis de Riesgos.* Obtenido de Análisis de Riesgos: [http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos\\_files/Analisis\\_de\\_Riesgos.pdf](http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf)
- Shuttleworth, M. (2008). *Diseño de la Investigación* obtenido en: <https://explorable.com/es/disenio-de-investigacion-descriptiva> [Consulta: 08 de octubre de 2016]
- T. Vivas, M. A. (2007). *Aplicación de Mecanismos de Seguridad en una Red de Telemedicina Basados. IFMBE Proceeding Vol. 18, 2.*
- Trapaga, A. L. (2015). *Relaciones laborales y nuevas tecnologías de la información y de la comunicación. Una relación fructífera no exenta de dificultades.* Dykinson, S.L.
- UIT. (s.f.). *Actualidades de la UIT.* Obtenido de <http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx>
- Vasquez, K. d. (Octubre de 2013). *Universidad Politecnica Salesiana sede Cuenca.* Obtenido de Universidad Politecnica Salesiana sede Cuenca.
- Vásquez, K. d. (Octubre de 2013). *Universidad Politecnica Salesiana Sede Cuenca.* Obtenido de Universidad Politecnica Salesiana Sede Cuenca: <http://www.ups.edu.ec/sede-cuenca>



Welivesecurite. (17 de 06 de 2013). <https://www.welivesecurity.com/la-es/2013/06/17/nueva-funcionalidad-de-monitoreo-continuo-de-nessus/>. Obtenido de

<https://www.welivesecurity.com/la-es/2013/06/17/nueva-funcionalidad-de-monitoreo-continuo-de-nessus/>: <https://www.welivesecurity.com/la-es/2013/06/17/nueva-funcionalidad-de-monitoreo-continuo-de-nessus/>

Wikipedia. (29 de 12 de 2017). *Wikipedia*. Obtenido de Wikipedia: [https://es.wikipedia.org/wiki/Pruebas\\_de\\_caja\\_gris](https://es.wikipedia.org/wiki/Pruebas_de_caja_gris)

## ANEXOS

## Anexo A: Lista de Chequeo

## Anexo A 1: Lista de chequeo política de seguridad de la información

| Requerimientos  | Controles  | Preguntas   | Respuesta Corta | Detalles/ Comentarios  | Valor | Porcentaje de cumplimiento |
|---|--|---|-----------------|--|-------|----------------------------|
| Orientación de la dirección para la gestión de la seguridad de la información | Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.               | ¿Cuenta con una política de seguridad informática aprobada por la dirección y enfocada a proteger la Confidencialidad, disponibilidad e integridad de la información? | Si              | Sin comentarios  | 100%  | 83%                        |
|   |  | ¿Cómo y con qué frecuencia son comunicadas las políticas de seguridad informática a empleados, subcontratistas, temporales y/o estudiantes en práctica?               | N/A             | No existe una programación para comunicar las políticas. Estas se comunican eventualmente. | 50%   |                            |
|   | Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. | ¿Son actualizadas las políticas de seguridad informática?   | Si              | Sin comentarios  | 100%  |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

## Anexo A 2: Lista de chequeo Organización de la seguridad de la información

| Requerimiento         | Controles  | Preguntas  | Respuesta Corta | Detalles/ Comentarios | Valor | Porcentaje de cumplimiento |
|-----------------------|--|--|-----------------|-----------------------|-------|----------------------------|
| Organización Interna. | Se deben definir y asignar todas las responsabilidades de la seguridad de la información   | ¿Se definen y asignan todas las responsabilidades de la seguridad de la información?   | Si              | Si comentarios        | 100%  | 83.3%                      |
|                       | Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización. | ¿Se separan las tareas y áreas de responsabilidad que estén en conflicto?  | Si              | No siempre            | 50%   |                            |
|                       | Se debe mantener contactos apropiados con las autoridades pertinentes.   | ¿Se mantienen contactos con las autoridades pertinentes para la seguridad de la información?   | Si              | Si comentario         | 100%  |                            |
|                       | Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales   | ¿Se mantiene los controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad? | Si              | Sin comentarios       | 70%   |                            |



|                                     |  |  |    |  |      |  |
|-------------------------------------|--|--|----|--|------|--|
|                                     | especializadas en seguridad  |  |    |  |      |  |
|                                     | La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,                                    | ¿La seguridad de la información se trata en la gestión de proyectos, independiente del tipo de proyecto?                             | Si | Sin comentarios                        | 100% |  |
| Dispositivos Móviles y Teletrabajo. | Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles | ¿Se adoptan políticas y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles? | Si | Si, pero no está funcionado el al 100% | 80%  |  |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

### Anexo A 3: Lista de chequeo seguridad de los recursos humanos

| Requerimiento                   | Controles  | Preguntas  | Respuesta Corta | Detalles/ Comentarios                                    | Valor | Porcentaje de cumplimiento |
|---------------------------------|--|--|-----------------|--|-------|----------------------------|
| Antes de asumir el empleo       | Se recomienda realizar la verificación de antecedentes en todos los candidatos al empleo, contratistas, y usuarios de terceras partes de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos. | ¿Cuenta con políticas, estándares y procedimientos para la selección del personal?   | Si              | Sin Comentarios  | 100%  | 72.7%                      |
|                                 |  | ¿Qué tipo de verificaciones se realizan a los empleados?   | Si              | Antecedentes penales y disciplinario                     | 100%  |                            |
|                                 |  | ¿Cada cuánto actualiza las hojas de vida de los funcionarios, y las verificaciones realizadas?   | Si              | Anualmente se pide actualización                         | 100%  |                            |
|                                 |  | ¿Se realizan verificaciones adicionales para el personal (Ej. Visitas domiciliarias)?  | No              | Sin Comentarios  | 100%  |                            |
|                                 |  | ¿Firman los empleados un convenio de no divulgación o acuerdo de confidencialidad?   | Si              | Sin Comentarios  | 100%  |                            |
|                                 | Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y la de las organizaciones en cuanto a la seguridad de la información.  | ¿En los acuerdos contractuales con empleados y contratistas se establecen responsabilidades de la organización en cuanto a la seguridad de la información? | Si              | Si comentarios   | 100%  |                            |
| Durante la ejecución del empleo | Se recomienda que exista un proceso disciplinario formal para empleados que han perpetrado una violación a la seguridad.   | ¿Se establecen medidas disciplinarias para las personas que no cumplen con las políticas de seguridad?   | Si              | Sin Comentarios  | 100%  |                            |
|                                 | Se recomienda que todos los empleados de la organización y, donde sea relevante, contratistas y usuarios de terceras partes reciban formación adecuada en concientización y actualizaciones regulares  | ¿Tiene un programa formal de capacitación y sensibilización de seguridad relacionada con el sistema de información misionales?                             | Si              | Si, pero el programa está incompleto.                    | 50%   |                            |
|                                 |  | ¿Por qué medios y con qué frecuencia se realiza la concientización de seguridad informática?   | Si              | Correos y medio audiovisual. Se realiza esporádicamente. | 50%   |                            |



|   |  |    |                 |    |
|---|--|----|-----------------|----|
| en políticas y procedimientos organizacionales, relevantes para su función laboral. | ¿En el programa de capacitación y concientización incluye los contratistas, temporales y/o estudiantes en práctica?    | No | Sin Comentarios | 0% |
|   | ¿Cómo le da seguimiento o mide la efectividad del programa de capacitación y concientización de seguridad informática? | No | Sin Comentarios | 0% |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

