ANALISIS Y EVALUACIÓN DE RIESGOS DE LA INFORMACIÓN EN LAS OFICINAS DE COMFAORIENTE SECCIONAL PAMPLONA BASADO EN LA NORMA ISO/IEC 27000:2013

JORGE ENRIQUE ARAQUE ISIDRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA
2018

ANÁLISIS Y EVALUACIÓN DE RIESGOS DE LA INFORMACIÓN EN LAS OFICINAS DE COMFAORIENTE SECCIONAL PAMPLONA BASADO EN LA NORMA ISO/IEC 27000:2013

ING. JORGE ENRIQUE ARAQUE ISIDRO

Proyecto aplicado presentado como requisito de para optar por el título de Especialista en Seguridad Informática

Director
ING. JORGE ENRIQUE RAMÍREZ MONTAÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA
2018

DEDICATORIA

Dedico mi trabajo a mis padres quienes me han dado su apoyo cariño y comprensión para que se llevaran mis metas a cabo.

AGRADECIMIENTOS

Mis agradecimientos a mis padres por brindarme el apoyo y oportunidad de poder estudiar para ser mejor profesionalmente.

Sinceros agradecimientos a ComfaOriente por permitirme realizar este trabajo en sus instalaciones.

Sinceros agradecimientos a los docentes y tutores de la UNAD por hacer parte de mi formación en esta especialización, en especial al docente Jorge Enrique Ramírez Montañez por su paciencia y colaboración.

CONTENIDO

Pág.

INTRODUCCION....1
1. TITULO....3
2. FORMULACIÓN DEL PROBLEMA....4
2.1. ANTECEDENTES DEL PROBLEMA....4
2.2. FORMULACIÓN DEL PROBLEMA. 4
2.3. DESCRIPCIÓN DEL PROBLEMA....5
2.3.1. Limitaciones....5
2.3.2. Alcances....5
3. JUSTIFICACIÓN....7
4. OBJETIVOS....8
4.1. OBJETIVO GENERAL....8
4.2. OBJETIVOS ESPECÍFICOS....8
5. MARCO REFERENCIAL....9
5.1. MARCO DE ANTECEDENTES....9
5.2.1. Reseña Histórica, Caja de Compensación Familiar COMFAORIENTE. 13
5.2.2. Organización de la empresa....15
5.3. MARCO TEÓRICO....15
5.3.1. Activos de Información....15
5.3.2. Seguridad de la información....17
5.3.3. Gestión de seguridad....17
5.3.4. Análisis y Evaluación de Riesgos de Seguridad de la Información....18
5.3.5. Las acciones definidas para el tratamiento de los riesgos....20

5.3.6. MAGERIT. (Metodología de análisis y Gestión de Riesgos de los Sistemas de Información) 21
5.3.7. Ciclo de Deming....22
5.3.8. Sistema de Gestión de Seguridad de la Información 24
5.3.9. Evaluación de riesgos 26
5.3.10. Modelo de gobierno y gestión para las Tecnologías de la información y de la comunicación 26
5.3.11. Auditoría Informática....28
5.4. METODOLOGÍA DE EVALUACIÓN DEL RIESGO....28
5.4.1. Análisis de Riesgos....28
5.4.2. Matriz para el análisis de riesgo....30
5.5. PLANIFICACIÓN DEL ANÁLISIS Y EVALUACIÓN DE RIESGOS DE LA SEGURIDAD INFORMÁTICA EN COMFAORIENTE SEDE PAMPLONA, SIGUIENDO PARÁMETROS DE LA NORMA ISO 27001 34
5.5.1. Alcance del análisis y evaluación de riesgos 34
5.5.2. Métodos para la búsqueda de información 34
5.5.3. Observación directa....34
5.5.4. Entrevista....35
5.5.5. Ethical Hacking y Pentesting (Pruebas de penetración) 35
5.5.6. Población y Muestra 35
5.5.7. Diseño de la muestra....35
5.6. MARCO CONCEPTUAL 36
5.7. MARCO LEGAL 40
6. DISEÑO METODOLÓGICO 42
6.1. TIPO DE INVESTIGACIÓN 42
6.2. METODOLOGÍA DE DESARROLLO 42
6.3 DEFINICION DE HIPOTESIS 44
6.4. POBLACIÓN Y MUESTRA....45

6.5. TÉCNICAS DE RECOLECCIÓN DE DATOS 45
6.6. INSTRUMENTOS DE RECOLECCION DE DATOS 46
7. ESQUEMA TEMATICO 47
7.1. ACTIVOS, VULNERABILIDADES, AMENAZAS E IMPACTOS.....47
7.1.1. Inventario de los Activos 47
7.1.2. Valoración de los Activos 49
7.2. ANÁLISIS DE VULNERABILIDADES 50
7.2.1. Análisis a los sistemas operativos 50
7.2.2. Resultados y vulnerabilidades encontradas.....50
7.2.3. Análisis al Recurso Humano 50
7.2.4. Inventario de los equipos y recursos relacionados con el manejo del sistema de información 51
7.3 ANÁLISIS DE VULNERABILIDADES 52
7.3.1 Análisis a los sistemas operativos 52
7.3.2. Resultados y vulnerabilidades encontradas.....52
7.3.3. Análisis al Recurso Humano 52
7.4. DESCRIBIR LA INFRAESTRUCTURA TECNOLÓGICA PRESENTE EN LA ORGANIZACIÓN. 54
7.4.1. Centros De Datos 54
7.4.3. Servidores.....56
7.4.4. Servidor de archivo 56
7.4.5. Servidor de Impresión. 57
7.4.6. Servidor Web. 57
7.4.7. Servidor de Aplicaciones. 57
7.4.8. Servidor de Correo.....57
7.4.9. Servidor de Bases de Datos. 57
7.4.10. Servidor de Medios. 57

7.4.11. Servidor de Colaboración. 57
7.4.12. Clientes. 57
7.4.13. Dispositivos de Red 58
7.4.14. Swtich. 58
7.4.15. Access Point. 58
7.4.16. Router. 59
7.4.17. Medios de Comunicación. 59
7.4.18. Cable. 60
7.4.19. Inalámbrico. 60
7.4.20. Tipos de Redes. 60
7.4.21. LAN. 60
7.4.22. Backbone. 61
7.4.23. MAN. 61
7.4.24. WAN. 61
7.4.25. Intranet. 61
7.4.26. Extranet. 61
7.5. INFRAESTRUCTURA TECNOLÓGICA DE COMFAORIENTE 61
7.6. EJECUTAR UN HACKING ÉTICO A LOS SISTEMAS DE INFORMACIÓN PARA ESTABLECER VULNERABILIDADES. 62
7.7. ESTABLECER UN CONJUNTO DE CONTROLES QUE PERMITAN CONTRARRESTAR LAS FALENCIAS ENCONTRADAS EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN. 81
7.7.1. Relación de las vulnerabilidades y amenazas detectadas. 81
7.7.2. Matriz para el análisis de riesgo. 81
7.7.3. Matriz de clasificación del riesgo. 82
7.7.4. Clasificación del riesgo. 83
7.8. PLAN DE TRATAMIENTO DE RIESGOS 84
7.8.1. ISO 27002. Código de buenas prácticas. 84

7.8.2Controles. 87
7.8.3. Acción de mitigación del riesgo.....88
7.8.4. Periodicidad de la acción de mitigación. 88
7.8.5. Seguimiento del riesgo. 88
7.8.6. Por qué implementar controles. 88
7.8.7. Estructuración completa del plan de tratamiento. 89
8. PROPONENTES 93
8.1. PROPONENTES PRIMARIOS 93
8.2. PROPONENTES SECUNDARIOS 93
9. RECURSOS DISPONIBLES 94
9.1. RECURSOS.....94
9.1.1. Recursos Materiales. 94
9.1.2. Recursos Institucionales. 94
9.1.3. Presupuesto.....94
10. CRONOGRAMA PROPUESTO INICIAL 95
11. RESULTADOS ESPERADOS 96
12. CONCLUSIONES 97
RECOMENDACIONES.....98
BIBLIOGRAFIA.....100
ANEXOS.....103

LISTA DE TABLAS

Pag.

Tabla 1. Inventario de los Activos COMFAORIENTE sede Pamplona. 47
Tabla 2. Criterio para valoración de activos 49
Tabla 3. Encuesta al personal para determinar vulnerabilidades 50
Tabla 4. Criterio para valoración de activos 52
Tabla 5. Resultados de la encuesta 53
Tabla 6. Cronograma 95

LISTA DE FIGURAS

Pag.

Figura 1. Organigrama institucional 15
Figura 2. Activos de la información 16
Figura 3. Ciclo de Deming.....23
Figura 4. Plan análisis del riesgo ISO 27001 30
Figura 5. Matriz para análisis de riesgo 31
Figura 6. Interpretación de la matriz para análisis de riesgo.....33
Figura 7. Fases de la norma ISO 27005 43
Figura 8. Nagios.....55
Figura 9. Componentes de una LAN.....56
Figura 10. Switch 58
Figura 11. Access Point 59
Figura 12. Router 59
Figura 13. Diagrama de la infraestructura TI.....62
Figura 14. Interfaz Network Scanner 66
Figura 15. Rango de IPs 67
Figura 16. Resultado del escaneo 68
Figura 17. Workstation Network Scanner.....69
Figura 18. Additional Network Scanner.....69
Figura 19. General Network Scanner.....70
Figura 20. Browsing Network Scanner.....70
Figura 21. Interfaz Modem ADSL.....71
Figura 22. Resultado escaneo carpetas compartidas 71
Figura 23. Desactivar NetBIOS paso 1 72
Figura 24. Desactivar NetBIOS paso 2 73
Figura 25. Desactivar NetBIOS paso 3 73
Figura 26. Desactivar NetBIOS paso 4 74
Figura 27. Desactivar NetBIOS paso 5 74
Figura 28. Interfaz Nmap 76
Figura 29. Topología Nmap 76
Figura 30. Nmap Output.....77
Figura 31. Ports/Hosts Nmap.....77

Figura 32. Host Details.....78
Figura 33. DO tratamiento de los Riesgos 86
Figura 34. Tratamiento de los riesgos.....87
Figura 35. Modelo del plan para el tratamiento del riesgo 89

LISTA DE CUADROS

Pag.

Cuadro 1. Matriz para el análisis de riesgo 82
Cuadro 2. Matriz de clasificación del riesgo 83
Cuadro 3. Clasificación de los riesgos encontrados 83
Cuadro 4. Controles 90

RESUMEN

Las oficinas de COMFAORIENTE seccional Pamplona cuentan con una infraestructura tecnológica para cumplir su trabajo como caja de compensación familiar y otros servicios que presta. De esta forma cuenta con equipos de cómputo en donde se puede ingresar a una plataforma en donde se realiza todos los procesos que esta entidad lleva a cabo subiendo la información a bases de datos.

La información que se recolecta tiene como principal objetivo que llegue a la central de las oficinas en Cúcuta, Norte de Santander, las cuales son las encargadas de manejar la seguridad de la información en la seccional Pamplona. Debido a esto no se realizan revisiones periódicas sino cuando ya se presenta algún problema.

Debido a esto se deben realizar algunas recomendaciones y controles para evitar la pérdida o fuga de información que perjudique a la caja de compensación y a los usuarios de la misma.

Por lo que mediante un análisis y evaluación de riesgos se tendrá en cuenta la seguridad existente y sus falencias, para esto se tienen en cuenta la observación a los equipos y el manejo de los mismos, así como la información prestada por funcionarios encargados de los sistemas informáticos mediante entrevistas que pretenden establecer numerosos factores que intervienen como vulnerabilidades, amenazas, entre otros.

ABSTRACT

The offices of COMFAORIENTE sectional Pamplona have a technological infrastructure to fulfill their work as a family compensation fund and other services provided. In this way, it has computer equipment in which it is possible to enter a platform where all the processes carried out by this entity are carried out by uploading the information to databases.

The main objective of the information that is collected is that it reaches the headquarters of the offices in Cúcuta, Norte de Santander, which are in charge of managing the security of information in the Pamplona branch. Due to this, periodic reviews are not made until a problem has already occurred.

Due to this, some recommendations and controls must be made to avoid the loss or leakage of information that harms the compensation box and the users of it. Therefore, through an analysis and evaluation of risks, the existing security and its shortcomings will be taken into account, for this, the observation of the equipment and the management of the same, as well as the information provided by officials in charge of the systems, are taken into account. computer networks through interviews that seek to establish numerous factors that intervene as vulnerabilities, threats, among others

INTRODUCCION

Los sistemas de la información son la base de todas las empresas e instituciones, estos llevan el nivel de responsabilidad más alto debido a su importancia debido a lo que puede aportar y soportar estos sistemas que manejan la información.

En Colombia la gran mayoría de empresas, negocios e instituciones tiene plataformas de comunicación y redes que sirven para el intercambio y flujo de información muy importante para el funcionamiento de cada una de ellas, las cuales no cuentan con seguridad de la información para proteger sus negocios.

El manejo que se le da a la información en las diferentes organizaciones es determinante para la protección de la misma y esto se ve reflejado en diferentes aspectos que van desde los medios físicos como lo son los procesos de gestión documental, hasta los sistemas de información de la organización o externos a los que tenga que reportar información, como por ejemplo el almacenamiento de datos, respaldos, planes de contingencia, entre otros.

Por lo que para este trabajo se tomó como base de análisis COMFAORIENTE, que es una caja de compensación familiar, en la cual dentro de su accionar debe enfocar sus procesos de sistemas de información a la protección de la misma debido a la gran cantidad de clientes con los que cuentan y las sedes que maneja ya que en ella se dictan cursos y tienen un colegio de preescolar.

Para esto se tienen en cuenta la observación a los equipos y el manejo de los mismos, así como la información prestada por funcionarios encargados de los sistemas informáticos mediante entrevistas que pretenden establecer numerosos factores que intervienen como vulnerabilidades, amenazas, entre otros.

Se conforma en la primera parte por las generalidades que componen una propuesta de investigación, pasando al segundo capítulo donde se procede a conocer la parte teórica del proyecto, en el marco referencial que incluye los principales términos a utilizar en el tipo de estudios, los marcos legales y la información de teorías sobre el tema; si como la descripción de la empresa, en el

tercer capítulo se explica de manera rigurosa la metodología a utilizar para realizar la investigación para en el último capítulo detallar el análisis de los instrumentos de recolección y dar los resultados encontrados, además de las recomendaciones para posibles soluciones.

1. TITULO

ANALISIS Y EVALUACIÓN DE RIESGOS DE LA INFORMACIÓN EN LAS OFICINAS DE COMFAORIENTE SECCIONAL PAMPLONA BASADO EN LA NORMA ISO/IEC 27001:2013

Área conocimiento: Seguridad informática

Línea de investigación: Análisis y riesgo de seguridad información con ISO 27000:2013

2. FORMULACIÓN DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

En la gran mayoría de las oficinas que se dedican a diferentes tipos de actividades podemos encontrar equipos de cómputo y demás accesorios para oficina que facilitan los procesos que se ejecutan y de esta forma agilizan el trabajo de las personas. Este tipo de herramientas tecnológicas que han surgido al pasar el tiempo y han sido mejoradas requieren de ciertas características y especificaciones para ser controladas y administradas para su mejor funcionamiento y aprovechamiento, para este tipo de operaciones se requiere que se tenga una red o redes internas que comuniquen toda la oficina.

Aparte de estas redes internas es casi indispensable que una oficina hoy en día cuente con conexión a internet la cual ofrece muchos beneficios a la hora de la comunicación bien sea dentro de la oficina o en otras ubicadas en la misma ciudad o en otras y la obtención de información al instante y sin pérdidas de tiempo.

Para realizar la conexión a internet a los equipos que se encuentran en las oficinas existen dos tipos que son las más comunes las cuales son por cable y por WiFi (LAN y WLAN), cada una de ellas en su utilización tiene sus puntos a favor y en contra. Al utilizar todos estos medios de comunicación, para hacer de las tareas de la oficina, acciones más rápidas y eficientes, también se pueden presentar algunos problemas de seguridad de la información debido a que se abren muchos posibilidades de acceso a los datos que se manejan, por lo que si no se toman medidas de prevención se puede llegar a perder información o se puede presentar robo de la misma por personas ajenas a esta o los mismos funcionarios.

2.2. FORMULACIÓN DEL PROBLEMA.

¿De qué manera mediante un análisis y evaluación de riesgos aplicando la ISO 27000, es posible mejorar el panorama de la seguridad informática en las oficinas de la empresa COMFAORIENTE de la ciudad Pamplona?

2.3. DESCRIPCIÓN DEL PROBLEMA

COMFAORIENTE, es una empresa privada que cumple funciones de caja de compensación familiar en el Norte de Santander, a parte de estas funciones, esta institución presta servicios de formación académica en la seccional de Pamplona, Norte de Santander, cuenta con cursos de diferentes áreas y también con un jardín infantil.

Para el manejo de todos estos servicios poseen varias oficinas, las cuales tienen un sistema interno para la comunicación en intercambio de información entre las diferentes dependencias de la misma. Así las cosas, La red interna de las oficinas, no cuenta con una normalización o regulación a la hora de su utilización para proteger la información que se maneja, esta información es vulnerable al ataque de cualquier índole, este riesgo se hace más evidente ya que dentro de estas oficinas se encuentra una sala de cómputo para las personas afiliadas a esta empresa o que lleven a cabo cursos en la misma y este recurso es compartido junto con las demás áreas de la institución.

Por lo anterior, es necesario realizar un análisis y evaluación de riesgos de la información para evidenciar y proponer soluciones a los diferentes problemas técnicos; lo que conllevara a proteger la información de la institución y por tanto de las personas que pertenecen a la misma, y así COMFAORIENTE en la seccional Pamplona podrá brindar mayor confiabilidad de sus servicios a las personas que pertenecen a la institución.

2.3.1. Limitaciones. Se notan como limitaciones, la imposibilidad de acceder a las bases de datos más importantes que se analizan ya que es imposible que COMFAORIENTE como institución prestadora de servicio permita a un particular conocer a fondo estos datos por lo importante de ellos y clasificados.

2.3.2. Alcances. El Sistema de Gestión de Calidad en COMFAORIENTE se rige por los requisitos planteados en la Norma NTC ISO 9001-2008 y abarca los

procesos de prestación de servicio: Prestación de servicios de afiliación, aportes y subsidios, Multibanco de servicios, crédito, vivienda, Fovis y Cavis. Fondo de promoción al empleo y protección al desempleado.

Planeación y proyectos, Programas especiales tales como: amigos y sonrisas, sala cuna y guardería, biblioteca fija y biblioteca viajera, centro de atención a niños discapacitados, programas para la tercera edad. Servicios sociales, centro recreacional villa Silvana, Club ejecutivo, Institución educativa para el trabajo y el desarrollo humano.

Prestación de servicios de educación para el trabajo y el desarrollo humano en áreas administrativas, comerciales, de seguridad ocupacional, sistemas de información, artes, diseño gráfico, confecciones, mantenimiento electrónico, estética y belleza. Diseño y prestación de servicio educativo en los ciclos de preescolar, primaria y bachillerato Estos servicios son prestados en la Sede principal, ubicada en la Avenida 2 Calle 14 No 13-75 Barrio La Playa en Cúcuta y en la sede de la Guardería Pasitos ubicada en la Calle 16 No. 1-21 Barrio La Playa, centro recreacional villa Silvania Km 3 vía Bocono.

3. JUSTIFICACIÓN

Este trabajo de grado tuvo como propósito realizar un análisis y evaluación de riesgos de la información en la empresa COMFAORIENTE con el fin de que sus directivos conozcan las vulnerabilidades que se tienen en la red interna de sus oficinas y se materializan las amenazas.

Como parte del Sistema de Gestión de Seguridad de la Información, es necesario para la empresa hacer una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer y complementar las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información lo cual es el objetivo en este proyecto.

Este análisis y evaluación de riesgos de la información se realizará bajo la norma ISO/IEC 27001:2013 para que se garantice las buenas prácticas en el manejo de la información y se minimicen los riesgos de perdida y robo de información que afecte a COMFAORIENTE.

Se busca con este trabajo que las personas que trabajan en estas oficinas se den cuenta de que ellos son el componente más importe de la seguridad de la información en su institución, debido a que son los que permanentemente se encuentran en contacto con la misma y al mismo tiempo la pueden modificar.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Realizar un análisis y evaluación de riesgos de la información que gestiona la oficina de COMFAORIENTE seccional Pamplona, siguiendo la norma ISO/IEC 27000:2013 para el hallazgo de vulnerabilidades y amenazas y así proponer políticas de buenas prácticas de la seguridad informática.

4.2. OBJETIVOS ESPECÍFICOS

1. Realizar un diagnóstico en la infraestructura tecnológica en la oficina de COMFAORIENTE seccional Pamplona para documentar el panorama actual de la seguridad de la información.

2. Ejecutar un inventario de los equipos y recursos relacionados con el manejo del sistema de información en las oficinas de COMFAORIENTE seccional Pamplona.

3. Realizar un análisis y evaluación de riesgos de la seguridad informática mediante un Hacking ético a los sistemas de COMFAORIENTE seccional Pamplona para detectar las vulnerabilidades presente

4. Proponer un conjunto de controles basados en la norma ISO 27002 que permitan mitigar los riesgos encontrados en la infraestructura tecnológica y la gestión de la información en la oficina de COMFAORIENTE seccional Pamplona.

5. MARCO REFERENCIAL

5.1. MARCO DE ANTECEDENTES

Dentro de las investigaciones encontradas al respecto del tema tenemos:

- "Metodología de análisis de riesgo de la empresa la casa de las baterías S.A de C.V" realizado por varios estudiantes de la Universidad Tecnología de El Salvador, en el año 2009.

Resumen: En el presente trabajo se ha realizado la documentación sobre una consultoría de seguridad en la empresa "LA CASA DE LAS BATERIAS S.A DE C.V". La cual se encuentra ubicada en el lugar (parte de la dirección) siendo el principal rubro (actividad a la que se dedica). Para llevar a cabo la investigación se hizo uso de diferentes técnicas de recolección de información como entrevistas a encargados del área de informática para determinar diversos factores que intervienen como vulnerabilidades, amenazas, entre otros. En la seguridad de la empresa antes mencionada se ha desarrollado la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, en este informe detallamos tanto información general como específica sobre lo que se refiere esta metodología llamada Magerit, elaborado por el Ministerio español de Administraciones Públicas, Dado su carácter abierto que también se utiliza fuera de la Administración.[1]

- Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de Pamplona - Norte De Santander. Realizada por Jorge Enrique Ramírez Montañez. De la Universidad Nacional Abierta y a Distancia UNAD. En el año 2015.

---

1 Arévalo o, Escalante K, Guevara N, Jiménez, M Montoya A y Orellana J. (2009) Metodología de análisis de riesgo de la empresa la casa de las baterías S.A de C.V". Universidad Tecnológica del Salvador.

Resumen: Su objetivo principal fue, realizar un análisis y evaluación de riesgos para asesorar e implementar mejoras en la seguridad informática el área de redes y sistemas de la Alcaldía de Pamplona - Norte Santander. Lo que se llevó a cabo mediante el análisis de riesgos con el que se pretende llegar a determinar los factores que amenazan la información y los bienes del entorno informático y formular una serie de controles de acuerdo a los bienes en riesgo, teniendo en cuenta normas referentes al tratamiento de los riesgos y su administración como los son la norma ISO 27001 y ISO 27002 dentro de un plan del gestión de la seguridad de la información. Finalmente la asesoría está dirigida a la aplicación de controles y su sostenibilidad que permitirá que la entidad este en el espectro seguro para el manejo de la información.

- Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001, realizada por Francisco Nicolás Javier Solarte Solarte, Edgar Rodrigo Enriquez Rosero, Mirian del Carmen Benavides Ruano. Y publicado por la Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, en el año 2015.

Resumen. El artículo tiene como objetivo desarrollar habilidades en los ingenieros de sistemas, que les permitan conducir proyectos de diagnóstico, para la implementación e implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002. Se presentan los resultados de una experiencia aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos con el diseño y aplicación de diversos instrumentos como cuestionarios aplicados a los administradores, clave de seguridad, entrevistas al personal del área informática y usuarios de los sistemas, pruebas de intrusión y testeo que permitieron establecer el diagnóstico de seguridad actual. Posteriormente se aplica una lista de chequeo basada en la norma, para verificar la existencia de controles de seguridad en los procesos organizacionales. Finalmente y de acuerdo a los resultados del análisis y evaluación de los riesgos, se proponen los controles de seguridad para que sean

integrados hacia el futuro dentro de un SGSI que responda a las necesidades de seguridad informática y de la información acorde a sus necesidades.[2]

- Análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial, realizada por Vivian Andrea García Balaguero y Jon Jarby Ortiz González. Estudiantes de Universidad Nacional abierta y a Distancia, UNAD. En el año 2017.

Resumen: El presente trabajo consistió en realizar un análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial, el uso de estas por la comunidad educativa, es una política institucional obligatoria para los docentes de Tiempo Completo (TC) y Medio Tiempo (MT), al volverse una política el uso de las Aulas virtuales, el uso de éstas aumenta por parte de docentes y estudiantes y la posibilidad de un ataque informáticos se [3]convierte en un peligro eminente.[4]

- Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Realizado por John Jairo Perafán Ruiz y Mildred Caicedo Cuchim, en el 2014, de la Universidad Nacional Abierta y a Distancia UNAD.

Resumen. La Institución Universitaria Colegio Mayor del Cauca es una entidad en crecimiento que debe involucrar dentro de sus procesos buenas prácticas encaminadas a la protección de la información; razón por la cual es necesario el desarrollo del análisis de riesgo de la seguridad de la información aplicado a cada uno de los activos de información. El análisis de riesgo permite realizar un diagnóstico para conocer las debilidades y fortalezas internas encaminadas en la

2 Francisco N, Solarte E, Rosero, M. (2015) Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de Pamplona - Norte De Santander.

Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507.

3 Página Web Comfaoriente. http://comfaoriente.com/

4 Garcia V y Ortiz G. (2017) Análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial. Universidad Nacional abierta y a Distancia, UNAD [5] Perafán J y Caicedo M. (2014) Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. en el 2014. Universidad Nacional Abierta y a Distancia UNAD.

generación de los controles adecuados y normalizados dentro de las políticas de seguridad informática que hacen parte de un Sistema de Gestión de Seguridad de la Información (SGSI), además de facilitar su continuo monitoreo a través de procesos de auditorías y mejoras continuas. Con este trabajo se Identificaron y clasificaron los activos de información presentes en la Institución Universitaria Colegio Mayor del cauca, Aplico una metodología de evaluación de riesgos que permita definir las vulnerabilidades y amenazas de seguridad existentes, y evaluar los riesgos de acuerdo a la escala definida por la metodología Magerit. Sugerir mecanismos de control y gestión que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado, se elaboró un informe de recomendaciones donde se muestre los hallazgos que permita definir un Sistema de seguridad de la información ajustada a la realidad de la Institución Universitaria Colegio Mayor del Cauca.[5]

- Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. san Bartolomé de Capitanejo, Santander, tesis realizada por José Leonardo Cordero Moreno y Yadimyr Oswaldo García Reyes de la Universidad Nacional Abierta y a Distancia en 2016.

Resumen. El objetivo de este trabajo fue Realizar el análisis de riesgos y recomendaciones en los niveles de seguridad informática mediante el uso de aplicaciones que permitan evidenciar vulnerabilidades en los sistemas de información y telecomunicaciones del Hospital E.S.E. San Bartolomé de Capitanejo, Santander Desde este punto de vista el E.S.E. Hospital San Bartolomé de Capitanejo, Santander; en sus procesos informáticos se encuentra en alta vulnerabilidad ya que existen riesgos que no se han tenido en cuenta al momento de proteger la información; estos riegos o vulnerabilidades deben ser analizados y revisados para tomar medidas de control que permitan minimizar los riesgos inminentes que puedan afectar el sistema de información de la institución. En el presente trabajo de grado se documenta una serie de análisis de riesgos que se han detectado en la empresa E.S.E. hospital San Bartolomé del municipio de Capitanejo, esto debido al cambio de la infraestructura y la falta de implementar unas políticas de seguridad adecuadas en la administración de tres (3) servidores

en los cuales se encuentra almacenada la información de todos los procesos administrativos operativos y financieros de la empresa, se hace necesario plantear diversas recomendaciones de seguridad informática para optimizar el fortalecimiento de dichos procesos garantizando su confidencialidad, integridad y disponibilidad. El producto resultante de este estudio serán las recomendaciones y alternativas para darle tratamiento a los riesgos encontrados sobre los procesos, procedimientos y recursos que tienen información sensible para el hospital, permitiendo la creación de mecanismos, estrategias y cultura en las personas mediante un proceso de capacitación y/o concienciación del personal del hospital en el uso correcto de los recursos tecnológicos.[5]

5.2. MARCO CONTEXTUAL

5.2.1. Reseña Histórica, Caja de Compensación Familiar COMFAORIENTE.

COMFAORIENTE nace en 1954, con el objeto de crear un club donde estuvieran afiliados los trabajadores que obligatoriamente debían pagar subsidio para una caja de compensación familiar.

En el Norte de Santander un pequeño grupo de rectores de Colegios afiliados a la Asociación Nacional de Rectores de Colegios Privados ANDERCOP, desplegaron toda su actividad en obtener el reconocimiento jurídico el cual se produjo mediante Resolución No. 083 del 26 de junio de 1968 otorgada por la Gobernación del Norte de Santander.[6] Con este nombre permaneció durante 18 años, en 1986 con el fin de permitir la vinculación de nuevas empresas de diferentes actividades económicas, la Asamblea General de Afiliados introdujo una reforma estatutaria donde le asignó a la Caja el nombre de COMFAORIENTE, La Caja de Compensación Familiar del Oriente Colombiano, acto que reactivó la afiliación de importantes empresas del orden oficial y particular, del sector de la Salud, la Educación, la Banca, la Minería, el Comercio, la Construcción, los Servicios, etc.[7]

---

5 Cordero J y García Y. (2016) Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. san Bartolomé de Capitanejo, Santander. Universidad Nacional Abierta y a Distancia. UNAD.

6 Idem

7 Idem

COMFAORIENTE cumple rigurosamente con los postulados del sistema del Subsidio Familiar, enmarcados en la Ley 21 de 1982 y bajo nobles principios de concertación, equidad, solidaridad y compensación que permiten aliviar las cargas económicas de miles de trabajadores afiliados de menores recursos, con el pago de una cuota de subsidio en dinero y brindándoles la oportunidad de acceder a menor costo, junto con su familia a los servicios sociales de salud, capacitación, educación, recreación, créditos con intereses blandos y facilidades de pago en diferentes modalidades.[8]

En el campo de la Educación Formal, el Colegio de Bachillerato inició sus labores en 1977, como Centro Vocacional Andercop, dos años más tarde se le denominó Colegio Diversificado Andercop y así sucesivamente fue encuadrando sus servicios académicos de acuerdo a los lineamientos del Ministerio de Educación Nacional, hasta llegar a lo que es hoy, el COLEGIO COMFAORIENTE, donde se asisten educandos en Pre-escolar, Básica Primaria, Básica Secundaria y Media Técnica con énfasis en Ciencias Naturales e Informática.

En 1996, COMFAORIENTE pensando en la población afiliada de la Provincia de Pamplona adquirió el inmueble en el cuál actualmente funciona la sede administrativa y de Servicios Sociales en la Ciudad Mitrada del Norte de Santander, Pamplona. En Pamplona cuenta con una sede propia y en Ocaña se adquirió el Centro en 1997. COMFAORIENTE analizando la imperiosa necesidad de reubicar el Centro de Educación No Formal en un sector estratégico que ofreciera a los afiliados y sus familias la facilidad de tomar los cursos de capacitación sin contratiempos y abordando temas relacionados con la pobreza que registra la región como consecuencia de la recesión económica, la falta de industrialización y las bajas tasas de empleo, el Consejo Directivo y la Administración de la Caja emprendieron el estudio de factibilidad para la construcción del edificio con destino a la Sede Administrativa, Capacitación y Mercadeo de COMFAORIENTE.

8 Idem

Es un centro de educación, de recreación y de subsidios que cuenta con una planta de personal importante y que por sus negocios y capacidad empresarial debe mantener sus equipos en excelente forma para asegurar el buen funcionamiento de todo un sistema.

5.2.2. Organización de la empresa. En la caja de compensación COMFAORIENTE cuentan con el siguiente organigrama.

Figura 1. Organigrama institucional

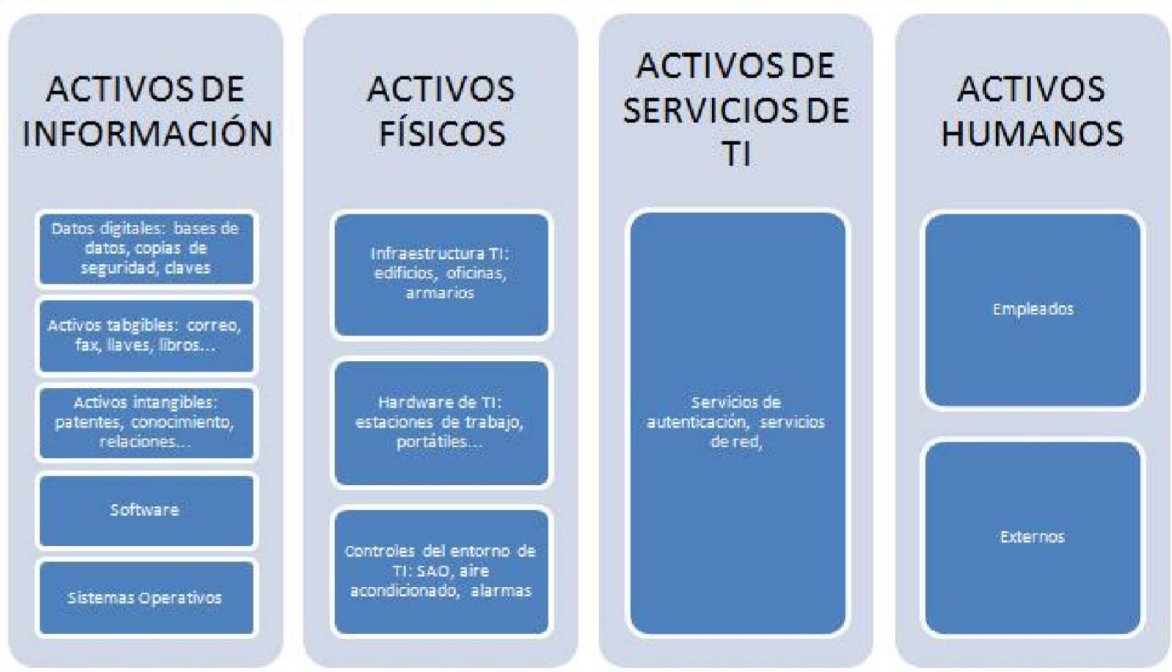
Fuente: http://comfaoriente.com/

5.3. MARCO TEÓRICO

5.3.1. Activos de Información. Los activos son todos los elementos presentes al interior de un sistema de información que tiene una organización, por lo tanto debe

protegerse, tales como los datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos, administrativos, recursos físicos y recursos humanos.[9]

Figura 2. Activos de la información



Fuente: https://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-normaiso-27001/

Una vez identificados los activos, se procede a realizar la valoración para estimar qué valor tiene cada activo para la organización, según su importancia, para ello se definen las dimensiones o los criterios por los cuales se van a evaluar, los criterios de evaluación son los siguientes:

[C] Confidencialidad: Cuanto daño hace a la empresa si se publica su información confidencial.

9 Bueno Shirley. (2015) Diseñar un Sistema de Gestión de Seguridad de la Información mediante la Norma ISO 27001 en el Instituto Colombiano de Bienestar Familiar Centro Zonal Virgen y Turístico de la Regional Bolívar.. Universidad Nacional Abierta y a Distancia UNAD Cartagena. Colombia.

[I] Integridad: Si el activo es modificado, que daño causaría a la empresa. [D] Disponibilidad: Cuando se necesite el activo y no esté disponible, cuanto perjuicio causaría esta situación a la empresa.

[T] Trazabilidad: Si no se sabe quién accede al activo y que acciones realiza, se evalúa el daño que esta situación causaría a la empresa.

[A] Autenticidad: Saber si el activo no es propio de la persona, qué perjuicio causaría no saber si el activo es propio de la persona.[10]

5.3.2. Seguridad de la información. La Seguridad de la Información, de acuerdo a la norma ISO 27000:2014, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información.4 De acuerdo a la Asociación Española para la Calidad, la Seguridad de la Información tiene como propósito la protección de la información y de los sistemas de la información contra las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada. [11]

5.3.3. Gestión de seguridad. La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La gestión de la seguridad de la información requiere la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información. (Cordero, 2017) Primero se define como SGSI que es la abreviatura

---

10 Idem

11 Cordero Liñán Ronal. (2017) Diagnóstico del estado actual de la seguridad de la información basado en la norma ISO 27001:2013, de la IPS Medicsalud de la ciudad de Valledupar – Cesar. Universidad Nacional Abierta y a Distancia “UNAD”. Valledupar Colombia.

utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System.[12]

Para este caso específico, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.),la seguridad además consiste en la conservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.[13]

Es necesario que la gestión de seguridad de la información, realice diagnóstico de los riesgos y busque estrategias para la minimización de los mismos.