#### Anexo A 4: Lista de chequeo Gestión de activos

| Requerimiento                   | Controles   | Preguntas   | Respuesta Corta | Detalles/ Comentarios  | Valor | Porcentaje de cumplimiento |
|---------------------------------|---|---|-----------------|--|-------|----------------------------|
| Responsabilidad por los activos | Todos los activos sean claramente identificados y es conveniente que se realice y mantenga un inventario de los activos importantes.        | ¿Mantiene un inventario de hardware, software, información, activos físicos y recursos en donde se procesa la información del Sistema de información misional?                              | Si              | Sin comentarios  | 100%  |                            |
|                                 |   | ¿Con qué frecuencia se revisa y actualiza el inventario de activos?   | N/A             | Anualmente se realiza una revisión.  | 100%  |                            |
| Clasificación de la información | Se recomienda que la información se clasifique en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización. | ¿Cuenta con un esquema de clasificación de la información, en términos de su valor utilizado en el sistema misional?  | No              | Sin comentarios  | 0%    |                            |
|                                 |   | ¿Cuáles son los procedimientos para etiquetar (identificar) los informes?   | N/A             | No existe procedimiento.   | 0%    |                            |
| Manejo de medios                | Se recomienda que existan Procedimientos implementados para la gestión de los medios removibles.  | ¿Tiene procedimientos para la autorización, instalación y administración controlada de medios removibles que puedan utilizarse para copiar información del Sistema de información misional? | No              | Por el modelo de negocio de sistema de información, se hace necesario la utilización de medios removibles. | 50%   | 32%                        |
|                                 |   | ¿Están configurados todos los servidores y estaciones de trabajo para prevenir un <i>boot up</i> desde algún dispositivo periférico?  | No              | Sin comentarios  | 0%    |                            |
|                                 |   | ¿Cuáles son los procedimientos para proteger la información confidencial que se almacena en medios de almacenamiento removibles?  | N/A             | No existen procedimientos  | 0%    |                            |
|                                 | Se recomienda eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.                 | ¿Cuenta con procedimientos de borrado y reutilización de medios?  | Si              | Sin comentarios  | 100%  |                            |
|                                 |   | ¿Está cifrada (encrypted) toda la información digital en tránsito?  | No              | Sin comentarios  | 0%    |                            |
|                                 |   | ¿Cuál es el esquema de cifrado utilizado y servicio de transporte de los medios físicos en tránsito que contienen información confidencial del Sistema de información misional?             | N/A             | No existen esquemas de cifrado para el sistema   | 0%    |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)



## Anexo A 5: Lista de chequeo Control de acceso

| Requerimiento                                 | Controles  | Preguntas   | Respuesta Corta | Detalles/ Comentarios   | Valor | Porcentaje de cumplimiento |
|---|--|---|-----------------|---|-------|----------------------------|
| Requisitos del negocio para control de acceso | Se recomienda establecer, documentar y revisar una política de control de acceso, basada en requisitos de negocio y seguridad de la información. | ¿Existe una política de control de accesos?   | No              | Sin comentarios   | 0%    | 67%                        |
|   |  | ¿Están todos los funcionarios de planta, temporales y subcontratistas identificados por un nombre de usuario único (User ID)?   | Si              | Sin comentarios   | 100%  |                            |
|   |  | ¿En qué casos usan cuentas de usuario (User ID) compartidas?  | N/A             | Sin comentarios   | 100%  |                            |
|   |  | ¿Se desactivan los nombres de usuario (User ID) después de un periodo de inactividad?   | Si              | Sin comentarios   | 100%  |                            |
|   |  | ¿Se usan cuentas con altos privilegios (genéricos o de administración) para la operación de las aplicaciones o recursos que procesan información del Sistema de información misional? | Si              | Sin comentarios   | 100%  |                            |
|   |  | ¿Cómo se controlan las cuentas con altos privilegios usadas en sistemas operativos, bases de datos o que utilizan los procesos automatizados?   | N/A             | actualmente no se controlan las cuentas con privilegios altos | 0%    |                            |
|   |  | ¿Qué controles están implementados para verificar el acceso a los sistemas, bases de datos, redes o plataformas (Ejemplo: ¿declaraciones de responsabilidad, revisión de logs, etc.)? | N/A             | revisión de logs  | 100%  |                            |
|   |  | ¿Se encuentra autorizado, protegido y controlado el acceso a archivos del sistema   | No              | Sin comentarios   | 0%    |                            |
| Gestión de acceso de usuarios                 | Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.                                     | ¿Existe módulo, menú u opción para la administración de usuarios (User IDs), contraseñas y los derechos de acceso?  | Si              | Sin comentarios   | 100%  |                            |
|   | Se recomienda restringir y controlar la asignación y uso de privilegios.   | ¿Existe un procedimiento para otorgar, modificar y/o revocar derechos de acceso?  | No              | Sin comentarios   | 0%    |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

### Anexo A 6: Lista de chequeo Criptografía

| Requerimiento            | Controles  | Preguntas   | Respuesta Corta | Detalles/ Comentarios | Valor | Porcentaje de cumplimiento |
|--------------------------|--|---|-----------------|-----------------------|-------|----------------------------|
| Controles criptográficos | Se recomienda desarrollar una política sobre el empleo de controles criptográficos y establecer una gestión de claves para dar soporte al empleo de técnicas criptográficas. | ¿La aplicación desarrollada utiliza algoritmos de cifrado (encryption)?   | No              | Sin comentarios       | 0%    | 67%                        |
|                          |  | ¿La aplicación usa certificados digitales o soluciones asimétricas de cifrado (public key technology)?  | Si              | Sin comentarios       | 100%  |                            |
|                          |  | ¿Cómo se protegen los archivos de configuración, seguridad y contraseñas de usuarios durante el almacenamiento (ejemplo: cifrado, control de acceso, etc.)? | Si              | Control de accesos    | 100%  |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