5.3.4. Análisis y Evaluación de Riesgos de Seguridad de la Información.

12 Idem
13 Idem

a. Identificación de las amenazas. Las amenazas puede surgir de manera natural o humana; dependiendo de dónde vienen; igualmente pueden ser deliberadas o accidentales y pueden afectar a más de un activo generando diferentes impactos.[14]

b. Identificación de las vulnerabilidades. Las vulnerabilidades de los activos de información son debilidades que son aprovechadas por amenazas y generan un riesgo, una vulnerabilidad que no tiene una amenaza, puede no requerir de la implementación de un control, para lo cual es necesario identificarla y monitorear. Pero es necesario dejar claro que un control mal diseñado e implementado puede constituir una vulnerabilidad. La identificación de las vulnerabilidades se basa las entrevistas con los responsables de los activos de información y serán registradas en la Matriz de Riesgos.

c. Identificación de los Riesgos. Los riesgos en seguridad de la información se identificaran mediante el resultado de las pruebas de seguridad, identificación por parte de los empleados quienes tienen claridad y han experimentado la materialización de algunos riesgos en sus procesos. [15] Los riesgos son relacionados a las vulnerabilidades y amenazas de los activos de información los cuales se deberán listar en la matriz de riesgos. Los riesgos se clasifican en: Lógico, Físico, Legal y Locativo.[16]

d. Selección de la Probabilidad de Ocurrencia. El valor de la probabilidad estará determinado por el responsable del proceso con base a su experiencia, de acuerdo a la estimación del riesgo asociado con la amenaza y vulnerabilidad de los activos de información. Para los riesgos que no se han materializado en la

---

14 Suarez Padilla Yomay. (2015) análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & CÍA. LTDA, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia.

15 Idem

16 Ídem

organización y a los cuales no existe claridad por parte del responsable en el grado de estimación de la materialización, el valor de probabilidad estará sujeto a datos de referencias externas (Información de probabilidad de materialización en otras organizaciones) o finalmente por criterio de experto en riegos. Luego se deberá consolidar una matriz que describe cada uno de los activos involucrados en el análisis. Con ella se revisa cada uno de los riesgos existentes en seguridad y se relacionaron con los activos de información.[17]

e. Determinar el impacto de los Activos de Información. El impacto está determinado por el máximo valor de la calificación registrada en términos de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) de los activos de información. [18]

f. Valoración del Riesgo Inherente. El marco de referencia utilizado en la evaluación del riesgo para los activos es la norma ISO 2700518 . Para la valoración y evaluación de los riesgos se tendrán en cuenta las siguientes variables definidas anteriormente: Valor del activo (VA). Probabilidad P(A,V). Valor Impacto (IMP). Donde Valor Riesgo = P(a,v) * Valor Impacto * Valor Activo (2) Con la anterior formula se obtendrá el valor del riesgo asociado a cada activo de información en términos de su confidencialidad, integridad, disponibilidad, valor económico, la probabilidad de ocurrencia y el impacto asociado al SGSI.

g. Identificación de controles existentes. Se realizará la identificación de controles documentados, implementados y monitoreados por la organización para la gestión del riesgo. Después será necesario verificar el valor del riesgo residual y determinar si es posible aplicar un plan de Tratamiento de Riesgo.[19]

5.3.5. Las acciones definidas para el tratamiento de los riesgos. Evitar: la acción que da origen al riesgo particular. Se evalúa y determina la viabilidad de si se puede o no evitar el riesgo en la compañía mediante el impacto que esto generaría. 21

17 Idem

18 Idem

19 Idem

Transferir: a organizaciones como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo. Para seleccionar una tercerización de un riesgo se evalúa el costo beneficio es decir sea la opción adecuada y económica en su implementación, adicionalmente se debe verificar que el riesgo residual este en los niveles de aceptación de la compañía tras su implementación.[20]

Mitigar: mediante la aplicación de controles apropiados de manera que el riesgo residual se pueda revaluar como aceptable.

Aceptar: con el conocimiento y objetividad, siempre que cumplan con la política de seguridad previamente establecida por la organización. Es la última decisión que se toma en el tratamiento de riesgos y aplica cuando no existe opción alternativa bien sea por costo económicos o por tiempos de implementación. [21]

5.3.6. MAGERIT. (Metodología de análisis y Gestión de Riesgos de los Sistemas de Información). Esta metodología es desarrollada por CSAE (Consejo Superior de Administración Electrónica) metodología desarrollada como respuesta a la necesidad de hacerfrente al creciente uso de medios electrónicos para el manejo de la información en todas sus formas: generación, procesamiento, comunicación, registro, respaldo. De esta manera en la norma se reúne un conjunto de las mejores prácticas para brindar seguridad en el manejo de la información.[22]

Además MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Actualizada en 2012 en su versión 3. Esta metodología contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información. A continuación se relacionan cada uno de los pasos que se deben

20 Idem

21 Idem

22 Álvarez Jerzon. (2016) Diseño de un sistema de gestión de seguridad de la información - SGSI basado en la norma iso27001 para el Colegio Procolombiano de la ciudad de Bogotá, que incluye: asesoría, planeación. Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia.

contemplan en un proceso de análisis de riesgos, teniendo en cuenta un orden sistémico que permita concluir el riesgo actual en que se encuentra la empresa. Como se mencionó anteriormente, los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, etc.). Magerit diferencia los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. A la hora de realizar el análisis de riesgo el primer paso es identificar los activos que existen en la organización y determinar el tipo. En la tabla No. 2 se relacionan cada tipo de activos.[23]

5.3.7. Ciclo de Deming. El ciclo de Deming (de Edwards Deming), también conocido como círculo PDCA (del inglés plan-do-check-act, esto es, planificar-hacer-verificar-actuar) o espiral de mejora continua, es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart.[24]

La norma ISO/IEC 27001:2013 realiza el análisis de procesos con apoyo en el ciclo Deming. Este análisis plantea la gestión de la seguridad como un proceso de mejora continua, imagen 1, aplicando la repetición cíclica de cuatro fases, como se muestra en la Figura 3.

- Planificar: Realizar la planeación significa establecer los objetivos y definir los medios que permitirán su logro.

- Hacer: Llevar a cabo las acciones planeadas para el logro de los objetivos empleando los medios preestablecidos.

23 Cordero José y García Yadynir. (2016) Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé De Capitanejo, Santander. Universidad Nacional Abierta y a Distancia UNAD. Málaga.

24 Henao Rodríguez Jaime. (2016) Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 para la empresa USOMET LTDA. en la ciudad de Ibagué. Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia.

- Verificar: Seguimiento que trata de establecer el grado de avance en la consecución de los objetivos planeados.

- Actuar: Luego de realizar el análisis de la verificación, se debe estudiar y definir y aplicar los correctivos que sean necesarios encaminar nuevamente la acción hacia el logro de los objetivos.[25]

Figura 3. Ciclo de Deming

Autor: Espinoza, 2013)

Por esta metodología creada por el Consejo Superior de Administración Electrónica es posible que las empresas puedan depender de la tecnología y sus avances para sus procesos administrativos obteniendo como resultado el cumplimiento de su razón misional y visional. [26]

25 Idem

26 Bojaca Garavito Edgar.(2016) Diseño de un sistema de gestión de seguridad informatica basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco De Gachetá. . Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia. [29] Idem

Su principal objetivo es el de observar y evaluar el uso de los activos informáticos dentro de una organización para corregir acciones que generen un riesgo contribuyendo así con la mitigación del mismo.

Con esta herramienta se permite a los analistas en seguridad de la información establecer acciones de mejora las cuales deben responder a una serie de controles que contribuyan a la mitigación del riesgo. [29]

Los activos de información son todos aquellos elementos que utiliza la entidad para la elaboración, edición, transferencia y eliminación de su información, Magerit realiza la clasificación de los mismo de acuerdo a sus características particulares, similitudes o usos elementales lo que permitirá establecer de mejor manera el tratamiento del riesgo para mitigarlo y hacer más segura la infraestructura informática. [27]

5.3.8. Sistema de Gestión de Seguridad de la Información. El Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, ofrece la protección ante cualquier amenaza que pueda poner en peligro a las organizaciones, tanto públicas como privadas, por el contrario podrían realizarse algún daño para la salud empresarial.[28]

La realidad nos ofrece que las empresas se enfrentan diariamente a un enorme número de riesgos e inseguridad que proviene de una elevada variedad de fuentes diferentes, entra las que podemos entrar los nuevos negocios y nuevas herramientas relacionadas con la tecnología de la información y la comunicación, que los directores generales y los directores informáticos de la organización deben aplicar.

---

27 Idem

28 SGSI(2015) Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001.Recuperado en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/42965/7/mmanozTFC0615memoria.pdf [32] Idem

Todas las herramientas se tiene que aplicar según los diferentes objetivos que tengan fijados las organizaciones con la mayor seguridad, y garantizando la confidencialidad, integridad y disponibilidad. (SGSI, 2015)

Para poder proteger la información se tiene que realizar la implementación, el mantenimiento y la mejora de las medidas de seguridad para que cualquier tipo de organización consiga sus objetivos y además garantice que cumple con la legislación, aumentando el prestigio y la imagen de la compañía.

La norma ISO27001, Sistema de Gestión de Seguridad de la Información, es la solución de mejora continua más apropiada para poder evaluar los diferentes riesgos y establecer una serie de estrategias y controles oportunos para asegurar la protección y defender la información.[32]

El Sistema de Gestión de Seguridad de la Información (SGSI) se encuentra fundamentado en la norma ISO-27001, que sigue el enfoque basado en procesos que usan el ciclo de Deming o el ciclo de mejora continua, consistente en Planificar-Hacer-Verificar-Actuar (PHVA), conocido con las siglas en inglés PDCA. (SGSI, 2015)[29] El principal objetivo de la norma ISO 27001 es analizar y gestionar los riesgos basados en los procesos. Resulta muy útil el análisis y la gestión de riesgos basados en los procesos ya que evalúa y controla a la organización en relación a los diferentes riesgos a los que se encuentra sometido el sistema de información.

Los procesos se establecen en los activos de la TIC que ofrecen soporte a éstos. Por lo que se exige la realización de un análisis y gestión de riesgos de los sistemas de información de una forma realista y orientada a los objetivos plantados por la empresa.[30] Una vez evaluados los riesgos y aplicados todos los controles, siempre queda un riesgo residual que la alta dirección de la organización debe aprobar y que será revisado por lo menos una vez al año.

29 Idem

30 Idem

Tenemos que destacar que el Sistema de Gestión de Seguridad de la Información ISO27001 además de contar con el ciclo Deming (PDCA) tiene ciertos indicadores y métricas para realizar la medición de la eficiencia de los diferentes controles utilizados, aportando datos reales cada día de la seguridad de los Sistemas de Información. (SGSI, 2015)[31]

5.3.9. Evaluación de riesgos. La evaluación de riesgos es el primer proceso en la metodología de gestión de riesgos. Las organizaciones utilizan la evaluación de riesgos para determinar el alcance de la amenaza potencial y el riesgo asociado con un sistema de tecnología de la información a través del desarrollo del ciclo de vida del sistema. El resultado de este proceso ayuda a identificar los controles adecuados para reducir o eliminar los riesgos durante el proceso de mitigación de los mismos. La metodología de evaluación de riesgos trabaja bajo nueve pasos principales, que se describen a continuación 1. Caracterización del Sistema 2. Identificación de amenazas 3. Identificación de vulnerabilidades 4. Análisis de Control 5. Determinación de la probabilidad 6. Análisis de Impacto 7. Determinación de Riesgos 8. Recomendaciones de los controles 9. Documentación de Resultados. [32]

5.3.10. Modelo de gobierno y gestión para las Tecnologías de la información y de la comunicación. La norma ISO-27001 presenta relación con otras normas que constituyen el modelo de gobierno y la gestión de las TIC. Dicho modelo propone dos certificaciones al máximo nivel:

- ISO 38500 “Gobierno corporativo de las TIC”
- ISO 22301 “Sistemas de Continuidad de Negocio”

La implementación de los Sistemas de Gestión hace que se gestione la calidad y la seguridad de los servicios de Tecnologías de la Información y la Comunicación

---

31 Idem

32 Sossa Johanna (2012) Análisis de Riesgos Estándares para la administración de riesgos. Universidad Javeriana Recuperado de.
http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

(TIC), con lo que se consigue disminuir los riesgos en torno a la Seguridad de la Información y aumentar la seguridad de las TIC. (SGSI, 2015)[33]

En la otra área de gestión se agrupan todas las actividades de desarrollo de programas, que se dirigen a la calidad del proceso de ingeniería del software, el modelo de evaluación, mejora y madurez del software. Este modelo genera un cambio radical que impacta en el mundo empresarias y las administraciones públicas en la ración las TIC. La norma ISO 27001 es un sistema activo, que se encuentra integrado en la organización, orientado a os objetivos empresariales y con una proyección de vistas al futuro. Es muy importante resaltar que cada vez se introduce una nueva herramienta de TIC a la organización que tiene que actualizar el análisis de riesgos para mitigar de forma responsable todos los riesgos y considerar la regla básica del riego, es decir, minimizar los riesgos empleando medidas de control ajustadas y considerando los costes del control. (SGSI, 2015)[34]

Los certificados amparan que se cumplan las normas, en este caso la norma ISO27001. En el mercado en el que vivimos, cada vez más globalizados, en el que las organizaciones de bienes y servicios tienen que competir con mercados que abastecen a todo el mundo. (SGSI, 2015)

Hoy día, son cada vez más las empresas certificadas con la norma ISO-27001, lo que fomenta es que las actividades de protección de la información en las organizaciones, aumentando su seguridad de la información, su imagen y la confianza antes los consumidores. (SGSI, 2015)[35]

---

33 SGSI(2015) Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001.Recuperado en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/42965/7/mmanozTFC0615memoria.pdf [37] Idem

34 Idem

35 Idem

5.3.11. Auditoría Informática. La auditoría informática comprende gran variedad de conceptos, parámetros y normativas tendientes a mejorar procesos y procedimientos internos a nivel organizacional, por medio de mecanismos de control interno; algunos métodos se basan en buenas prácticas de gobierno corporativo o la aplicación de transparencia en el actuar de las organizaciones vista como un activo más de la misma y encaminada o proyectada en términos de eficiencia corporativa. Según el autor Fernando Pons en un artículo publicado en la revista nuevas tecnologías, En sus inicios, el auditor informático surge como un apoyo a los tradicionales equipos de auditoría. Su labor de apoyo consistía básicamente en la obtención de información financiera de los sistemas de información en los que residía y tratarla, con herramientas específicas para cantidades masivas de datos así facilitar la labor de los equipos de auditoría financiera. Entre las grandes ventajas que el apoyo del auditor informático ofrecía era el dar la validación del total de la información revisada o auditada, en lugar de los habituales procedimientos de muestreo. Dicha labor continúa siendo hoy día una de las principales tareas del auditor informático. [36]

Actualmente es fácil encontrar auditores informáticos manipulando información para validar información compleja de obtener, tal como lo es la información del ámbito financiero, información académica en instituciones de educación superior, o en ámbitos productivos el de la amortización de inmovilizados o la valoración de existencias. Conforme el auditor, indaga y cuestiona o valora cada dato en un proceso organizacional va profundizando su conocimiento en la gestión de los negocios importantes de la organización y a su vez es capaz de plantear objetivos de control que tratarán de proteger la información en su totalidad o parcialmente de acuerdo a las funciones organizacionales y a la definición de límites de acuerdo a los niveles de criticidad de la información identificados por cada organización.

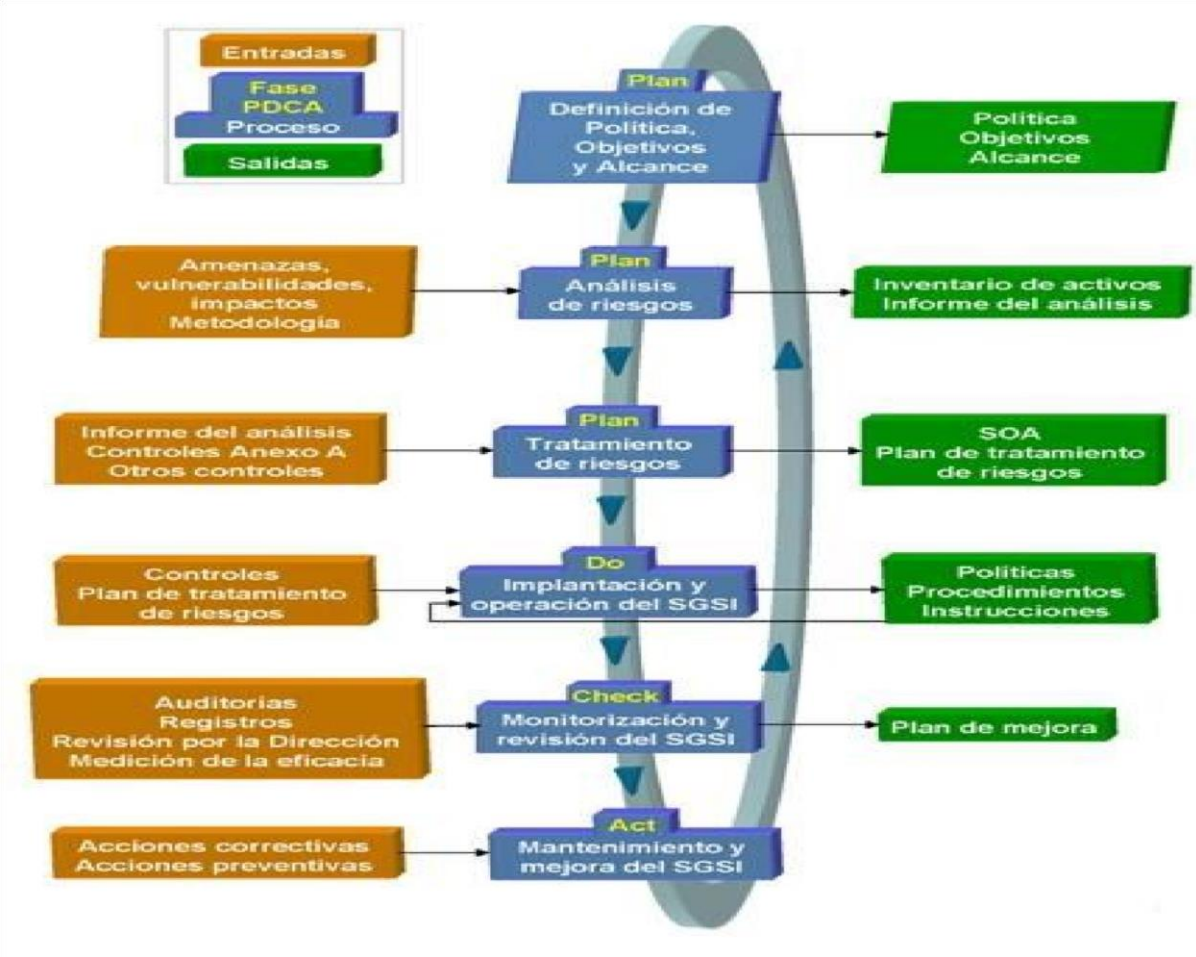
5.4. METODOLOGÍA DE EVALUACIÓN DEL RIESGO

5.4.1. Análisis de Riesgos. Es una herramienta de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este

36 Perafan Jairo y Caicedo Mildred. (2014) Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Universidad Nacional Abierta y a Distancia. Popayán.

análisis tiene como objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y posteriormente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos. El objetivo general del análisis de riesgos, es identificar sus causas potenciales de los principales riesgos que amenazan el entorno informático. Según Harold F. Tipton y Micki Krause1. “la seguridad informática puede ser definida, básicamente, como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información” (Benavides Ruano & Solarte, 2012).

Figura 4. Plan análisis del riesgo ISO 27001



Fuente: http://www.iso27000.es/sgsi.html

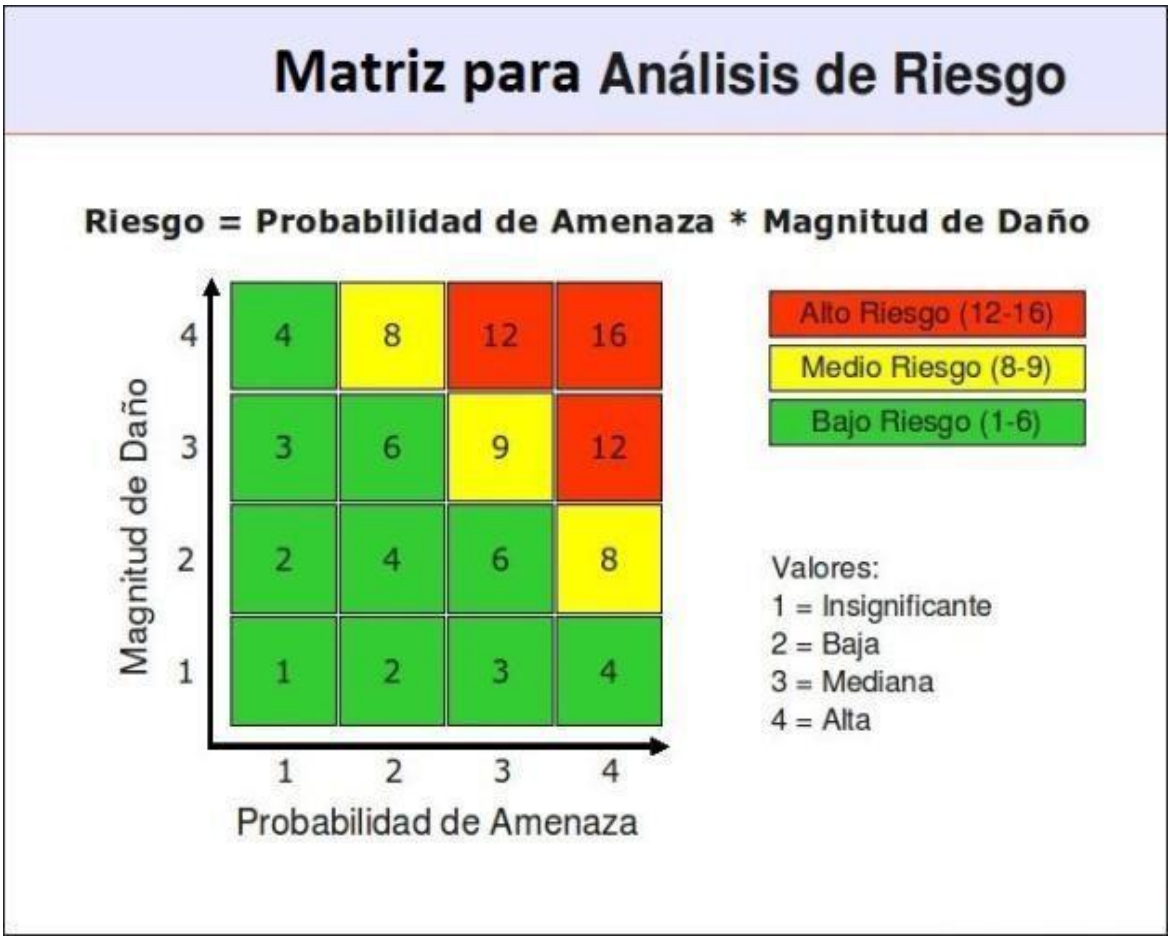
El proceso de análisis genera habitualmente un documento que se conoce como matriz de riesgo, donde se ilustran todos los elementos identificados, sus relaciones y los cálculos realizados.

5.4.2. Matriz para el análisis de riesgo. Es una herramienta utilizada para indicar los riesgos, los controles y su valoración por probabilidad e impacto. Normalmente es utilizada para identificar las actividades, los procesos y productos más importantes de una organización, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos

denominados factores de riesgo. El estándar ISO/IEC 27001 adopta una metodología dada por Alan Calder y Steve.

Watkins que es la del “análisis de riesgos cualitativa” la cual se trata en mediante las matrices. (Benavides Ruano & Solarte, 2012).

Figura 5. Matriz para análisis de riesgo



Fuente: ERB, M. (2008). *Gestión de Riesgo en la Seguridad Informática*.

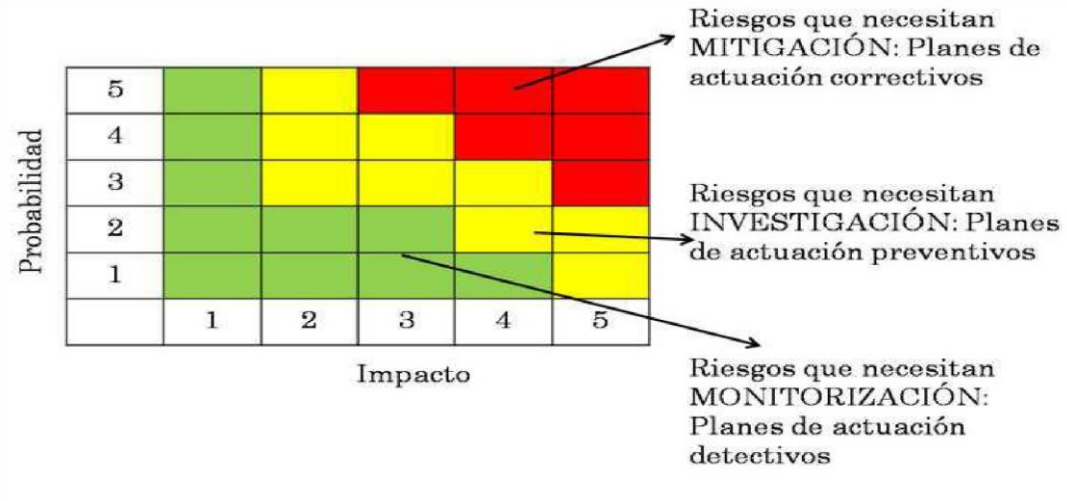
El riesgo total es la combinación de los elementos que lo conforman, calculando el valor del impacto por la probabilidad de ocurrencia de la amenaza y cuál es el activo que ha sido impactado. Presentado en una ecuación matemática para la combinación válida de activos y amenazas. La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente, por

lo tanto la valoración de los riesgos se realiza teniendo en cuenta los siguientes valores, los cuales se distribuyen en la matriz de análisis de riesgo.

- Bajo Riesgo = 1 – 6 (verde)
- Medio Riesgo = 8 – 9 (amarillo)
- Alto Riesgo = 12 – 16 (rojo)
- RT (riesgo total) = probabilidad x impacto (Magnitud del daño)

Para calcular el riesgo es preciso identificar primero la magnitud del daño de cada uno de los elementos de información y también se debe identificar las probabilidades que ocurran las amenazas, basta con multiplicar de manera individual cada probabilidad con su respectiva magnitud de daño; de esta forma se identifica el índice de riesgo que se obtiene en la escala de 1-16 de acuerdo a lo mencionado anteriormente; es importante saber la probabilidad que tiene cada recurso de ser vulnerable porque no todos poseen la misma ya que dependiendo de la función y el entorno de los recursos que sirven a la información, algunos se encuentran más expuestos a ser vulnerables por el nivel de importancia en el proceso de gestión de la información por tal motivo necesitan mayor protección dependiendo de la valoración de activos.

Figura 6. Interpretación de la matriz para análisis de riesgo.



Fuente: ERB, M. (2008). Gestión de Riesgo en la Seguridad Informática.

- Probabilidad. Para determinar la probabilidad de ocurrencia es posible de la forma cualitativa o cuantitativamente, considerando que la medida no debe contemplar la existencia de acciones de control.

- Impactos. Son las consecuencias de la materialización de las distintas amenazas y los daños que éstas puedan causar. Las pérdidas generadas pueden ser financieras, tecnológicas, físicas, entre otras.

- Amenazas. Son acciones que pueden generar consecuencias negativas en la operación de la organización. Se referencian como amenazas a las fallas, los ingresos no autorizados, los virus, los desastres ocasionados por fenómenos naturales o ambientales, etc.

- Vulnerabilidades. Son ciertas condiciones a las que se exponen los activos, están presentes en su entorno, facilitan que las amenazas se materialicen y se conviertan en vulnerabilidad.

- Activos. Los activos en tecnología, es todos lo relacionado con los sistemas de información, las redes las, comunicaciones y la información en sí misma.

5.5. PLANIFICACIÓN DEL ANÁLISIS Y EVALUACIÓN DE RIESGOS DE LA SEGURIDAD INFORMÁTICA EN COMFAORIENTE SEDE PAMPLONA, SIGUIENDO PARÁMETROS DE LA NORMA ISO 27001

El análisis de riesgos de la seguridad informática está enfocado para aplicar en el ente objeto del estudio un análisis de riesgos con el fin de interpretar mediante el análisis la metodología la información sobre las vulnerabilidades, amenazas y los riesgos que forman el conjuntos de elementos que crean el campo de falencias de la seguridad de la informática y la información, haciendo evidentes la necesidades de tomar decisiones y medidas con el fin evitar desastres en la información. La Organización Internacional define riesgo tecnológico como “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños”. Este análisis tiene como objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y las implicaciones a que conduzca.

5.5.1. Alcance del análisis y evaluación de riesgos. Busca llegar a las finalidades de gestión mediante un análisis, en donde se evalúan los recursos, los servicios, los medios, usuarios y configuración del sistema local para buscar posibles vulnerabilidades y amenazas que generen riesgos a la seguridad informática de la sede y establecer una matriz de riesgos articulado con el alcance general:

El plan estratégico de Seguridad de la información en COMFAORIENTE sede Pamplona busca lograr la implementación de un Sistema de Gestión de Seguridad de la Información, tomando como base los lineamientos de la norma ISO 27001:2013 para la protección, preservación y administración de la información derivada de los procesos misionales, salvaguardando la confidencialidad, integridad y disponibilidad de ésta.

5.5.2. Métodos para la búsqueda de información. En este proceso de encontrar los datos suficientes para realizar el análisis de riesgos se implementaron técnicas comunes para este tipo de procesos.

5.5.3. Observación directa. Mediante esta técnica se lograra evidenciar diversas vulnerabilidades presentes en los medios tangibles que conforman los bienes informáticos de la sede.

5.5.4. Entrevista. A través de una serie de preguntas a los funcionarios usuarios de los servicios informáticos de la entidad se lograron distinguir vulnerabilidades presentes en la sede.

5.5.5. Ethical Hacking y Pentesting (Pruebas de penetración). Con el uso de programas especializados se realizaron diversas pruebas con el propósito de encontrar vulnerabilidades y brechas de seguridad en los equipos y la red; estas pruebas fueron realizadas con consentimiento y teniendo en cuenta los artículos de la ley 1273 del 2009.

5.5.6. Población y Muestra. Para llevar a cabo la investigación se logró determinar la población de elementos que componen las redes y sistemas que conforman el entorno informático de COMFAORIENTE sede Pamplona. El objeto del análisis distingue: Población de equipos de cómputo, población de equipos de red, población de usuarios finales.

5.5.7. Diseño de la muestra. Mediante el esquema de muestreo aleatorio simple se determina el tamaño de la muestra donde.

- N = tamaño de la muestra
- p = población
- m = media de la población

- Formula: $n = p/m$

Se analizaran los entes de forma individual bajo los criterios que determinan las variables de estructura y configuración de sus sistemas informáticos y así de terminar, vulnerabilidades y estado del sistema ante un prospecto de seguridad informática. Este método se repite en cada muestra partiendo de patrones comunes. En la población objeto de estudio se encuentra el recurso humano como variable en el proceso de manejo de la información y administración de los equipos.

5.6. MARCO CONCEPTUAL

Los siguientes conceptos son de vital importancia para esta investigación, serán lo que más se utilizaran dentro del estudio. Los atributos de seguridad de la información son:

- Confidencialidad La información se revela únicamente si así está estipulado, a personas, procesos o entidades autorizadas y en el momento autorizado.[37] [38]

- Integridad La información es precisa, coherente y completa desde su creación hasta su destrucción[42].

- Disponibilidad La información es accedida por las personas o sistemas autorizados en el momento y en el medio que se requiere. [39]

- Políticas o normativas. La seguridad de la información requiere adoptar un conjunto de reglas, estatutos legales y políticas institucionales que no dejen nada al azar y que integren el esfuerzo y conocimiento humano con las técnicas de mecanismos automatizados para aplicar los mejores controles y procedimientos que sistematicen la forma en que una organización prevenga, proteja y manejo los riesgos de seguridad de sus activos de información en diversas circunstancias.[40]

- Tecnología: La tecnología es uno de los aspectos importantes al momento de generar un cambio en la organización, ya que resulta difícil tratar de implementar una certificación de seguridad en la que no sea necesario invertir

37 Presidencia de la Republica. (2017)Guía para la calificación de la información de acuerdo con sus niveles de seguridad.

38 García Vivian & Ortiz Jhon. (2017) Análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial. Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia

39 García Vivian & Ortiz Jhon. (2017) Análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial. Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia.

40 Idem

en. Es necesario considerar este punto desde los inicios del estudio ya que los costos asociados generalmente no son bajos. Actualmente toda la tecnología de comunicaciones esta soportada por redes IP, por lo que es importante tener disponibilidad y con respecto a este ámbito de disponibilidad se debe considerar cuatro aspectos importantes, datos, aplicaciones, equipamiento y redes, en donde para cada aspecto se debe procurar la seguridad. Se tiene que recordar que no solo se soluciona la seguridad de un sistema implementando nuevo equipamiento, sino que, también se debe mantener. [41]

- Vulnerabilidad, amenaza y riesgo: Los conceptos de vulnerabilidad, amenaza y riesgo están relacionados entre sí haciendo parte de la concepción de la seguridad en distintos ámbitos, que también han sido aplicados en referencia a la seguridad informática y de la información. En este artículo se tomará las vulnerabilidades como las debilidades del sistema o activo informático en cuanto a seguridad, las amenazas son los posibles ataques que puede hacer una persona (interna o externa) aprovechando las vulnerabilidades o los ataques que ya se han presentado, y los riesgos como las diversas maneras en que se presenta la amenaza y la posibilidad de que ese ataque llegue a presentarse en una organización específica. [42]

- Disponibilidad de datos: Lamentablemente no en todos los casos se puede contar con la disponibilidad de los datos y esta es una característica importante, la disponibilidad de los datos se debe procurar ya que una interrupción puede afectar de forma al funcionamiento normal de la organización. Los respaldos siempre son una oportunidad para restablecer información que por equivocación o por mala intención se ve comprometida ya sea por modificaciones o directamente por que se borra. En organizaciones

41 Maureira Daniel (2017) Norma Iso/Iec 27001 Aplicada a una Carrera Universitaria. Universidad Andres Bello. Santiago de Chile

42 Solarte Francisco, Enríquez Edgar & Benavidez Miriam. (2015) Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista

Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, (Diciembre 2015)

como una Universidad es muy recomendable contar con respaldos incrementales y totales ya que la información en este tipo de organizaciones va variando y aumentando día a día. Existen muchos mecanismos de seguridad que permiten contrarrestar la amenaza de acceso indiscriminado a los datos de la organización. Contar con acceso a información sensible y de forma indiscriminada genera consecuencias que terminan en delitos, fraudes o lo más probable de todo en errores y omisiones. [43]

- Sistema de gestión de seguridad de la información – SGSI El SGSI: Tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados. 499 Dentro de los activos informáticos se han establecido dos categorías que permiten diferenciarlos de acuerdo con su naturaleza y existencia física, la primera categoría agrupa los activos intangibles y la segunda los activos tangibles. Dentro de los activos intangibles están los bienes inmateriales tales como: relaciones inter institucionales, capacitaciones del personal, las habilidades y motivación de los empleados, las bases de datos, las herramientas tecnológicas, el conocimiento y la experiencia, y los procesos operativos. Los bienes tangibles son los de naturaleza material como: mobiliario, infraestructura tecnológica, espacios físicos, materiales y elementos de trabajo, equipos informáticos, hardware de redes, equipos de protección. [44]

---

43 Maureira Daniel (2017) Norma Iso/Iec 27001 Aplicada a una Carrera Universitaria. Universidad Andres Bello. Santiago de Chile

44 Solarte Francisco, Enríquez Edgar & Benavidez Miriam. (2015) Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista

- Control: Segú la ISO/IEC 27002:2005 es el medio para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. [45]

- ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005. [46]

- Activos. Los activos en tecnología, es todos lo relacionado con los sistemas de información, las redes las, comunicaciones y la información en sí misma. [47]

- Impactos. Son las consecuencias de la materialización de las distintas amenazas y los daños que éstas puedan causar. Las pérdidas generadas pueden ser financieras, tecnológicas, físicas, entre otras.[48]

- Riesgos informáticos: Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y

---

Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, (Diciembre 2015)

45 Solarte Francisco, Enríquez Edgar & Benavidez Miriam. (2015) Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, (Diciembre 2015)

46 Idem

47 García Ramírez German & Castro Jaime. (2017) Diseñar un Sistema de Gestión de la Seguridad de la

Información (SGSI) a la Empresa Unitransa S.A. Ubicada en la Ciudad de Bucaramanga. Universidad

Nacional Abierta y a Distancia UNAD. Bucaramnaga. Colombia

48 Idem

amenazas en cualquier momento, por lo tanto los riesgos se pueden clasificar en: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgo de infraestructura. [49]

- Riesgo aceptable No se trata de eliminar totalmente el riesgo, ya que muchas veces no es posible ni tampoco resultaría rentable, sino de reducir su posibilidad de ocurrencia y minimizar las consecuencias a unos niveles que la organización pueda asumir, sin que suponga un perjuicio demasiado grave a todos los niveles: económico, logístico, de imagen, de credibilidad, etc. (Norma ISO 27001)

- Riesgo residual Se trata del riesgo que permanece y subsiste después de haber implementado los debidos controles, es decir, una vez que la organización haya desarrollado completamente un SGSI. Es un reflejo de las posibilidades de que ocurra un incidente, pese a verse implantado con eficacia las medidas evaluadoras y correctoras para mitigar el riesgo inherente. (Norma ISO 27001)

5.7. MARCO LEGAL

Norma ISO/IEC 270014: Familia de estándares donde especifica claramente los parámetros sobre seguridad de la información, para desarrollar, implementar y mantener los sistemas de gestión de seguridad de la información, entre ellos:

- Ley 527 de 1999: Por medio de esta ley se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.