### Anexo A 7: Lista de chequeo Seguridad física y del entorno

| Requerimiento | Controles   | Preguntas  | Respuesta Corta | Detalles/ Comentarios           | Valor | Porcentaje de cumplimiento |
|---------------|---|--|-----------------|---------------------------------|-------|----------------------------|
| Áreas seguras | Se recomienda diseñar y aplicar medios de protección física contra daños por incendio, inundación, terremoto, explosión, disturbios civiles, y otras formas de desastre natural o artificial. | ¿Están protegidas las instalaciones con sistemas de alarma o de detección de humo y fuego?   | Si              | Sin comentarios                 | 100%  | 87.5%                      |
|               |   | ¿Están los sistemas contra incendio o alarmas conectados a la central de bomberos o a las autoridades correspondientes?                            | No              | Sin comentarios                 | 0%    |                            |
|               |   | ¿Están protegidas las instalaciones por sistemas automáticos de supresión de fuego (rociadores/gas inerte)?  | Si              | Sin comentarios                 | 100%  |                            |
|               |   | ¿Tiene un generador de energía eléctrica de respaldo y por cuanto tiempo soporta la operación?   | Si              | Soporta un máximo de 30 minutos | 100%  |                            |
| Equipos       | Se recomienda que el equipamiento se ubique o se proteja para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.                   | ¿Existe techo o pisos falsos que puedan ser usados para acceder sin autorización a los centros de datos, cuartos de servidores y/o comunicaciones? | No              | Sin comentarios                 | 100%  | 87.5%                      |
|               |   | ¿Las paredes del exterior de los centros de datos, cuartos de servidores y/o comunicaciones están construidas del piso al techo?                   | Si              | Sin comentarios                 | 100%  |                            |
|               |   | ¿El centro de datos (data center) está identificado desde el exterior?   | No              | Sin comentarios                 | 100%  |                            |
|               |   | ¿Qué controles de accesos existentes en el centro de cómputo?  | Si              | Sin comentarios                 | 100%  |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)



## Anexo A 8: Lista de chequeo Seguridad de operaciones

| Requerimiento                                    | Controles   | Preguntas   | Respuesta Corta | Detalles/ Comentarios  | Valor | Porcentaje de cumplimiento |
|--|---|---|-----------------|--|-------|----------------------------|
| Procedimientos operacionales y responsabilidades | Se recomienda controlar los cambios en los sistemas e instalaciones de procesamiento de información.  | ¿Se cuenta con un procedimiento para control de cambios en los servidores y sistemas de procesamiento?  | No              | Sin comentarios  | 0%    | 69%                        |
|  |   | ¿Se cuenta con el procedimiento de soporte a producción y cambios de emergencia de software en producción?  | No              | Sin comentarios  | 0%    |                            |
|  |   | ¿Cómo mantiene informado a los funcionarios de los cambios críticos que puedan tener un impacto en la prestación del servicio del sistema misional?         | Si              | Con anterioridad se informa por medio del correo institucional o medio audiovisual.                                      | 100%  |                            |
|  | Se recomienda supervisar y adaptar el uso de recursos, así como proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema. | ¿Qué alarmas se han implementado para monitorear el estado de la infraestructura tecnológica, que permitan identificar y corregir las fallas oportunamente? | Si              | Los responsables de cada recurso tecnológico a cargo deben monitorizar continuamente a través de software especializado. | 100%  |                            |
|  | Se recomienda que los recursos para desarrollo, prueba y producción se separen para reducir los riesgos de acceso no autorizado o los cambios al sistema operacional. | ¿Está el ambiente de sistemas en producción segregado, física o lógicamente, de los ambientes de desarrollo de software y realización de pruebas?           | Si              | Sin comentarios  | 100%  |                            |
|  |   | ¿Cómo se protege la información confidencial contra acceso no autorizado en los sistemas de producción, prueba y desarrollo?                                | Si              | Se manejan perfiles de acceso dependiendo de los privilegios a la información  | 100%  |                            |
| Procedimientos operacionales y responsabilidades | Se recomienda que los recursos para desarrollo, prueba y producción se separen para reducir los riesgos de acceso no autorizado o los cambios al sistema operacional. | ¿Está el ambiente de sistemas en producción segregado, física o lógicamente, de los ambientes de desarrollo de software y realización de pruebas?           | Si              | Sin comentarios  | 100%  |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

## Anexo A 9: Lista de chequeo Seguridad de las comunicaciones

| Requerimiento                        | Controles  | Preguntas  | Respuesta Corta | Detalles/ Comentarios | Valor | Porcentaje de cumplimiento |
|--------------------------------------|--|--|-----------------|-----------------------|-------|----------------------------|
| Gestión de la seguridad de las redes | Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.  | ¿Se cuenta con controles de conectividad LAN y WAN?            | Si              | Sin comentarios       | 100%  | 75%                        |
|                                      | Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea | ¿Se tienen ANS en caso de caídas de canales de comunicaciones? | Si              | Sin comentarios       | 100%  |                            |

|                              |   |   |    |                 |      |  |
|------------------------------|---|---|----|-----------------|------|--|
|                              | que los servicios se presten internamente o se contraten externamente.  |   |    |                 |      |  |
|                              | Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.       | ¿La red se encuentra segmentada, de tal forma que se pueda identificar servicios?   | Si | Sin comentarios | 100% |  |
| Transferencia de información | Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. | ¿Se cuenta con políticas y procedimientos para las transferencias de información relacionadas con los sistemas de información misionales? | No | Sin comentarios | 0%   |  |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