- Ley 1581 de 2012: La ley de protección de datos personales, complementa la regulación vigente para la protección del derecho fundamental que tienen

49 Solarte Francisco, Enríquez Edgar & Benavidez Miriam. (2015) Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, (Diciembre 2015)

todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

- Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

- Ley 1273 de 2009: se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos, añade dos nuevos capítulos al Código Penal: Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver, esta Ley está relacionada a la ISO2700029 .

- Ley 1341 Del 30 De Julio De 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones

- Ley 1273 de 2009: sobre los delitos informáticos y la protección de la información y de datos en Colombia.

6. DISEÑO METODOLÓGICO

6.1. TIPO DE INVESTIGACIÓN

Este proyecto es basado en la investigación aplicada, según Roberto Hernández Sampieri, en su libro Introducción a la Metodología de la Investigación, se define la investigación aplicada como “la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables.”. [50]

La investigación es considerada de tipo aplicada porque está basada en la recolección de información, para poder realizar la nueva distribución en planta de acuerdo al análisis de los ocho factores, para influir en los tiempos de traslados innecesarios y establecer el conjunto de actividades de mantenimiento que se realizaran en forma programada para el mantenimiento preventivo de los equipos influyendo así en la disponibilidad de los mismos.

6.2. METODOLOGÍA DE DESARROLLO

Inspección de la forma en que los empleados de la institución manejan la información de la institución y como la utilizan y así poder determinar si ellos ponen en riesgo la integridad de la información de la empresa y Entrevista semiestructurada a funcionario de COMFAORIENTE.

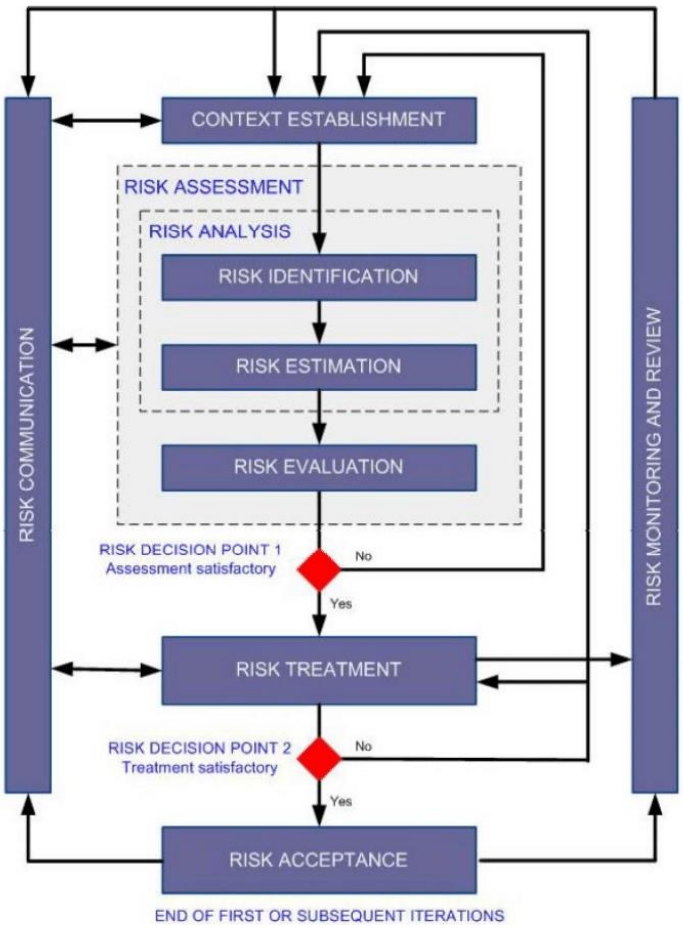
Realizados los estudios y análisis técnicos de los diferentes equipos que se utilizan en la institución se dan las recomendaciones para mejorar la seguridad de su información.

---

50 Hernández Sampier. (2003) Metodología de la investigación . Editorial Mac Graw Hill. España

Lo anterior conlleva a buscar la implementación de una serie de fases para realizar el análisis y riesgos de seguridad informática, aplicando la metodología ISO:27005:2013.

Figura 7. Fases de la norma ISO 27005



Fuente: https://www.researchgate.net/figure/ISO-27005-Risk-Management-Framework-7_fig1_263023688

Fase 1: Establecer el contexto: en esta fase permite focalizar en el área tecnológica de la empresa y observar los activos informáticos con los que cuenta haciendo un recolección de datos.

Fase 2: Al tener una idea de cómo funciona la empresa se realiza un análisis de los datos obtenidos y se identifican los riesgos potenciales a los que está expuesto la empresa.

Fase 3: Se estima el potencial de daño que puede llegar a ocurrir si se hacen realidad estos riesgos en los activos informáticos.

Fase 4: Se realiza una evaluación de los riesgos encontrados y se hacen pruebas de hacking ético para determinar los puntos débiles y poder determinar las acciones a seguir.

Fase 5: Se dan a conocer las acciones de control a seguir según el tipo de riesgos encontrados.

Fase 6: Después de conocidas las acciones de control a seguir se determina cuales son de mayor impacto y cuales tienen una mayor probabilidad de ocurrir y con esta información se toman las medidas de control y cambios que se deban realizar en los activos informáticos.

6.3 DEFINICION DE HIPOTESIS

- VARIABLES
  Nivel de seguridad informática en los activos de información de la empresa COMFAORIENTE.
- INDICADORES
  Alto, medio, bajo y ninguno

  DIMENSIONES

  - organización de los procesos y políticas de la empresa
  - aplicabilidad de controles de seguridad informática
  - actualizaciones periódicas de hardware y software
  - auditorias de seguridad informática.

- HIPOTESIS DE INVESTIGACION (HI): existe controles de seguridad informática para mitigar riesgos en los activos de información de la empresa COMFAORIENTE seccional pamplona.

- HIPOTESIS NULA (HO): No existe controles de seguridad informática para mitigar riesgos en los activos de información de la empresa COMFAORIENTE seccional pamplona.

6.4. POBLACIÓN Y MUESTRA

Este proyecto está dirigido a los empleados de la caja de compensación familiar COMFAORIENTE, con sede en Pamplona, Norte de Santander la cual ofrece servicios para los empleados de distintas empresas a nivel departamental, en la cual se enfoca a la atención de grupos familiares. Estos manejan una base de datos de información en donde se relaciona los vínculos familiares de los empleados y los beneficios a los que ellos tienen, a parte en la sede de Pamplona brinda otros servicios como por ejemplo un jardín infantil entre otros servicios de educación.

También se toma como población la infraestructura tecnológica de COMFAORIENTE. Se tiene en cuenta las listas de recurso humano y con ayuda de la base de la empresa se obtiene la muestra, que es la totalidad de los equipos

6.5. TÉCNICAS DE RECOLECCIÓN DE DATOS

Se toman como técnicas de recolección de datos en este trabajo, instrumentos cualitativos como la observación, las entrevistas semiestructuradas y el Hacking ético.

El hacking ético es una herramienta de prevención y protección de datos. Lo que se pretende es estar constantemente adelante de aquellos que nos intentan agredir haciendo pruebas y ataques propios con la ayuda de los expertos

informáticos, los cuales han sido entrenados en la mentalidad delictiva de los piratas informáticos así como en las diferentes técnicas de ataque digital.[51]

Para la recolección de datos se realizará visitas a las oficinas de COMFAORIENTE sede Pamplona, y se procederá a recolectar la información requerida, mediante entrevista semiestructurada esto incluirá el formular una serie de preguntas a cada uno de los empleados acerca del uso de la información en sus equipos y que tipo de software usan para realizar las operaciones en especial las financieras, estas preguntas también incluirán inquietudes acerca del uso de redes sociales, correos electrónicos personales, uso de dispositivos extraíbles personales en los equipos de trabajo, entre otros. En este proyecto se debe hacer una serie de inspecciones técnicas a los diferentes equipos utilizados en red y todas las instalaciones para verificar y enumerar las diferentes partes de la red y determinar el sistema operativo de los equipos de cómputo y demás software que se utilice en las oficinas.

Es importante diseñar y aplicar un instrumento de entrevista semiestructurada con las cuales se tomaran datos por parte de los funcionario encargados.
Y se diligenciaran formatos de observación para realizar los inventarios y otros documentos necesarios para el diagnóstico.

6.6. INSTRUMENTOS DE RECOLECCION DE DATOS

Se debe realizar un análisis técnico de la red, de los equipos y de los recursos informáticos con diferentes herramientas de software como lo son Wireshark y Nmap para encontrar las debilidades de la red de información.

Entrevista semiestructurada a funcionario de COMFAORIENTE

51 http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

7. ESQUEMA TEMATICO

7.1. ACTIVOS, VULNERABILIDADES, AMENAZAS E IMPACTOS.

7.1.1. Inventario de los Activos. En el inventario realizado a cada sector de las oficinas de COMFAORIENTE sede Pamplona, se verificó mediante la observación cada uno de los equipos informáticos registrando sus características y afinidades a los recursos de la red presentes.

Tabla 1. Inventario de los Activos COMFAORIENTE sede Pamplona.

OFICINAS	EQUIPOS	CARACTERISTICAS	Dispositivo	UPS	CONEXIÓN A INTERNET
Capacitación	1. HP Compag 6000 pro A.O Business PC	Procesador: Pentium (R) puatico CPU E5800@3,70Hz Memoria RAM: 2,00GB Tipo de sistema operativo de 32bits Nombre de equipoPAM-04.ad.comfaoriente.com Dominio: ad.comfaoriente.com Sistema operativo: Windows 7 Profesional	3 en oficina 2 fuera conexión a la red eléctrica	internet office 500- no funcional	LAN

OFICINAS	EQUIPOS	CARACTERISTICAS	Dispositivo	UPS	CONEXIÓN A INTERNET
Secretaria	1.PAM.01 HP 100-5110la 2. .PAM.05 HP 100-5110la	Los dos tienen las mismas carcateristicas. Sistema operativo Windows 7 Basic Fabricante: Driver Pack Solution Modelo: HP 100-5110la Procesador: AMD Athbn™ 4x2 260$_u$procesador 1,80 RAM: 3,00GB (2,75 utilizable)32 bits	2 no conectado a la red interna	interne t offic e 500no funcional	LAN
Subsidio	1.PAM 02 HP Compag 6000 pro A.O Business PC Panasoni c . Elec tric modular switching system	Procesador: Pentium (R) puatico CPU E5800@3,70Hz Memoria RAM: 2,00GB Tipo de sistema operativo de 32bits Nombre de equipoPAM-04.ad.comfaoriente.com Dominio: ad.comfaoriente.com Sistema operativo: Windows 7 Profesional Disco 2901 router AMP Notconnect XG catGA HP Siwitch V1910-249	conectados al equipo 2en oficina 2 fuera Entrada de línea telefónica	interne t offic e 500no funcional	LAN WIFI

OFICINAS	EQUIPOS	CARACTERISTICAS	Dispositivo	UPS	CONEXIÓN A INTERNET
Servicio de empleo	1.Em Pam o1 2.Em Pam 02 3.Em Pam	Todos con las mismas características. Fabricante : HP Modulo: HP Pro One 400 61ª;O Evaluación 5.0 Procesador: Intel (R) Corg (TM) i;-4160T	1-2 fuera 2-1 0ficina 2 fuera	NO NO NO	LAN
		CPU@3,106 Hz RAM 4,00GB Sistema 64 bits Sistema Operativo: Windows 7 professional	3-1 0ficina 2 fuera		

7.1.2. Valoración de los Activos. Para determinar el valor de cada activo y clasificarlo se tuvo en cuenta la importancia que tiene para la sede y para la organización, los siguientes criterios estipulados en la tabla 4 muestran la valoración de activos en donde se verifica el ítem, el valor y la descripción.

Tabla 2. Criterio para valoración de activos

Valor cualitativo para la Sede	Valor	Descripción
Mb: muy bajo	Cuantitativo1	No es indispensable
B: bajo	2	Indispensable, alguna tarea.
M: medio	3	Importante para varias tareas.
A: Alto	4	Muy importante. Paraliza algunas
Ma: muy alto	5	Áreas. Su falta genera parálisis en la operación.

7.2. ANÁLISIS DE VULNERABILIDADES

Las vulnerabilidades constituyen debilidades presentes en los activos de COMFAORIENTE sede Pamplona, estas pueden ser explotadas por las amenazas lo que causa en realidad incidentes nada favorables a la seguridad o deterioro a los activos, por si sola la vulnerabilidad no causa fallas, pero si genera el ambiente para que se materialicen las amenazas. En esta parte se analizan las vulnerabilidades y se obtiene como resultado una matriz de vulnerabilidades presentes en los activos de la institución.

7.2.1. Análisis a los sistemas operativos. Se realizan mediante pruebas de penetración (Pentesting), escaneo de la red, escaneo de puertos y pruebas de vulnerabilidades realizadas y en el área de redes y sistemas de sede, cabe anotar que solo se permitió realizar un escaneo a la red con una herramienta de monitoreo. (el análisis está en el ítem 5.4)

7.2.2. Resultados y vulnerabilidades encontradas. En el análisis realizado mediante el escaneo a la red se encontraron vulnerabilidades asociadas al manejo y gestión de archivos, en este sentido se puede observar en la zona sombreada como existe un árbol de carpetas al cual se puede acceder sin ninguna restricción, también se encontraron problemas asociados con hardware.

7.2.3. Análisis al Recurso Humano. Respecto al factor humano se indaga sobre las personas midiendo el nivel de conocimiento en el manejo y uso de la información y de los dispositivos computacionales tanto hardware como software.

Se implementa la siguiente encuesta para detectar las vulnerabilidades:

Tabla 3. Encuesta al personal para determinar vulnerabilidades

Pregunta	Si	No	N/A
1. ¿El equipo cuenta con contraseña para su ingreso?			

2. ¿Cuenta con software (antivirus) de protección para el ingreso de memorias (usb)?			
3. ¿Todas las personas pueden ingresar memoria (usb)?			
4. ¿Se dan claves de WiFi?			
5. ¿Los equipos tienen conexión por wifi?			
6. ¿Existen dos redes de internet Wifi comfaOpam, COMFAORIENTE?			
7. ¿Todos los documentos en físico que ya no se utilizan son desechados sin una destrucción previa?			
8. ¿Se recomienda por parte de la empresa ingresar o no memorias?			
9. ¿Se puede acceder al correo personal como a diferentes páginas web?			
10. ¿Se cuenta con un software de chat interno?			
11. ¿Se puede llevar algún tipo de trabajo a la casa?			
12. ¿Las conexiones eléctricas de los equipos se encuentran en mal estado?			
13. ¿Las UPS's están en funcionamiento?			
Pregunta Si No N/A			
14. ¿El software utilizado se puede abrir en sitios diferentes de las oficinas?			

7.2.4. Inventario de los equipos y recursos relacionados con el manejo del sistema de información. Mediante observación realizada en visitas en todas las instalaciones de COMFAORIENTE y entrevista a funcionario, se encuentra que no existe un inventario de equipos, por lo que se decide realizar el inventario de manera manual, verificando los datos de todos los equipos. Como se observa en la tabla. 1.

Se encontró como se visualiza en la tabla No. 1. Que existen 4 oficinas en la parte administrativa, Capacitación, Secretaria, Subsidio y servicio de empleo y 7 computadores en total.

Tabla 4. Criterio para valoración de activos

Valor cualitativo para la Sede	Valor Cuantitativo	Descripción
Mb: muy bajo	1	No es indispensable
B: bajo	2	Indispensable, alguna tarea.
M: medio	3	Importante para varias tareas.
A: Alto	4	Muy importante. Paraliza algunas
Ma: muy alto	5	Su falta genera parálisis en la

7.3 ANÁLISIS DE VULNERABILIDADES

Las vulnerabilidades constituyen debilidades presentes en los activos de COMFAORIENTE sede Pamplona, estas pueden ser explotadas por las amenazas lo que causa en realidad incidentes nada favorables a la seguridad o deterioro a los activos, por si sola la vulnerabilidad no causa fallas, pero si genera el ambiente para que se materialicen las amenazas. En esta parte se analizan las vulnerabilidades y se obtiene como resultado una matriz de vulnerabilidades presentes en los activos de la institución.

7.3.1 Análisis a los sistemas operativos. Se realizan mediante pruebas de penetración (Pentesting), escaneo de la red, escaneo de puertos y pruebas de vulnerabilidades realizadas y en el área de redes y sistemas de sede, cabe anotar que solo se permitió realizar un escaneo a la red con una herramienta de monitoreo.

7.3.2. Resultados y vulnerabilidades encontradas. En el análisis realizado mediante el escaneo a la red se encontraron vulnerabilidades asociadas al manejo y gestión de archivos, en este sentido se puede observar en la zona sombreada como existe un árbol de carpetas al cual se puede acceder sin ninguna restricción, también se encontraron problemas asociados con hardware.

7.3.3. Análisis al Recurso Humano. Respecto al factor humano se indaga sobre las personas midiendo el nivel de conocimiento en el manejo y uso de la información y

de los dispositivos computacionales tanto hardware como software. Mediante la encuesta que aparece en la Tabla 3.

Tabla 5. Resultados de la encuesta

No. Pregunta	No. Personas entrevistadas	Personas que respondieron Si	Personas que respondieron No	Personas que no respondieron
1	8	0	8	0
2	8	8	0	0
3	8	4	4	0
4	8	0	8	0
5	8	0	8	0
6	8	8	0	0
7	8	8	0	0
8	8	0	8	0
9	8	8	0	0
10	8	8	0	0
11	8	0	8	0
12	8	8	0	0
13	8	0	8	0
14	8	0	8	0

Según los resultados de la encuesta se determinan las siguientes vulnerabilidades:

- Falta de medidas de seguridad que protejan la información de personas dentro de las oficinas.

- Problemas con los equipos que pueden evitar daños eléctricos en los computadores de cada una de las oficinas.

7.4. DESCRIBIR LA INFRAESTRUCTURA TECNOLÓGICA PRESENTE EN LA ORGANIZACIÓN.

De acuerdo a lo observado en las visitas a las instalaciones de COMFAORIENTE, después de definir algunos conceptos básicos en la materia se describirán las características de la infraestructura, empezando por manifestar que la infraestructura de tecnología de información es la arquitectura de hardware y software que compone red de comunicación y manejo de datos de una empresa, institución, oficinas, entre otros tipos de entidades en este caso las oficinas de COMFAORIENTE que se encuentran en Pamplona ya que es una sede de la central que se encuentra en Cúcuta, Norte de Santander. La infraestructura de tecnología de información cuenta con los siguientes elementos básicos:

- Centros de datos.
- Servidores y clientes.
- Dispositivos de red.
- Medios de comunicación.
- Tipos de redes de datos.

Cada uno de estos elementos es de vital importancia para el bueno manejo de información de manera eficiente y con la mayor rapidez para la atención de los clientes, por lo que se conceptualizaran así:

7.4.1. Centros De Datos. Es un espacio físico donde se albergan servidores y equipos de redes los cuales debido a su importancia requieren control de acceso que permitan solo el paso a personal autorizado, enfriamiento debido a que por su trabajo suele calentarse por ejemplo se suelen utilizar aires acondicionados y fuentes de energía de respaldo como lo pueden ser UPS’s (uninterruptible power supply por sus siglas en inglés), o plantas eléctricas que se alimentan con diesel y de esta forma evitar daños o pérdidas de información.