#### Anexo A 10: Lista chequeo Adquisición, desarrollo y mantenimiento de sistemas

| Requerimiento  | Controles   | Preguntas  | Respuesta Corta | Detalles/ Comentarios   | Valor | Porcentaje de cumplimiento |
|--|---|--|-----------------|---|-------|----------------------------|
| Requisitos de seguridad de los sistemas de información | Se recomienda que las declaraciones de requisitos de negocio para nuevos sistemas de información, o mejoras a sistemas de información existentes especifiquen los requisitos para controles de seguridad. | ¿Desarrolla sistemas de información o aplicaciones que son integradas con los Sistemas de información misionales?  | Si              | Sin comentarios   | 100%  | 85.7%                      |
|  |   | ¿Cuáles son los requerimientos de seguridad que se solicitan para el desarrollo de software?   | Si              | Sin comentarios   | 100%  |                            |
|  |   | ¿Se hace validación de los datos de entrada para detectar y reducir el riesgo de errores y prevenir ataques estándar, incluyendo desbordamiento de pila (buffer overflow) e inyección de código (code injection)?<br>• ¿Esto se incluye en la metodología de desarrollo de software? | Si              | Sin comentarios   | 100%  |                            |
|  |   | ¿Tiene procedimientos para la revisión de código fuente? ¿En qué parte del ciclo de vida se ejecuta la revisión?   | No              | se hace revisión, pero no se tienen procedimientos establecidos | 0%    |                            |
|  |   | ¿Cómo protegen las herramientas de desarrollo o utilitarios para prevenir acceso no autorizado en producción?  | Si              | Sin comentarios   | 100%  |                            |
|  |   | ¿La información se encuentra en una misma base de datos o servidor común? Si es así, ¿Cómo se mantiene segregada la información?   | No              | Sin comentarios   | 100%  |                            |



|  |  |  |    |   |      |  |
|--|--|--|----|---|------|--|
|  |  | <p>Si las informaciones de los Sistema de información misionales están almacenadas en una base de datos, proporcione los siguientes detalles:</p> <ul style="list-style-type: none"> <li>- Tipo de base de datos y número de versión,</li> <li>- Si la información tiene controles de restricción acceso y/o actualización,</li> <li>- Si la información está almacenada en una base de datos en forma cifrada (encrypted).</li> </ul> | Si | BD SQL Server 2014<br>Tiene controles de perfiles de Acceso<br>La Información no está cifrada | 100% |  |
|--|--|--|----|---|------|--|

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

#### Anexo A 11: Lista de chequeo Relación con los proveedores

| Requerimiento   | Controles  | Preguntas   | Respuesta Corta | Detalles/ Comentarios  | Valor | Porcentaje de cumplimiento |
|---|--|---|-----------------|--|-------|----------------------------|
| Seguridad de la información en las relaciones con los proveedores | Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.                              | ¿Cuántos subcontratistas tiene contratados para el servicio con los Sistemas de información misionales?                           | N/A             | Un contratista   | 100%  | 86%                        |
|   |  | ¿Firman los terceros un convenio de no divulgación o acuerdo de confidencialidad?   | Si              | cada vez que se realiza un contrato se firma el acuerdo de confidencialidad                                | 100%  |                            |
| Seguridad de la información en las relaciones con los proveedores | Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.                              | ¿Qué servicios prestan los subcontratistas existentes?  | N/A             | Mantenimiento y garantía de los sistemas   | 100%  |                            |
|   |  | ¿Qué tipo de información confidencial de los Sistemas de información misionales comparte con los subcontratistas?                 | N/A             | El contratista accede a toda la información registrada en las bases de datos, pero del ambiente de pruebas | 100%  |                            |
|   |  | ¿Qué requerimientos de seguridad informática les solicita a los subcontratistas con los que comparte información confidencial?    | N/A             | Cambio periódico de la clave de acceso a la red de la entidad  | 100%  |                            |
|   |  | ¿Está cifrada la información confidencial que se intercambia de los Sistemas de información misionales o con los subcontratistas? | No              | Sin comentarios  | 0%    |                            |
| Gestión de la prestación de servicios de proveedores              | Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. | Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.      | Si              | Sin comentarios  | 100%  |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

#### Anexo A 12: Lista de chequeo Gestión de incidentes de la seguridad informática

| Requerimiento                         | Controles   | Preguntas  | Respuesta Corta | Detalles/ Comentarios | Valor | Porcentaje de cumplimiento |
|---------------------------------------|---|--|-----------------|-----------------------|-------|----------------------------|
| Gestión de incidentes y mejoras en la | Se recomienda que existan mecanismos establecidos | ¿Existe un procedimiento para reportar, registrar, investigar y escalar incidentes de seguridad informática? | No              | Sin comentarios       | 0%    | 75%                        |



|   |   |   |    |   |      |     |
|---|---|---|----|---|------|-----|
| seguridad de la información                                       | para permitir que los tipos, volúmenes y costos de los incidentes de seguridad informática sean cuantificados y supervisados.   | ¿Existe una lista de contactos de los Sistemas de información misionales con nombres, números de teléfono y siempre disponible para permitir una rápida escalación de incidentes? | Si | Existe la lista, pero no siempre existe disponibilidad de personal para el escalamiento de los incidentes | 100% |     |
| Gestión de incidentes y mejoras en la seguridad de la información | Se recomienda que existan mecanismos establecidos para permitir que los tipos, volúmenes y costos de los incidentes de seguridad informática sean cuantificados y supervisados. | ¿Se toman en cuenta las lecciones aprendidas para futuros incidentes de seguridad?  | Si | Sin comentarios   | 100% | 75% |
|   |   | ¿Se sensibiliza a los funcionarios sobre la importancia de reportar incidentes de seguridad?  | Si | Sin comentarios   | 100% |     |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

### Anexo A 13: Lista chequeo Aspectos de seguridad de la información de la gestión de continuidad del negocio

| Requerimiento                              | Controles  | Preguntas  | Respuesta Corta | Detalles/ Comentarios   | Valor | Porcentaje de cumplimiento |
|--|--|--|-----------------|---|-------|----------------------------|
| Continuidad de seguridad de la información | La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres      | ¿La organización determina los requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres?    | Si              | Si, pero hasta ahora se están determinando                              | 50%   | 52.5%                      |
|  | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa | ¿La organización establece, documenta, implementa y mantiene procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa? | Si              | Si, pero muchos de ellos aún no están documentados                      | 60%   |                            |
|  | La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas          | ¿La organización verifica a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas?        | Si              | Si, pero no lo hace con frecuencia ni se establecen tiempo para hacerlo | 50%   |                            |
| Redundancias                               | Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad  | ¿Las instalaciones de procesamiento de información se implementan con redundancia suficiente para cumplir los requisitos de disponibilidad?  | Si              | Si, pero no lo suficiente   | 50%   |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)