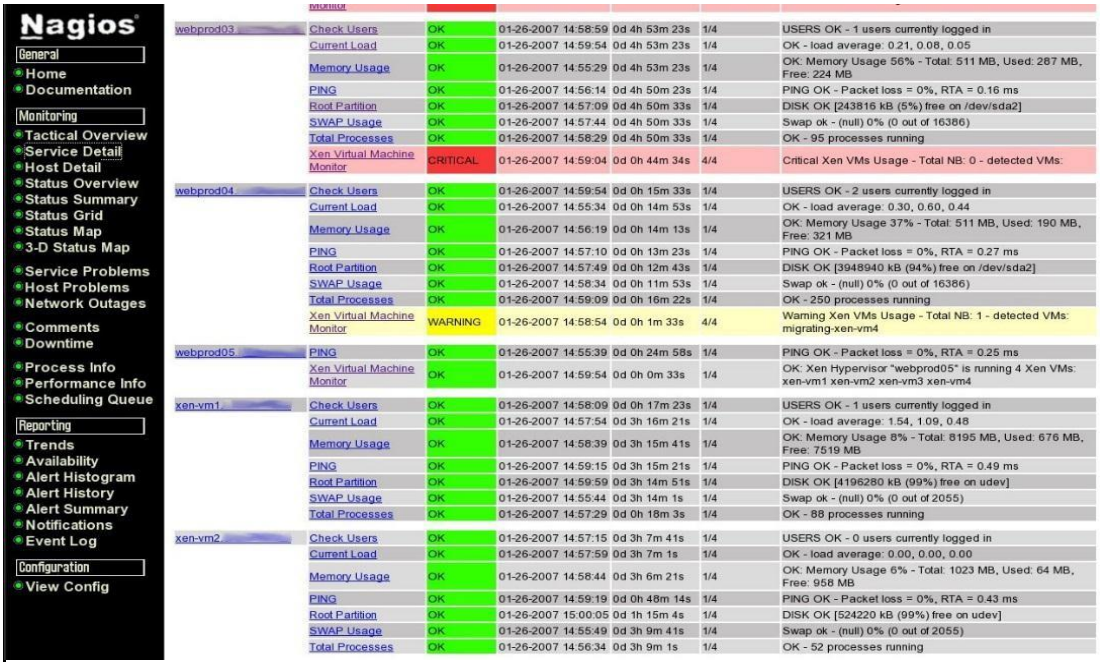
Usualmente los servidores y equipos de red se encuentran ubicados u organizados en gabinetes o “racks” que son estructuras verticales, los centros de

datos varían de tamaño dependiendo de la complejidad de las operaciones con el manejo de la información o por el tamaño de la empresa.

En estos centros de datos se encuentra el administrador de sistemas que generalmente es un ingeniero que se encarga del control de estos equipos y de la configuración de los mismos y por lo tanto tiene una gran importancia para la empresa así como responsabilidades, en algunos casos estos centros de datos no son tan organizados como deberían ser y por tanto complica el trabajo del administrador que cumple funciones como lo es el de diagramar para tener un mapa de cómo está organizada la arquitectura de la empresa.

Existen diferentes tipos de software que permiten diagramar y algunos hasta monitorear el estado de cada uno de los dispositivos que se encuentran en red y de esta forma gestionar el centro de datos.

Figura 8. Nagios



webprod03	Check Users	OK	01-26-2007 14:58:59	0d 4h 53m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:59:54	0d 4h 53m 23s	1/4	OK - load average: 0.21, 0.08, 0.05
	Memory Usage	OK	01-26-2007 14:55:29	0d 4h 53m 23s	1/4	OK: Memory Usage 56% - Total: 511 MB, Used: 287 MB, Free: 224 MB
	PING	OK	01-26-2007 14:56:14	0d 4h 50m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Root Partition	OK	01-26-2007 14:57:09	0d 4h 50m 33s	1/4	DISK OK [243816 kB (5%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:57:44	0d 4h 50m 33s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:58:29	0d 4h 50m 33s	1/4	OK - 95 processes running
	Xen Virtual Machine Monitor	CRITICAL	01-26-2007 14:59:04	0d 0h 44m 34s	4/4	Critical Xen VMs Usage - Total NB: 0 - detected VMs:
webprod04	Check Users	OK	01-26-2007 14:59:54	0d 0h 15m 33s	1/4	USERS OK - 2 users currently logged in
	Current Load	OK	01-26-2007 14:55:34	0d 0h 14m 53s	1/4	OK - load average: 0.30, 0.60, 0.44
	Memory Usage	OK	01-26-2007 14:56:19	0d 0h 14m 13s	1/4	OK: Memory Usage 37% - Total: 511 MB, Used: 190 MB, Free: 321 MB
	PING	OK	01-26-2007 14:57:10	0d 0h 13m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.27 ms
	Root Partition	OK	01-26-2007 14:57:49	0d 0h 12m 43s	1/4	DISK OK [3948940 kB (94%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:58:34	0d 0h 11m 53s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:59:09	0d 0h 16m 22s	1/4	OK - 250 processes running
	Xen Virtual Machine Monitor	WARNING	01-26-2007 14:58:54	0d 0h 1m 33s	4/4	Warning Xen VMs Usage - Total NB: 1 - detected VMs: migrating-xen-vm4
webprod05	PING	OK	01-26-2007 14:55:39	0d 0h 24m 58s	1/4	PING OK - Packet loss = 0%, RTA = 0.25 ms
	Xen Virtual Machine Monitor	OK	01-26-2007 14:59:54	0d 0h 0m 33s	1/4	OK: Xen Hypervisor "webprod05" is running 4 Xen VMs: xen-vm1 xen-vm2 xen-vm3 xen-vm4
xen-vm1	Check Users	OK	01-26-2007 14:58:09	0d 0h 17m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:57:54	0d 3h 16m 21s	1/4	OK - load average: 1.54, 1.09, 0.48
	Memory Usage	OK	01-26-2007 14:58:39	0d 3h 15m 41s	1/4	OK: Memory Usage 8% - Total: 8195 MB, Used: 676 MB, Free: 7519 MB
	PING	OK	01-26-2007 14:59:15	0d 3h 15m 21s	1/4	PING OK - Packet loss = 0%, RTA = 0.49 ms
	Root Partition	OK	01-26-2007 14:59:59	0d 3h 14m 51s	1/4	DISK OK [4196280 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:44	0d 3h 14m 1s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:57:29	0d 0h 18m 3s	1/4	OK - 88 processes running
xen-vm2	Check Users	OK	01-26-2007 14:57:15	0d 3h 7m 41s	1/4	USERS OK - 0 users currently logged in
	Current Load	OK	01-26-2007 14:57:59	0d 3h 7m 1s	1/4	OK - load average: 0.00, 0.00, 0.00
	Memory Usage	OK	01-26-2007 14:58:44	0d 3h 6m 21s	1/4	OK: Memory Usage 6% - Total: 1023 MB, Used: 64 MB, Free: 958 MB
	PING	OK	01-26-2007 14:59:19	0d 0h 48m 14s	1/4	PING OK - Packet loss = 0%, RTA = 0.43 ms
	Root Partition	OK	01-26-2007 15:00:05	0d 1h 15m 4s	1/4	DISK OK [524220 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:49	0d 3h 9m 41s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:56:34	0d 3h 9m 1s	1/4	OK - 52 processes running

Fuente: https://medium.com/linux-monitoring-with-nagios/what-is-nagios-64e547db57ca

7.4.2. Componentes de una LAN (Local Área Network). Para establecer una red se necesitan una serie de componentes y dispositivos que cumplen diferentes

funciones y tiene un unificador que facilita la comunicación entre todos estos dispositivos.

Figura 9. Componentes de una LAN

Fuente: https://es.123rf.com/photo_23981313_lan-diagrama-de-red-illustrator-paraconcepto-negocios-y-tecnologia.html

En la figura 6 anterior se pueden observar los dispositivos básicos que se pueden encontrar en una empresa como lo son los servidores, equipos de redes, clientes y la conexión a internet.

7.4.3. Servidores. Un servidor es una computadora que cuenta con el mismo hardware que un equipo personal como por ejemplo procesador, disco duro, memorias, entre otros, pero con la diferencia que sus especificaciones son más robustas y también cumplen funciones específicas como lo son proveer datos o correr aplicaciones para el uso de los clientes.

Los servidores son llamados de diferentes formas y estos nombres los reciben teniendo en cuenta la función que cumplen, estos son:

7.4.4. Servidor de archivo. Este se utiliza para almacenar archivos, documentos, imágenes entre otros. Algunos software utilizados para estos servidores son *Samba* que corre sobre Linux y que permite que los computadores con cualquier plataforma bien sean Windows, mac o Linux puedan acceder a estos archivos; o también un servidor FTP (File Transfer Protocol por sus siglas en inglés) el cual es un protocolo clásico para este tipo de acciones como lo son copiar, pegar y mover archivos.

7.4.5. Servidor de Impresión. Son aquellos servidores que ayudan a realizar la conexión de la impresora o impresoras a la red para que cualquier equipo pueda enviar realizar una impresión.

7.4.6. Servidor Web. Son aquellos servidores que permiten servir páginas web, el más utilizado es *Apache* el cual es Open Source, *Nginx*, y Microsoft IIS este último es el menos utilizado.

7.4.7. Servidor de Aplicaciones. Estos servidores son los encargados de correr las aplicaciones de la empresa como por ejemplo SAP (Sistemas, Aplicaciones y Procesos).

7.4.8. Servidor de Correo. Son los servidores que soportan los correos electrónicos de las empresas, estos antes de que se utilizara la nube para este fin.

7.4.9. Servidor de Bases de Datos. Este servidor es clásico y se puede encontrar en casi todas las empresas ya que es donde se gestionan todas las bases de datos, estos se pueden basar en *Microsoft SQL*, *Oracle*, *MySQL* o *Maria DB*.

7.4.10. Servidor de Medios. Este servidor se encarga de servir de videos y audios al público.

7.4.11. Servidor de Colaboración. Este servidor en donde los clientes se conectan para poder interactuar entre sí, utilizan *Microsoft SharePoint* y *IBM Lotus*.

Si se habla con mayor tecnicismo los servidores los podemos nombrar según sus características que se refieren a su Hardware y Sistema Operativo, hardware como marca y modelo y sistemas operativos como *Microsoft Windows Server*, *Redhat*, *Linux* o *Unix*; por ejemplo IBM P-Series con Linux o Dell PowerEdge con Windows.

7.4.12. Clientes. Son todos aquellos dispositivos (hardware) que permiten la entrada y salida de información y son utilizados por los usuarios finales en general es cualquier dispositivo que se usa para conectarse a un servidor o a otros

clientes, los ejemplos más comunes que se encuentran son los PC's y laptos, pero también se pueden encontrar otro tipo de dispositivos como lo son terminales transaccionales ATM y POS, así como teléfonos inteligentes, tablets, relojes, entre otros.

7.4.13. Dispositivos de Red. Son aquellos dispositivos que permiten la conexión de los clientes con los servidores y la interacción de los mismos con el internet, estos son los siguientes:

- Switch.
- Acces Point.
- Router.

7.4.14. Swtich. Es un punto fundamental de interconexión en la red local ya que todos los dispositivos que se encuentran en esta se conectan gracias al swtich

Figura 10. Switch

Fuente: https://www.zyxel.com/co/es/products_services/smb-switches.shtml?t=c

7.4.15. Access Point. Es el dispositivo que permite conectarse inalámbricamente a los clientes a la red.

Figura 11. Access Point

Fuente:https://www.tutorialspoint.com/wireless_security/wireless_security_access_point.htm

7.4.16. Router. Es un equipo de hardware mediante el cual todo el tráfico de red local se interconecta con otras redes o con el internet en general con cualquier red externa de la red local.

Figura 12. Router

Fuente: http://www.nobbot.com/pantallas/tecnologia-forense-un-router-por-dentro/

7.4.17. Medios de Comunicación. Todos los elementos nombrados anteriormente como los servidores, clientes y dispositivos de red tienen que tener una forma de comunicarse y estos son los medios de comunicación los cuales son:

Cable.
Inalámbrico.

7.4.18. Cable. El cable de red se asemeja a un cable telefónico al cual denominamos UTP (Unshielded Twisted Pair, por sus siglas en inglés) se denominan así por ser cables trenzados no blindados, y el socket por el cual se conecta es un RJ45.

Otro tipo de cable utilizado es el cable coaxial que se usa en cable modem y debido a sus características de protección puede transmitir información a mayores distancias y mayores velocidades.

A medida que avanza la tecnología se trata de cambiar el cobre para pasar a las fibras ópticas.

7.4.19. Inalámbrico. La tecnología inalámbrica más popular es el WiFi, las señales WiFi son ondas electromagnéticas que como cualquier otra señal de radio están expuestas a interferencia como por ejemplo al encender un horno microondas cerca al Access point de una red de área local esta se verá afectada.

Otra tecnología inalámbrica es la utilizada por las compañías de telefonía móvil como lo son las redes 3G y 4G, así como también se pueden utilizar las señales de microondas y las señales satelitales.

7.4.20. Tipos de Redes. Los tipos de redes se pueden categorizar dependiendo de su extensión geográfica, estos son:

- LAN.
- Backbone.
- MAN.
- WAN.
-

7.4.21. LAN. Local Area Network por sus siglas en inglés, la cual contiene servidores, clientes, Access point, switch, impresoras y routers para salir de LAN, este puede ser utilizado para interconectar un cuarto hasta un edificio, las velocidades de esta red van a oscilar entre 100 Mbps a 1 Gbps.

7.4.22. Backbone. Este contiene LANs, switches o routers de alta velocidad, circuitos de altas velocidades (en fibra óptica) para interconectar LANs, su extensión es menor a unos cuantos kilómetros y las velocidades de este oscilan de 1 a 40 Gbps.

7.4.23. MAN. Metropolitan Area Network por sus siglas en inglés, LANs, BNs, circuitos arrendados a proveedores públicos y microondas, su extensión es de más de unos cuantos kilómetros, generalmente son caros y como alternativa se puede usar el internet, las velocidades oscilan entre 64 Kbps y 10 GBps.

7.4.24. WAN. World Area Network por sus siglas en inglés, la cual contiene los mismos componentes de la MAN pero a mayor distancia, su extensión es mayor a las decenas de kilómetros usualmente internacionales, las velocidades oscilan entre los 64 Kbps y 10 GBps.

También se pueden categorizar los tipos de red como intranet y extranet.

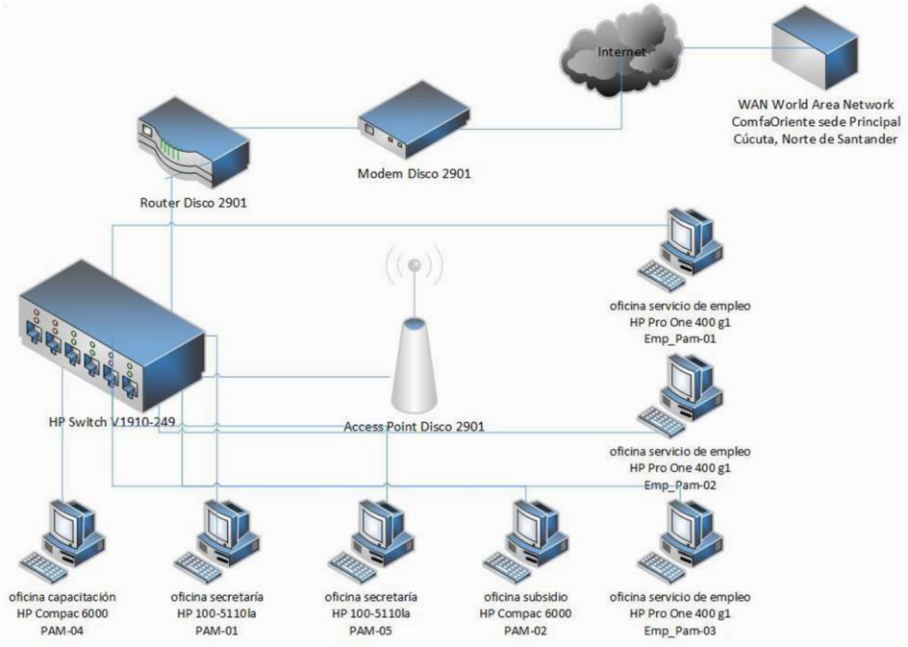
7.4.25. Intranet. Es una red donde solo los miembros internos de una organización tienen acceso, es decir los que se encuentran conectados en la LAN o MAN se puede decir que están en la intranet, sin embargo existen medios de encriptación y cifrados que permiten la conexión desde lugares de internet público, cafeterías, entre otros, a la intranet.

7.4.26. Extranet. Es una red que es accesible por entes externos a la organización como pueden ser clientes, proveedores entre otros, estos pueden acceder a la página web de comercio electrónico y redes WiFi para clientes

7.5. INFRAESTRUCTURA TECNOLÓGICA DE COMFAORIENTE

Para representar la infraestructura tecnológica de la información de COMFAORIENTE en la sede de Pamplona se utilizará el software Microsoft Visio Professional.

Figura 13. Diagrama de la infraestructura TI



Fuente: autor

En las oficinas de COMFAORIENTE sede Pamplona se contrató el servicio de internet con la empresa Movistar, estas oficinas cuentan con siete equipos en total que fueron descritos en el inventario los cuales se conectaban a la red LAN con medio de cable debido que es la única forma de conexión a la red permitida la cual se llama *comfaOpam*, ya que la conexión vía WiFi no está permitida en ningún equipo con el fin de que no se filtre la contraseña y así evitar que otros dispositivos diferentes a los encontrados en las oficinas accedan y puedan extraer información por alguna falla de seguridad.

En las oficinas no se encuentra un servidor debido a que la central se halla en la ciudad de Cúcuta, Norte de Santander, por lo tanto la LAN de las oficinas de Pamplona depende directamente de la WAN.

7.6. EJECUTAR UN HACKING ÉTICO A LOS SISTEMAS DE INFORMACIÓN PARA ESTABLECER VULNERABILIDADES.

Después de tener el inventario y conocer la infraestructura de COMFAORIENTE, se procede a ejecutar el hacking ético, que es una herramienta

de prevención y protección de datos. Lo que se pretende es estar constantemente adelante de aquellos que nos intentan agredir haciendo pruebas y ataques propios con la ayuda de los expertos informáticos, los cuales han sido entrenados en la mentalidad delictiva de los piratas informáticos así como en las diferentes técnicas de ataque digital.

Además con el hacking ético se utilizan de los conocimientos de seguridad en informática para realizar pruebas en sistemas, redes o dispositivos electrónicos, buscando vulnerabilidades que explotar, con el fin de reportarlas para tomar medidas sin poner en riesgo el sistema.

Es importante aclarar que para ejecutar hacking ético es importante tener en cuenta la Vulnerabilidades del Recurso Humano.