## Anexo A 14: Lista de chequeo Cumplimiento

| Requerimiento                                      | Controles  | Preguntas  | Respuesta Corta | Detalles/ Comentarios                          | Valor | Porcentaje de cumplimiento |
|--|--|--|-----------------|--|-------|----------------------------|
| Cumplimiento de requisitos legales y contractuales | Se recomienda que todos los requisitos estatutarios, reguladores, y contractuales relevantes y el enfoque de la organización para cumplir estos requisitos sean definidos explícitamente, documentados, y mantenidos al día para cada sistema de información y para la organización. | ¿Qué requisitos estatutarios, reguladores y contractuales relevantes aplican para el sistema de información misional?                                | Si              | Ley 743<br>Ley decreto 262<br>Ley 200 del 1995 | 100%  |                            |
|  |  | ¿Se ha evaluado el cumplimiento de los requerimientos (Normatividad) que aplican para el servicio contratado por el Sistema de información misional? | Si              | Sin comentarios                                | 100%  |                            |
| Revisiones de seguridad de la información          | Se recomienda que el enfoque de la organización hacia la gestión de la seguridad informática y su implementación sea revisado independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.                            | ¿Se hacen auditorias para verificar el cumplimiento de las políticas de seguridad informática aplicadas al sistema misional?                         | No              | Sin comentarios                                | 0%    | 33%                        |
|  |  | ¿Se les da tratamiento a las oportunidades de mejora detectadas?   | No              | Sin comentarios                                | 0%    |                            |
|  | Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.                                    | ¿Se realizan revisiones periódicas del cumplimiento de procedimientos del alcance de los SIM?  | No              | Sin comentarios                                | 0%    |                            |
|  | Revisión del cumplimiento técnico  | ¿Se revisa periódicamente para determinar el cumplimiento con las políticas y normas de seguridad información?                                       | No              | Sin comentarios                                | 0%    |                            |

Fuente: Elaboración propia con datos de la norma ISO/IEC 27001 (2013)

## Anexo B: Matriz de riesgo

### Anexo B 1: Identificación riesgo inherente para los activos software de los SIM

| Descripción de la amenaza   | Código | Vulnerabilidades identificadas  | Riesgo   | Probabilidad de materialización de la amenaza | Impacto     |              |       | Nivel de riesgo inherente |
|---|--------|---|--|---|-------------|--------------|-------|---------------------------|
|   |        |   |  |   | Operacional | Reputacional | Legal |                           |
| Abuso de privilegios de acceso  | S-1    | Asignación errada de los derechos de acceso<br>Ausencia de mecanismos de identificación y autenticación de usuario                        | Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios  | 5   | 3           | 4            | 5     | Extremo                   |
| Errores del administrador   | S-2    | Ausencia de procedimiento de control de cambios<br>Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información | Posible fallo en el funcionamiento de la base de datos por error del administrador   | 2   | 3           | 4            | 5     | Alto                      |
| Posible pérdida de disponibilidad de almacenamiento del sistema por falta de recursos | S-3    | Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información  | Caída del sistema por agotamiento de recursos  | 3   | 2           | 1            | 2     | Medio                     |
| Suplantación de la entidad del usuario  | S-4    | Tablas de contraseñas sin protección  | Posible suplantación de usuarios por falta de protección de contraseñas  | 2   | 3           | 4            | 4     | Alto                      |
| Errores de los usuarios   | S-5    | Interfaz de usuario compleja<br>Configuración incorrecta de parámetros<br>Habilitación de servicios innecesarios                          | Posible falta de integridad en el ingreso de la información al sistema   | 4   | 2           | 3            | 3     | Extremo                   |
| Explotación de Vulnerabilidades de los programas (sw)                                 | S-6    | Vulnerabilidades sobre el sistema operativo del servidor de aplicaciones<br>Configuración incorrecta de parámetros                        | Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de estas en los sistemas de información | 2   | 4           | 3            | 4     | Alto                      |
| Abuso de privilegios de acceso  | S-7    | Configuración incorrecta de parámetros<br>SW - Asignación errada de los derechos de acceso  | Posible afectación de la integridad de la configuración del sistema por abuso de privilegios   | 1   | 2           | 1            | 2     | Bajo                      |
| Errores de mantenimiento / actualización de programas (sw)                            | S-8    | SW - Ausencia de control de cambios eficaz  | Posible afectación en la disponibilidad del sistema por actualización de servicios de la aplicación  | 3   | 3           | 3            | 2     | Alto                      |
| Suplantación de la identidad del usuario  | S-9    | RH - Falta de conciencia acerca de la seguridad   | Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario   | 4   | 2           | 3            | 3     | Extremo                   |
| Manipulación de la configuración  | S-10   | SW - Configuración incorrecta de parámetros   | Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración.                                    | 1   | 3           | 3            | 5     | Alto                      |
| Denegación de servicio  | S-11   | SW - Software nuevo o inmaduro  | Posible denegación de servicio por errores en el software  | 3   | 3           | 3            | 2     | Alto                      |



|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  | SW - Ausencia o insuficiencia de pruebas de software |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|

Fuente: Elaboración propia

**Anexo B 2: Identificación riesgo residual para los activos de software de los SIM**

| Cód. | Riesgo   | Control   | Tipo de control | Frecuencia | Ejecución  | Complejidad | Documentación                 | Evidencia            | Recursos      | Valor residual probabilidad | Valor impacto Residual | Riesgo residual |
|------|--|---|-----------------|------------|------------|-------------|-------------------------------|----------------------|---------------|-----------------------------|------------------------|-----------------|
| S-1  | Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios  | Asignación de ID únicos de usuarios y roles     | Preventivo      | Continuo   | Automático | Simple      | Documentado                   | Ninguna              | Suficientes   | 2                           | 4                      | Alto            |
| S-2  | Posible fallo en el funcionamiento de la base de datos por error del administrador   | Rollback a los cambios realizados               | Correctivo      | Esporádico | Manual     | Moderado    | Sin documentar                | Informal             | Regulares     | 2                           | 2                      | Bajo            |
| S-3  | Posible pérdida de disponibilidad de almacenamiento del sistema por falta de recursos  | Liberación de espacio de almacenamiento         | Correctivo      | Esporádico | Manual     | Moderado    | Sin documentar                | Ninguna              | Regulares     | 3                           | 1                      | Bajo            |
| S-4  | Posible suplantación de usuarios por falta de protección de contraseñas  | No hay controles                                | N/A             | N/A        | N/A        | N/A         | N/A                           | N/A                  | N/A           | 2                           | 4                      | Alto            |
| S-5  | Posible falta de integridad en el ingreso de la información al sistema   | Contrato de Mantenimiento y Desarrollo          | Preventivo      | Continuo   | Mixto      | Complejo    | Parcialmente / desactualizado | Física / electrónica | Regulares     | 2                           | 3                      | Medio           |
| S-6  | Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de estas en los sistemas de información | No hay controles                                | N/A             | N/A        | N/A        | N/A         | N/A                           | N/A                  | N/A           | 2                           | 4                      | Alto            |
| S-7  | Posible afectación de la integridad de la configuración del sistema por abuso de privilegios   | Matriz de roles y perfiles                      | Preventivo      | Continuo   | Manual     | Simple      | Parcialmente / desactualizado | Física / electrónica | Regulares     | 1                           | 2                      | Bajo            |
| S-8  | Posible afectación en la disponibilidad del sistema por actualización  | Control de cambios y versionamiento de Software | Preventivo      | Continuo   | Mixto      | Moderado    | Documentado                   | Física / electrónica | Regulares     | 1                           | 3                      | Medio           |
| S-9  | Posible afectación de la confidencialidad e integridad de la información   | Sensibilización en seguridad de la información  | Preventivo      | Esporádico | Manual     | Moderado    | Parcialmente / desactualizado | Física / electrónica | Insuficientes | 3                           | 3                      | Alto            |

|      |  |  |            |          |       |          |             |                      |           |   |   |       |
|------|--|--|------------|----------|-------|----------|-------------|----------------------|-----------|---|---|-------|
| S-10 | Posible afectación en la disponibilidad e integridad de los sistemas por la manipulación de la configuración | No hay controles                       | N/A        | N/A      | N/A   | N/A      | N/A         | N/A                  | N/A       | 1 | 4 | Alto  |
| S-11 | Posible denegación de servicio por errores en el software  | Contrato de Mantenimiento y Desarrollo | Preventivo | Continuo | Mixto | Complejo | Documentado | Física / electrónica | Regulares | 1 | 3 | Medio |

Fuente: Elaboración propia a partir de datos tomados de la política de riesgos ANE (2018)

### Anexo B 3: Identificación de riesgos inherentes de activos tipo Datos de los SIM

| Descripción de la amenaza         | Código | Vulnerabilidades identificadas  | Riesgo  | Probabilidad materialización de la amenaza | Impacto     |              |       | Nivel de riesgo inherente |
|-----------------------------------|--------|---|---|--|-------------|--------------|-------|---------------------------|
|                                   |        |   |   |  | Operacional | Reputacional | Legal |                           |
| Modificación de la información    | D-1    | La información se puede modificar dependiendo de la configuración del perfil de usuario                 | Posible afectación de la integridad por modificación de la información                        | 2  | 3           | 3            | 2     | Medio                     |
| Robo de información               | D-2    | La información del sistema se puede descargar por todos los usuarios                                    | Posible fuga de la información sensible   | 5  | 1           | 4            | 3     | Extremo                   |
|                                   |        | Ausencia de procedimiento formal para la autorización de la información disponible al público           |   |  |             |              |       |                           |
|                                   |        | No hay bloqueos de medios extraíbles  |   |  |             |              |       |                           |
| Corrupción de la información      | D-3    | Falta de conciencia acerca de la seguridad  | Posible afectación de la integridad por corrupción de la información                          | 3  | 2           | 2            | 3     | Medio                     |
|                                   |        | Configuración incorrecta de parámetros  |   |  |             |              |       |                           |
| Errores de los usuarios           | D-4    | RH - Uso incorrecto de software y hardware  | Posible afectación de la disponibilidad e integridad de la información por errores de usuario | 4  | 3           | 2            | 2     | Alto                      |
|                                   |        | SW - Interfaz de usuario compleja   |   |  |             |              |       |                           |
|                                   |        | Falta de capacitación de los funcionarios   |   |  |             |              |       |                           |
| Divulgación de información        | D-5    | RH - Entrenamiento insuficiente en seguridad  | Posible afectación de la confidencialidad de la información                                   | 4  | 4           | 3            | 4     | Extremo                   |
|                                   |        | ORG - Ausencia de procesos disciplinarios definidos   |   |  |             |              |       |                           |
| Introducción de falsa información | D-6    | RH - Falta de conciencia acerca de la seguridad   | Posible afectación de la integridad por introducción de la información                        | 5  | 3           | 4            | 4     | Extremo                   |
|                                   |        | RH - Entrenamiento insuficiente en seguridad  |   |  |             |              |       |                           |
|                                   |        | ORG - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad |   |  |             |              |       |                           |



|                            |     |   |   |   |   |   |   |       |
|----------------------------|-----|---|---|---|---|---|---|-------|
| Destrucción de información | D-7 | SW - Ausencia de copias de respaldo         | Posible afectación de la disponibilidad e integridad de la información por destrucción de información | 2 | 2 | 2 | 2 | Bajo  |
| Espionaje Remoto           | D-8 | RED - Líneas de comunicación sin protección | Posible afectación de la confidencialidad de la información por espionaje remoto                      | 2 | 3 | 3 | 3 | Medio |

Fuente: Elaboración propia

**Anexo B 4: Identificación de riesgos residuales de activos de tipo Datos del SIM**

| Cod. | Riesgo  | Controles  | Tipo de control | Frecuencia | Ejecución | Complejidad | Documentación                 | Evidencia            | Recursos      | Valor residual probabilidad | Valor residual impacto | Riesgo residual |
|------|---|--|-----------------|------------|-----------|-------------|-------------------------------|----------------------|---------------|-----------------------------|------------------------|-----------------|
| D-1  | Posible afectación de la integridad por modificación de la información                        | Estructuración de la matriz de roles y perfiles            | Preventivo      | Esporádico | Manual    | Moderado    | Documentado                   | Física               | Regulares     | 1                           | 3                      | Medio           |
| D-2  | Posible fuga de la información sensible   | Articulación de funcionalidades con el módulo de seguridad | Detectivo       | Esporádico | Manual    | Moderado    | Parcialmente / desactualizado | Informal             | Insuficientes | 1                           | 3                      | Medio           |
| D-3  | Posible afectación de la integridad por corrupción de la información                          | Campañas sobre la seguridad de la información              | Preventivo      | Esporádico | Mixto     | Moderado    | Parcialmente / desactualizado | Física / electrónica | Regulares     | 1                           | 2                      | Bajo            |
| D-4  | Posible afectación de la disponibilidad e integridad de la información por errores de usuario | Campañas periódicas de capacitación                        | Preventivo      | Periódico  | Mixto     | Moderado    | Documentado                   | Física / electrónica | Regulares     | 2                           | 3                      | Medio           |
| D-5  | Posible afectación de la confidencialidad de la información                                   | Circulares internas de la entidad                          | Preventivo      | Continuo   | Mixto     | Moderado    | Documentado                   | Física / electrónica | Suficientes   | 2                           | 4                      | Alto            |
| D-6  | Posible afectación de la integridad por introducción de la información                        | Campañas sobre la seguridad de la información              | Preventivo      | Esporádico | Mixto     | Moderado    | Parcialmente / desactualizado | Física / electrónica | Regulares     | 1                           | 2                      | Bajo            |

|     |   |                     |            |            |       |          |                               |                      |           |   |   |      |
|-----|---|---------------------|------------|------------|-------|----------|-------------------------------|----------------------|-----------|---|---|------|
| D-7 | Posible afectación de la disponibilidad e integridad de la información por destrucción de información | Contrato de backups | Preventivo | Esporádico | Mixto | Moderado | Parcialmente / desactualizado | Física / electrónica | Regulares | 1 | 2 | Bajo |
|-----|---|---------------------|------------|------------|-------|----------|-------------------------------|----------------------|-----------|---|---|------|