En una empresa, oficina y demás organizaciones, es bueno recordar que no solo los recursos informáticos son los que ponen en riesgo la seguridad de la información sino que también las personas que trabajan en estos sitios la pueden colocar en riego debido a ciertas prácticas que pueden ser nocivas sin saberlo.

Para poder establecer que prácticas se realizan por parte del personal que atentan contra la seguridad de la información en las oficinas de COMFAORIENTE sede Pamplona se hace una ingeniería social y se encuentra que es recurrente y se identifica gracias a la técnica del *Trashing*.

Como se ha descrito Trashing consiste en una técnica de ingeniería social presencial no agresiva, que tiene como propósito escudriñar o buscar en las papeleras o en cestas de basura de las oficinas de una organización con el fin de encontrar documentos importantes, privados, datos personales, extractos bancarios, facturas de servicios y demás información que sirva al atacante obtener información para documentar e implementar otro tipo de ataque. (SEGURIDAD, e. (Octubre de 2014). Debilidades de seguridad comúnmente explotadas. [52]

52 https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

El Procedimiento para el implementar la técnica de ingeniería social para extraer información en una de las oficinas de la alcaldía municipal es el siguiente:

- Encontrar una papelera en una oficina importante.

- Se escoge una de las oficinas con más importancia en cuanto a la gestión y el manejo de información importante.

- Se solicita permiso de ingreso a la persona que se encuentra presente indicándole que se está llevando a cabo una campaña de reciclaje del papel y por ende que si es posible le permita tomar los papeles desechos en la cesta, cuando el funcionario accede se pasa la basura de la cesta a una bolsa y se lleva a otro sitio para ser analizada.

- En otro lugar se saca la basura de la bolsa y se clasifica entre hojas completas, hojas cortadas y papeles de notas.

- Las hojas rotas se intentan unir para darle forma original y visualizar su contenido. • Se Clasifican los papeles, ordenando los documentos encontrados

Se encontró que en los documentos encontrados había mucha información de alto nivel que colocaba en riesgo la seguridad de la información de la oficina y por ende se recomienda destruir estos documentos de forma definitiva antes de ser puestos en el bote de basura.

Para cumplir con este objetivo, en primer lugar se describen a continuación las pruebas de penetración (pentesting), escaneo de la red, escaneo de puertos y pruebas de vulnerabilidades, es importante aclarar que se pretendía realizar estas pruebas en las oficinas de COMFAORIENTE sede Pamplona, pero debido a que el control informático no se realiza en la sede estudiada, sino que se supervisa desde la sede principal que se encuentra ubicada en Cúcuta, Norte de Santander no se permitió realizar estas pruebas directamente en los equipos, por este motivo se hace la prueba simulada desde otra red para hacer ver las posibles falencias que se tienen.

Las pruebas de NetBIOS se realizaron con el software Network Scanner a equipos con sistemas operativos Windows 7, ya que los equipos utilizados en estas oficinas tienen este sistema operativo.

Para comprender un poco más lo que se realizó es necesario tener claro el concepto de lo que es NetBIOS.Network Basic Input/output System sobre lo cual se puede decir que se dio inicio en 1984 con IBM, con colaboración con Microsoft, donde anunciaron el desarrollo del Network Basic Input/Output System (NETBIOS), un código catalizador inicio el desarrollo de redes de comunicación. NetBIOS sobre TCP/IP, se conoce también como NBT o NetBT, es el protocolo que ha sido utilizado por Microsoft para la transmisión de bloques de mensajes de servidores, o SMBs por sus siglas en Ingles, y es esta instalado en todos los sistemas operativos Windows. (Blogs, T. (23 de Junio de 2009). NetBIOS sobre TCP/IP y resolución de nombres cortos. [53]

Para los sistemas operativos Windows NetBIOS sobre TCP/IP se entiende como el componente de red que resuelve y asigna los nombres de equipo a dirección IP (NETBT.SYS en Windows NT, y VNBT.VXD en Windows para Trabajo en Grupo y Windows 95). Por lo general utiliza los puertos del 135 al 139 el servicio NetBIOS que se encarga de compartir ficheros del computador, en la red interna. (MICROSOFT. (2014). Resolución de nombres de NetBIOS sobre TCP/IP y WINS.[54]

Una de las vulnerabilidades más conocida es el ataque por NetBIOS en los sistemas de Windows, esta constituye en una falla de seguridad al momento de compartir información en una red de datos, el ataque por NetBIOS es una de las intrusiones más conocidas.

Para este trabajo se utilizó un portátil con sistema operativo Windows 7, cables de red UTP y tarjetas de red inalámbrica para establecer conexión con la red y se

53 http://blogs.technet.com/b/latam/archive/2009/01/23/netbios-sobre-tcp-ip-y-resoluci-n-de-nombrescortos.aspx)

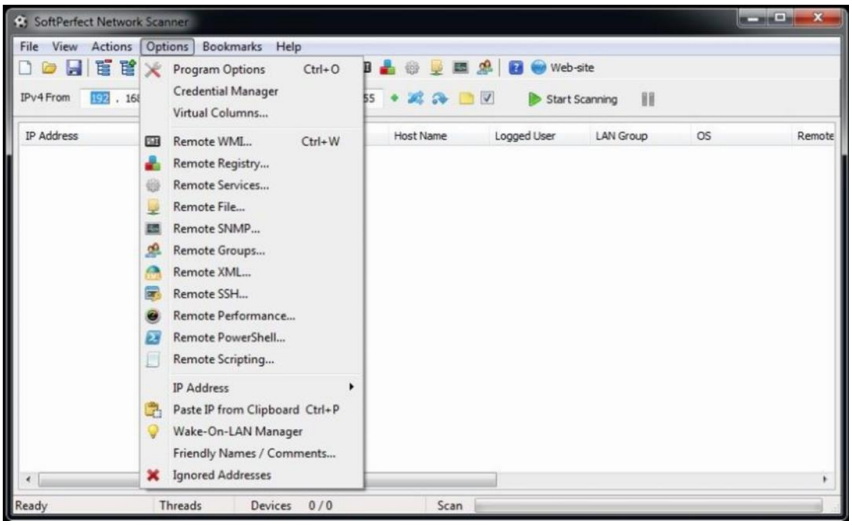
54 https://support.microsoft.com/es-es/kb/119493/es

utilizó el software Network Scanner que se descarga de la página https://www.softperfect.com/products/Network Scanner/.

Se descarga el archivo se descomprime y se procede a abrir el software, hay que tener en cuenta que se tiene que tomar a consideración si el equipo es de arquitectura de 32 Bits o de 64 Bits.

Al instalar Network Scanner se genera un acceso directo en el escritorio desde donde se puede acceder a programa, lo abrimos y se ve la siguiente interfaz.

Figura 14. Interfaz Network Scanner



Fuente: autor

Se conecta el equipo portatil con el cual se realiza el escaneo al switch de la red de datos, se utiliza un cable de conexión (patch cord) UTP, sigla que significa Unshielded Twisted Pair (Par trenzado no blindado) y se realizan los siguientes pasos:

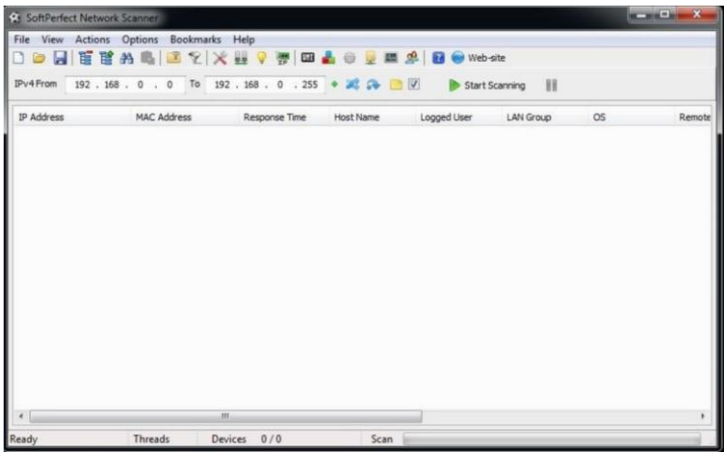
- Obtener una dirección IP de la misma red a la cual se va a escanear, esto se puede realizar con el mismo Network Scanner.

- Verificar el rango de IPs de la subred a la que pertenece la máquina.

- Conectada, se deduce su tamaño y el segmento para indicar el rango en las casillas “IPv4 from” de la aplicación.

- Se configura el rango de IPs en las casillas correspondientes como lo indica la siguiente figura 12 en donde se aprecian los equipos conectados.

Figura 15. Rango de IPs

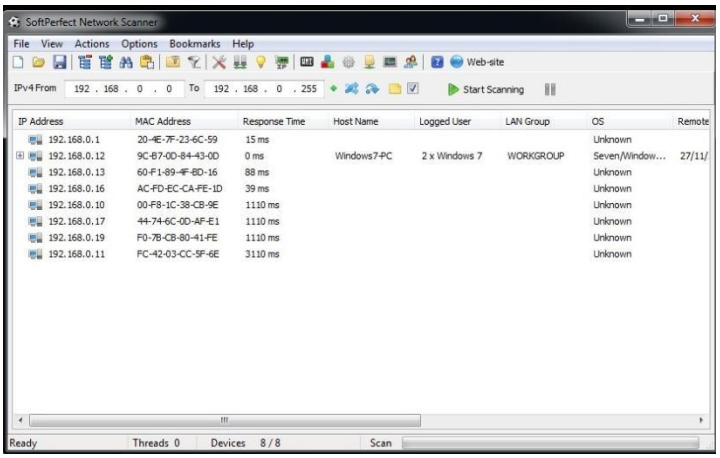


Fuente: autor

Se inicia el escáner de la red dando click en el botón Start Scanning y se obtienen los siguientes resultados.

Se obtiene la lista de equipos escaneados

Figura 16. Resultado del escaneo



Fuente: autor

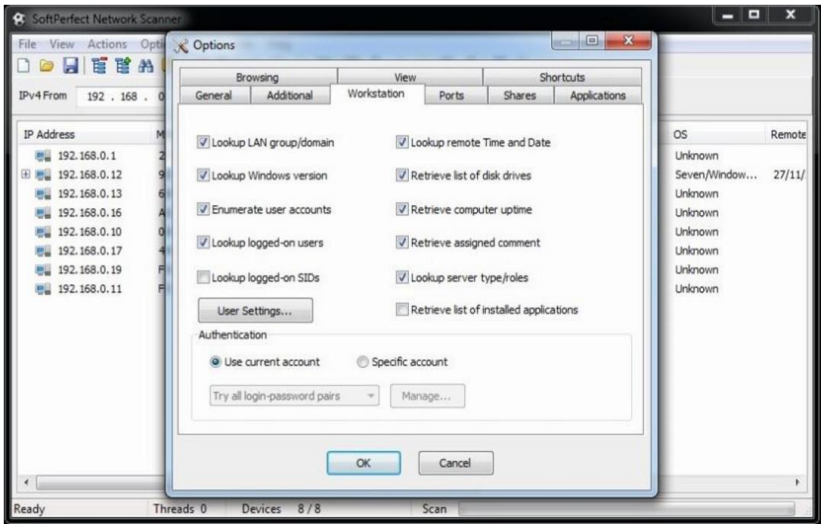
En la ventana de resultados se encuentra la lista de 8 equipos conectados sobre los cuales se obtiene la siguiente información de cada uno:

- Dirección Ip, nombre del equipo, dirección física o MAC, tiempo de respuesta, grupo de trabajo al que pertenece.

- Sistema operativo, espacio total y disponible de cada unidad de disco duro y estado de los puertos NetBIOS.

La información obtenida de cada equipo es posible configurarla mediante el menú Options, en donde se encuentran las pestañas de Network Scanner como se muestra en la siguiente figura.

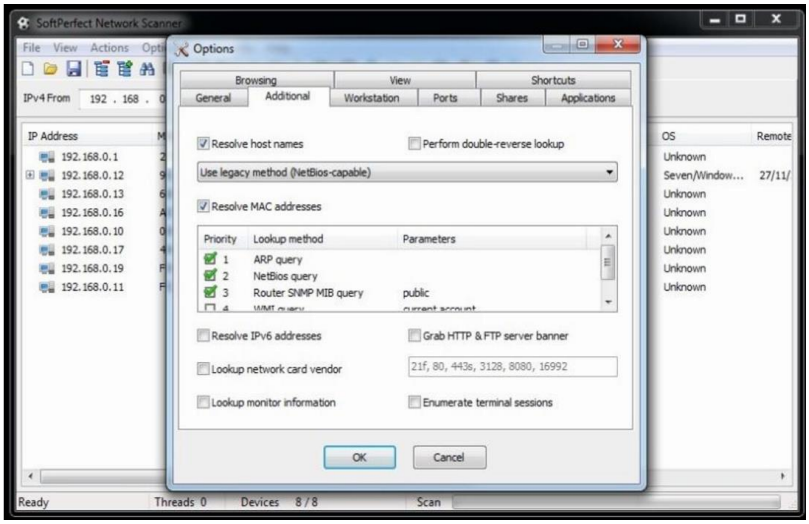
Figura 17. Workstation Network Scanner



Fuente: autor

Pestaña Workstation mediante la cual se selecciona las características sobre las cuales se desea información del equipo escaneado.

Figura 18. Additional Network Scanner



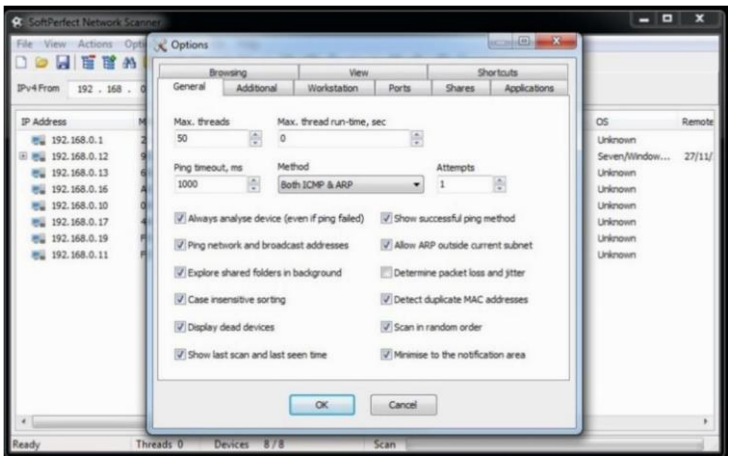
Fuente: autor

Pestaña Additional mediante la cual se selecciona la forma como la aplicación recupera parámetros y usa métodos para obtener información de los equipos escaneados. La configuración de los datos se realiza en base a una configuración

personalizada con el propósito de obtener suficiente información de un equipo, esto quiere decir que de acuerdo a los datos que se necesiten se configura la búsqueda.

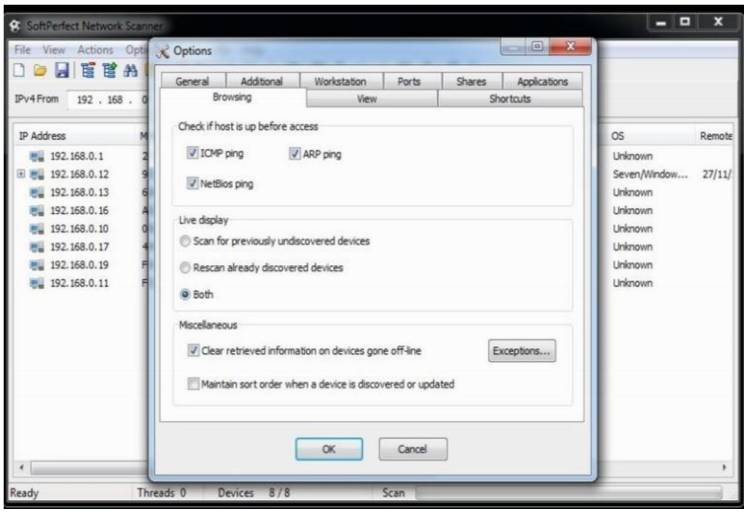
Por medio de la pestaña General se indica la forma de realizar el escaneo configurando los parámetros con el fin de optimizar los resultados. Como se muestra en las siguientes figuras, la pestaña Browsing se configura la búsqueda de los equipos en la red y el uso de los protocolos para ello

Figura 19. General Network Scanner



Fuente: autor

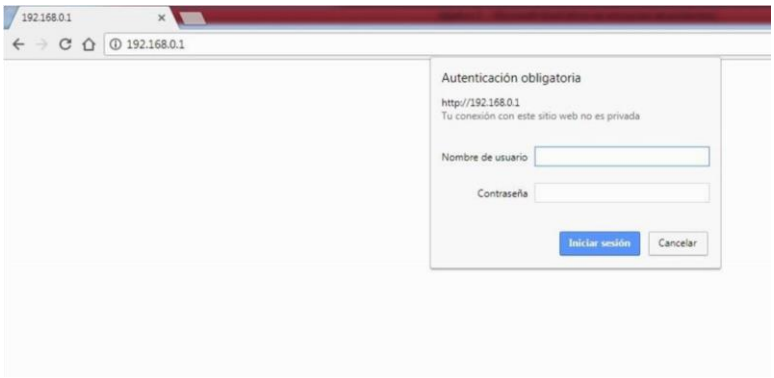
Figura 20. Browsing Network Scanner



Fuente: autor

Como Resultado del proceso de escaneo en la red seleccionada se identifican el servidor DHCP (protocolo de configuración dinámica de host) se registra un servidor (192.168.0.1) se deduce que además del modem ADSL el cual se verifica visualmente ingresando a la ventana de configuración del mismo como se ilustra en la siguiente figura.

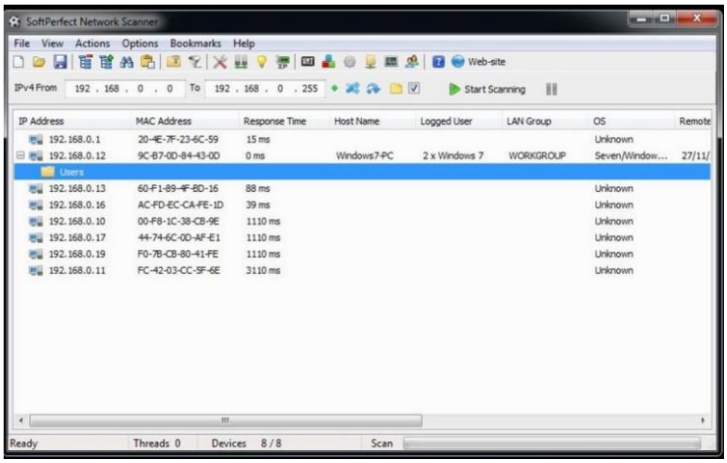
Figura 21. Interfaz Modem ADSL



Fuente: autor

EL resultado del análisis y despliegue de cada equipo analizado se muestra y evidencia que en la red hay equipos que tienen carpetas compartidas lo cual evidencia en la siguiente figura. Esto también ocurre en las oficinas de COMFAORIENTE en donde sus equipos se encuentran en red.