Fuente: Elaboración propia

**Anexo B 5: Identificación riesgos inherentes de activos de tipo Personal del SIM**

| Descripción de la amenaza     | Código | Vulnerabilidades identificadas   | Riesgos   | Probabilidad materialización de la amenaza | Impacto     |              |       | Nivel de riesgo inherente |
|-------------------------------|--------|--|---|--|-------------|--------------|-------|---------------------------|
|                               |        |  |   |  | Operacional | Reputacional | Legal |                           |
| Indisponibilidad del personal | P-1    | RH - Ausencia del personal   | Posible fallo en las operaciones del sistema por indisponibilidad de personal   | 5  | 4           | 3            | 3     | Extremo                   |
|                               |        | ORG - Ausencia de autorización de los recursos de procesamiento de la información                |   |  |             |              |       |                           |
|                               |        | ORG - Ausencia de resolución de adopción del grupo de apoyo al sistema de información            |   |  |             |              |       |                           |
| Errores de los usuarios       | P-2    | RH - Entrenamiento insuficiente en seguridad   | Posible error humano en la protección de la Información debido al insuficiente conocimiento y aceptación de las responsabilidades con la seguridad informática. | 3  | 3           | 2            | 2     | Medio                     |
|                               |        | RH - Ausencia de mecanismos de monitoreo   |   |  |             |              |       |                           |
|                               |        | SW - Asignación errada de los derechos de acceso   |   |  |             |              |       |                           |
|                               |        | ORG - Ausencia de procedimientos de identificación y valoración de riesgos                       |   |  |             |              |       |                           |
|                               |        | ORG - Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.                  |   |  |             |              |       |                           |
| Uso no previsto               | P-3    | ORG - Ausencia de procedimiento formal para el registro y retiro de usuarios                     | Posible uso no previsto por parte de los usuarios por ausencia de políticas para el uso de los recursos   | 3  | 3           | 3            | 3     | Alto                      |
| Destrucción de información    | P-4    | RH - Uso incorrecto de software y hardware   | Posible afectación en equipos o archivos por uso incorrecto de hardware y software  | 1  | 3           | 4            | 4     | Medio                     |
| Robo                          | P-5    | RH - Trabajo no supervisado del personal externo o de limpieza                                   | Posible robo de equipos e información por falta de supervisión de personal  | 4  | 2           | 3            | 3     | Extremo                   |
|                               |        | RH - Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería |   |  |             |              |       |                           |
|                               |        | SW - Asignación errada de los derechos de acceso   |   |  |             |              |       |                           |



|   |     |  |  |   |   |   |   |       |
|---|-----|--|--|---|---|---|---|-------|
| Extorsión o presión mediante amenazas, Afectación a la confidencialidad, integridad o disponibilidad de los sistemas de información | P-6 | RH - Ausencia de mecanismos de monitoreo   | Posible afectación a la confidencialidad, integridad o disponibilidad de los sistemas por extorsión o presión mediante amenazas  | 2 | 4 | 3 | 4 | Alto  |
| Ingeniería social o abuso de la buena fe, Obtención de información  | P-7 | RH - Falta de conciencia acerca de la seguridad  | Posible obtención de información mediante ingeniería social o abuso de la buena fe   | 3 | 2 | 2 | 3 | Medio |
|   |     | RH - Entrenamiento insuficiente en seguridad   |  |   |   |   |   |       |
| Deficiencias en la organización   | P-8 | RH - Falta de conciencia acerca de la seguridad  | Posible deficiencia en el tratamiento de la Información al interior de la entidad debido a la falta de una coordinación encargada de velar por la seguridad informática. | 3 | 2 | 4 | 3 | Alto  |
|   |     | ORG - Ausencia de la resolución de adopción de las políticas de seguridad de la información. |  |   |   |   |   |       |

Fuente: Elaboración propia

**Anexo B 6: Identificación riesgos residuales de activos de tipo Personal del SIM**

| Cód. | Riesgos   | Controles   | Tipo de control | Frecuencia | Ejecución | Complejidad | Documentación                 | Evidencia            | Recursos    | Valor Probabilidad Residual | Valor Impacto Residual | Riesgo residual |
|------|---|---|-----------------|------------|-----------|-------------|-------------------------------|----------------------|-------------|-----------------------------|------------------------|-----------------|
| P-1  | Posible fallo en las operaciones del sistema por indisponibilidad de personal   | Circulares internas y manual de funciones haciendo alusión al uso obligatorio del Sistema | Preventivo      | Continuo   | Manual    | Simple      | Documentado                   | Física / electrónica | Suficientes | 1                           | 3                      | Medio           |
| P-2  | Posible error humano en la protección de la Información debido al insuficiente conocimiento y aceptación de las responsabilidades con la seguridad informática. | Estructuración de la Matriz de Roles y Perfiles   | Correctivo      | Esporádico | Manual    | Complejo    | Parcialmente / desactualizado | Física / electrónica | Regulares   | 3                           | 1                      | Bajo            |
| P-3  | Posible uso no previsto por parte de los usuarios por ausencia de políticas para el uso de los recursos   | No existe control   | N/A             | N/A        | N/A       | N/A         | N/A                           | N/A                  | N/A         | 3                           | 3                      | Alto            |

|     |  |  |            |            |       |          |                               |                      |             |   |   |       |
|-----|--|--|------------|------------|-------|----------|-------------------------------|----------------------|-------------|---|---|-------|
| P-4 | Posible afectación en equipos o archivos por uso incorrecto de hardware y software   | Configuraciones de equipos según tipo de usuario                         | Preventivo | Periódico  | Mixto | Moderado | Parcialmente / desactualizado | Física / electrónica | Regulares   | 1 | 4 | Medio |
| P-5 | Posible robo de equipos e información por falta de supervisión de personal   | Controles de Acceso, cámaras de seguridad y Políticas para uso de correo | Preventivo | Continuo   | Mixto | Moderado | Parcialmente / desactualizado | Física / electrónica | Regulares   | 1 | 3 | Medio |
| P-6 | Posible afectación a la confidencialidad, integridad o disponibilidad de los sistemas por extorsión o presión mediante amenazas  | Manual de funciones de la entidad y Decreto 262 de 2000, Ley 734 2002    | Preventivo | Continuo   | Mixto | Moderado | Documentado                   | Física / electrónica | Regulares   | 1 | 3 | Medio |
| P-7 | Posible obtención de información mediante ingeniería social o abuso de la buena fe   | Jornadas extemporáneas en seguridad Informática                          | Preventivo | Esporádico | Mixto | Moderado | Documentado                   | Física / electrónica | Regulares   | 1 | 2 | Bajo  |
| P-8 | Posible deficiencia en el tratamiento de la Información al interior de la entidad debido a la falta de una coordinación encargada de velar por la seguridad informática. | Solicitudes a la alta dirección acerca del tema                          | Correctivo | Continuo   | Mixto | Complejo | Documentado                   | Física / electrónica | Suficientes | 3 | 1 | Bajo  |

Fuente: Elaboración propia

**Anexo B 7: Identificación riesgos Inherentes del escaneo de los SIM**

| Descripción de la amenaza                        | Código | Vulnerabilidades identificadas  | Riesgos  | Probabilidad materialización de la amenaza | Impacto     |              |       | Nivel de riesgo inherente |
|--|--------|---|--|--|-------------|--------------|-------|---------------------------|
|  |        |   |  |  | Operacional | Reputacional | Legal |                           |
| Ataques avanzados de usuarios maliciosos         | W-1    | Ausencia de configuración de permisos a archivos de configuración           | Posible robo o pérdida de información sensible debido a un archivo de configuración que se encuentra en el directorio de configuración | 3  | 3           | 4            | 3     | Alto                      |
|  |        | Asignación errada de los derechos de acceso a los archivos de configuración |  |  |             |              |       |                           |
| Ataques de negación de servicios al servidor web | W-2    | Entrenamiento insuficiente en seguridad                                     | Posible bloqueo o indisponibilidad del servidor web donde se encuentra alojado el SIM  | 3  | 3           | 2            | 2     | Medio                     |
|  |        | Ausencia de mecanismos de monitoreo   |  |  |             |              |       |                           |
|  |        | Ausencia de buen ancho de banda para los SIM                                |  |  |             |              |       |                           |
|  |        | Ausencia de la configuración de un proxy                                    |  |  |             |              |       |                           |
|  |        | Ausencia de actualización oportuna de parches al servidor                   |  |  |             |              |       |                           |



|   |     |   |   |   |   |   |   |       |
|---|-----|---|---|---|---|---|---|-------|
| Aplicación Técnica del Phishing                           | W-3 | Falta de configuración de las cabeceras X-frame-Options en el servidor WEB                            | Posible robo de información debido a técnicas maliciosas                                    | 2 | 2 | 2 | 3 | Baja  |
| Aplicación método del CSRF                                | E-1 | Ausencia de protección CSRF en un formulario HTML del sistema   | Posible robo de información debido al método CSRF   | 2 | 3 | 2 | 4 | Medio |
| Ataques de negación de servicios al servidor web          | E-2 | Entrenamiento insuficiente en seguridad   | Posible bloqueo o indisponibilidad del servidor web donde se encuentra alojado el sitio Web | 4 | 3 | 3 | 3 | Alto  |
|   |     | Ausencia de mecanismos de monitoreo   |   |   |   |   |   |       |
|   |     | Ausencia de buen ancho de banda para los SIM  |   |   |   |   |   |       |
|   |     | Ausencia de la configuración de un proxy  |   |   |   |   |   |       |
| Ausencia de actualización oportuna de parches al servidor |     |   |   |   |   |   |   |       |
| Ataques a usuario final y operacional del aplicativo web  | E-3 | Desactualización de la versión PHP que se ejecuta en el servidor donde se encuentra la aplicación web | Posible afectación de datos de los usuarios finales y operación de la aplicación web        | 2 | 3 | 4 | 2 | Alto  |

Fuente: Elaboración propia

**Anexo B 8: Identificación de riesgos residuales Escaneo de los SIM**

| Cód. | Riesgos  | Controles   | Tipo de control | Frecuencia | Ejecución         | Complejidad | Documentación                 | Evidencia            | Recursos    | Valor Probabilidad Residual | Valor Impacto Residual | Riesgo residual |
|------|--|---|-----------------|------------|-------------------|-------------|-------------------------------|----------------------|-------------|-----------------------------|------------------------|-----------------|
| W-1  | Posible robo o pérdida de información sensible debido a un archivo de configuración que se encuentra en el directorio de configuración | Eliminar o restringir el acceso a todos los archivos de configuración       | Preventivo      | Continuo   | Manual            | Simple      | Documentado                   | electrónica          | Suficientes | 2                           | 3                      | Medio           |
| W-2  | Posible bloqueo o indisponibilidad del servidor web donde se encuentra alojado el SIM  | Configuración de proxy, ampliación ancho de banda, actualización de parches | Preventivo      | Continuo   | Manual/Automático | Complejo    | Desactualizado                | Electrónica          | Regulares   | 2                           | 2                      | Bajo            |
| W-3  | Posible robo de información debido a técnicas maliciosas   | Configurar el servidor web para incluir una cabecera X-Frame-Options        | Preventivo      | Esporádica | Mixto             | Complejo    | Desactualizado                | Electrónica          | Suficientes | 1                           | 2                      | Bajo            |
| E-1  | Posible robo de información debido al método CSRF  | Instalar token  | Preventivo      | Continuo   | Mixto             | Simple      | Parcialmente / desactualizado | Física / electrónica | Suficientes | 1                           | 3                      | Medio           |
| E-2  | Posible bloqueo o indisponibilidad del servidor web donde se encuentra alojado el aplicativo Web                                       | Configuración de proxy, ampliación ancho de banda, actualización de parches | Preventivo      | Continuo   | Manual/Automático | Complejo    | Desactualizado                | Electrónica          | Regulares   | 2                           | 3                      | Medio           |

|     |  |  |            |          |       |          |             |                      |            |   |   |       |
|-----|--|--|------------|----------|-------|----------|-------------|----------------------|------------|---|---|-------|
|     |  |  |            |          |       |          |             |                      |            |   |   |       |
| E-3 | Posible afectación de datos de los usuarios finales y operación de la aplicación web | Actualización de la versión de PHP a la última versión | Preventivo | Continuo | Mixto | Moderado | Documentado | Física / electrónica | Suficiente | 2 | 3 | Medio |

Fuente: Elaboración propia



"TOMA: RUEDA VARGAS"



201002301