Figura 22. Resultado escaneo carpetas compartidas



Fuente: autor

Se determina que el equipo Windows 7-PC del grupo LAN WORKGROUP con Windows 7 comparte 1 carpeta. Equipo con NetBIOS Activo. Por ende esta carpeta puede ser vista por los demás equipos en esta red y también se puede copiar, pegar y mover información que en esta carpeta se encuentre. Por este motivo es aconsejable desactivar la NetBIOS.

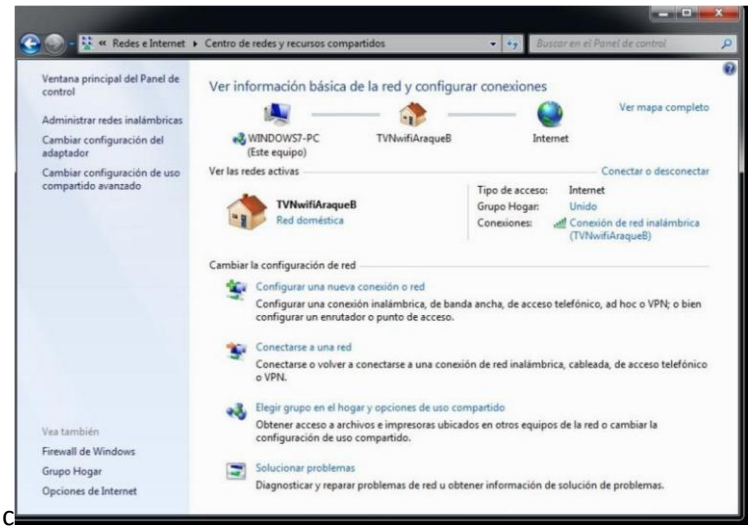
En Windows 7 haga clic en Inicio y, a continuación, haga clic en Panel de control. En Red e Internet, haga clic en Ver estado de la red y las tareas.

- Haga clic en Cambiar configuración del adaptador.

- Haga clic en Conexión de área local y a continuación, haga clic en Propiedades. En Esta conexión utiliza la lista siguientes elementos, haga doble clic en Protocolo de Internet versión 4 (TCP / IPv4), haga clic en Opciones avanzadas y, a continuación, haga clic en la ficha WINS.

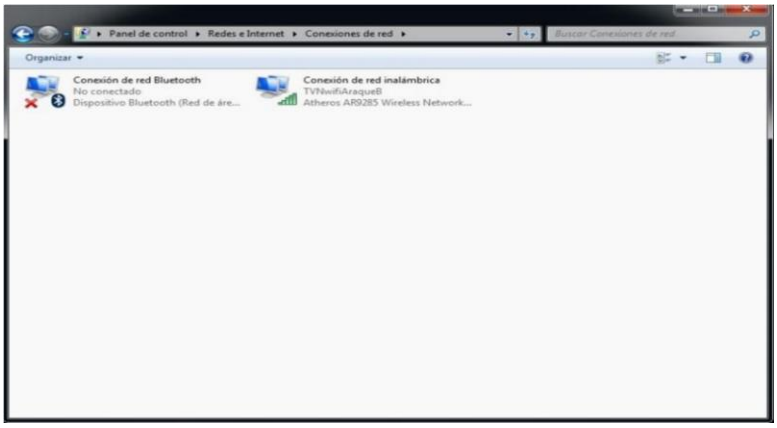
- Haga clic en configuración de uso de NetBIOS del servidor DHCP y, a continuación, haga clic en Aceptar tres veces, en las siguientes figuras se muestra la secuencia de pasos para desactivar NetBIOS.

Figura 23. Desactivar NetBIOS paso 1



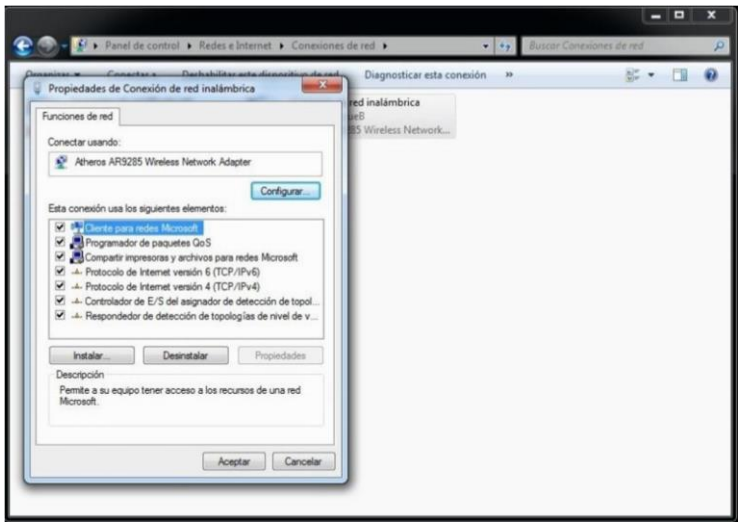
Fuente: autor

Figura 24. Desactivar NetBIOS paso 2



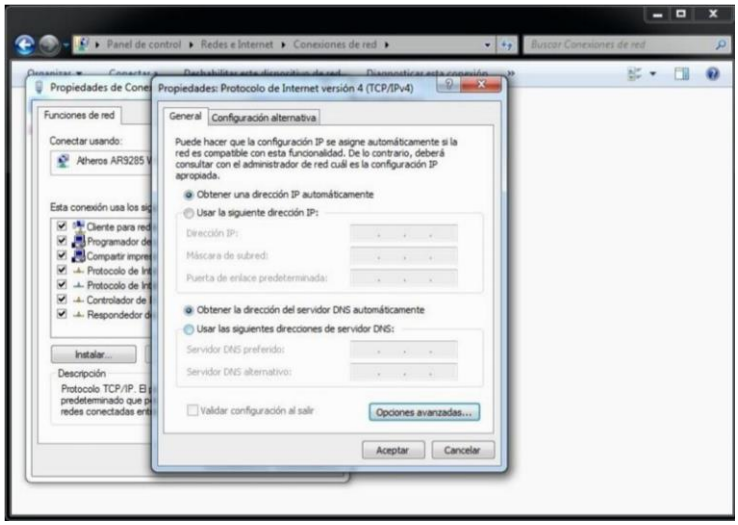
Fuente: autor

Figura 25. Desactivar NetBIOS paso 3



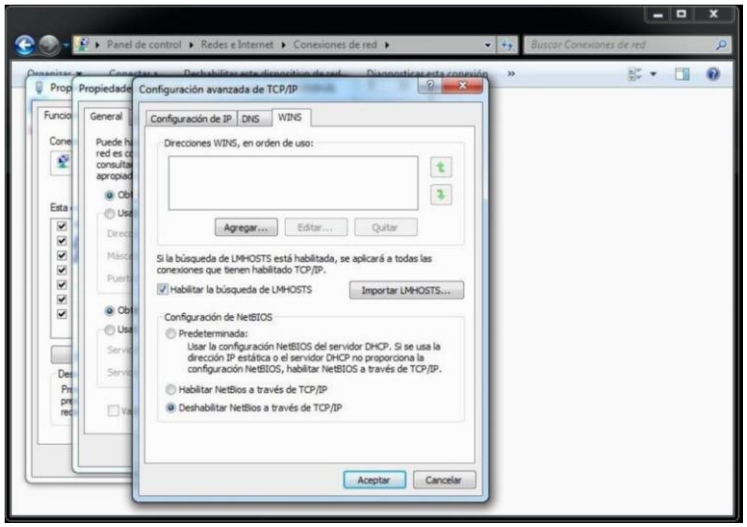
Fuente: autor

Figura 26. Desactivar NetBIOS paso 4



Fuente: autor

Figura 27. Desactivar NetBIOS paso 5



Fuente: autor

Luego de analizar el puerto de NetBIOS, se continúan las pruebas de análisis de puertos con el programa Nmap, para abordar esta etapa del análisis de la red de datos es necesario conocer las variables y parámetros sobre los cuales se obtendrá resultados por medio de las aplicaciones.

Para ejecutar el procedimiento de escaneo: se realiza la descarga del programa Nmap de la página: https://nmap.org/dist/nmap-6.47-setup.exe y se inicia la instalación de Nmap.

El programa necesita ser instalado en el equipo desde el cual se realizara el escaneo, se instalada como cualquier otro programa en Windows siguiendo intuitivamente los pasos y luego ejecutando el acceso directo que el instalador ubica en el escritorio del sistema operativo en este caso Windows 7. Luego de la instalación se ejecuta el programa desde el acceso directo creado en el escritorio del equipo; inmediatamente abre la interfaz principal del programa mediante la cual se ejecutan todas las acciones y eventos que conlleva la realización del escaneo a la red; antes de iniciar es preciso configurar o ingresar los parámetros las casillas disponibles en la interfaz del programa:

- Se conecta la máquina al switch de la red de datos.
- Se utiliza un Cable de conexión (patch cord) UTP.
- Obtener una dirección IP de la misma red a la cual se va a escanear.
- Verificando el rango de IPs de la subred a la que pertenece la máquina conectada, se deduce su tamaño y el segmento para indicar el rango en las casillas “Target” de la aplicación.
- Se indica al programa el tipo de escaneo en la casilla Command “nmap -T4 -A –v” con este parámetro se indica al programa que realice un mapeo de forma agresiva con una plantilla de tiempos y que imprime la versión de Nmap y finalice la ejecución.
- En la casilla Profile, seleccionar el nivel y las variable que se van a usar para el mapeo de la red, dependiendo del perfil el programa gasta un tiempo determinado. Se dispone de un listado completo de comandos, de acuerdo a lo que se pretenda conseguir con el escaneo se combinan los comandos para obtener los resultados.

En esta instancia se analiza la Red 192.168.0.1 como indica en la siguiente figura.

Figura 27. Interfaz Nmap

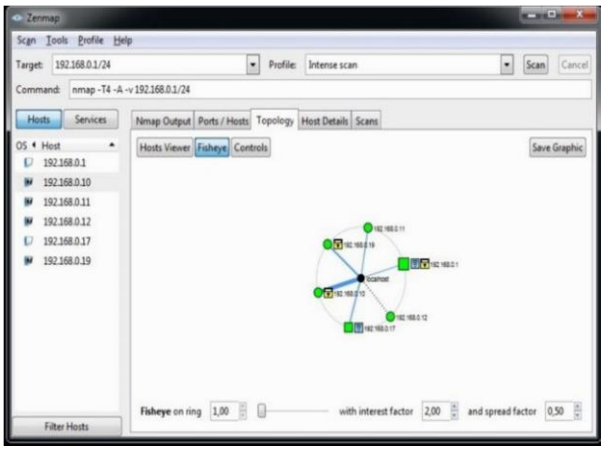
Figura 28. Interfaz Nmap

Fuente: autor

Con el escaneo configurado se procede a iniciar dando click con el botón “Scan”, de acuerdo al tamaño de la red y la cantidad de equipos es el tiempo que demorara en dar los resultados finales.

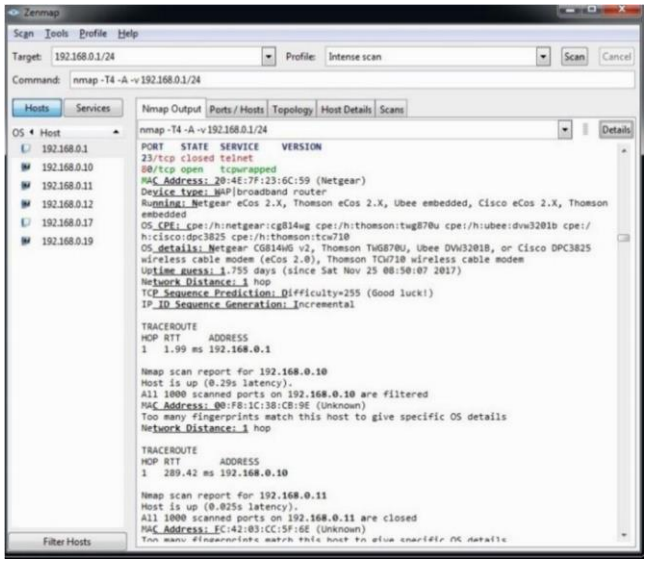
En la siguiente figura se ilustra el complejo de la red que el programa Nmap analiza, para cada equipo se ejecutara el mismo comando para recuperar la información que imprime Nmap.

Figura 29. Topología Nmap



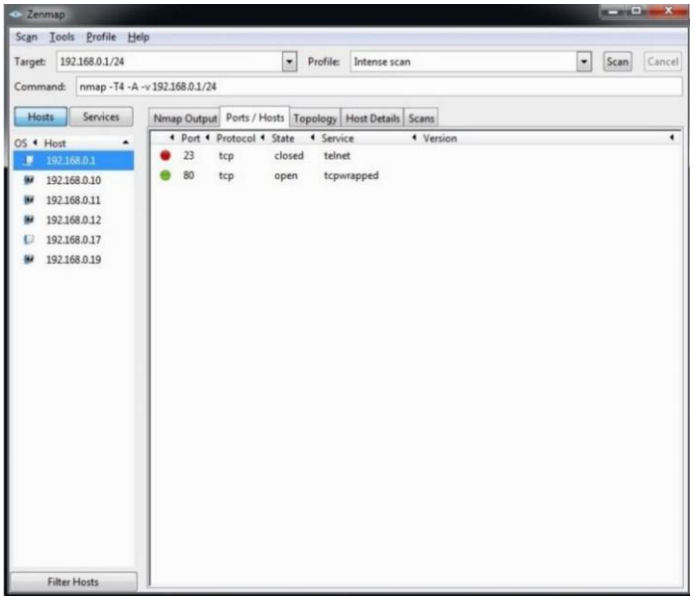
Fuente: autor

Figura 30. Nmap Output



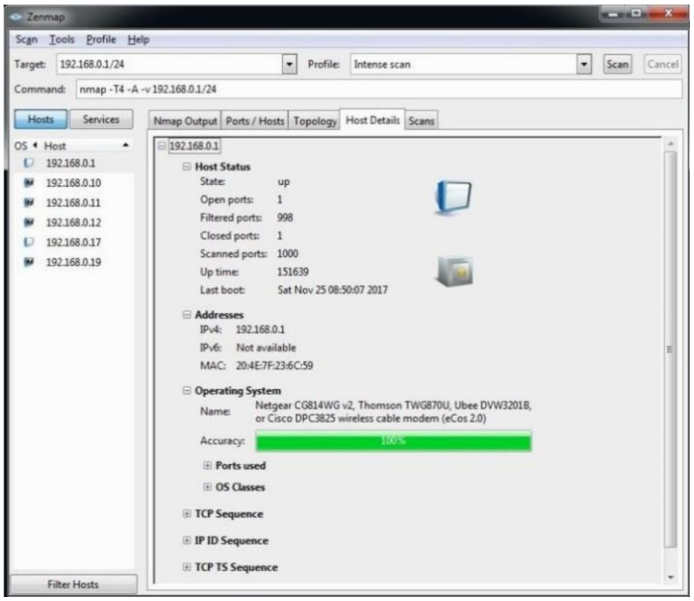
Fuente: autor

Figura 31. Ports/Hosts Nmap



Fuente: autor

Figura 32. Host Details



Fuente: autor

En estas figuras observamos el análisis completo de la red y se puede observar que el puerto 80 se encuentra abierto lo cual es una falla de seguridad que puede afectar a los equipos en esta red.

A continuación se puede observar parte del análisis hecho por Nmap.

Initiating Parallel DNS resolution of 1 host. at 02:51
Completed Parallel DNS resolution of 1 host. at 02:52, 11.14s elapsed
Initiating SYN Stealth Scan at 02:52
Scanning 5 hosts [1000 ports/host]
Completed SYN Stealth Scan against 192.168.0.17 in 1.41s (4 hosts left)
Discovered open port 80/tcp on 192.168.0.1
SYN Stealth Scan Timing: About 42.35% done; ETC: 02:53 (0:00:42 remaining)
SYN Stealth Scan Timing: About 53.96% done; ETC: 02:54 (0:00:57 remaining)
SYN Stealth Scan Timing: About 74.13% done; ETC: 02:54 (0:00:40 remaining)
Completed SYN Stealth Scan against 192.168.0.11 in 146.10s (3 hosts left)
Completed SYN Stealth Scan against 192.168.0.1 in 147.15s (2 hosts left)
Completed SYN Stealth Scan against 192.168.0.10 in 161.78s (1 host left)
Completed SYN Stealth Scan at 02:54, 168.33s elapsed (5000 total ports)
Initiating Service scan at 02:54
Scanning 1 service on 5 hosts
Completed Service scan at 02:54, 0.30s elapsed (1 service on 5 hosts)

Initiating OS detection (try #1) against 5 hosts

Retrying OS detection (try #2) against 4 hosts

NSE: Script scanning 5 hosts.
Initiating NSE at 02:55

Completed NSE at 02:57, 140.48s elapsed

Nmap scan report for 192.168.0.1

Host is up (0.0020s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

23/tcp closed telnet

80/tcp open tcpwrapped

MAC Address: 20:4E:7F:23:6C:59 (Netgear)

Device type: WAP|broadband router

Running: Netgear eCos 2.X, Thomson eCos 2.X, Ubee embedded, Cisco eCos 2.X, Thomson embedded

OS CPE: cpe:/h:netgear:cg814wg cpe:/h:thomson:twg870u cpe:/h:ubee:dvw3201b cpe:/h:cisco:dpc3825 cpe:/h:thomson:tcw710

OS details: Netgear CG814WG v2, Thomson TWG870U, Ubee DVW3201B, or Cisco

DPC3825 wireless cable modem (eCos 2.0), Thomson TCW710 wireless cable modem

Uptime guess: 1.755 days (since Sat Nov 25 08:50:07 2017)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=255 (Good luck!)

IP ID Sequence Generation: Incremental

TRACEROUTE

HOP RTT ADDRESS

1 1.99 ms 192.168.0.1

Nmap scan report for 192.168.0.10 Host
is up (0.29s latency).

All 1000 scanned ports on 192.168.0.10 are filtered

MAC Address: 00:F8:1C:38:CB:9E (Unknown)
Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 289.42 ms 192.168.0.10

Nmap scan report for 192.168.0.11 Host
is up (0.025s latency).

All 1000 scanned ports on 192.168.0.11 are closed

MAC Address: FC:42:03:CC:5F:6E (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 24.67 ms 192.168.0.11

Nmap scan report for 192.168.0.17 Host is up (0.052s latency).

All 1000 scanned ports on 192.168.0.17 are closed

MAC Address: 44:74:6C:0D:AF:E1 (Sony Mobile Communications AB)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Aruba IAP-93 WAP (98%), Gargoyle router firmware 1.5.10 (Linux 3.3) (98%), Linksys RV042 router (98%), Linux 2.6.18 (98%), Linux 2.6.18 - 2.6.24 (98%), Linux 2.6.23 (Gentoo) (98%), Linux 2.6.35 (98%), OpenWrt (Linux 2.6.32) (98%), Nokia N900 mobile phone (Linux 2.6.28) (98%), SonicWALL Aventail EX-6000 VPN appliance (98%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 51.51 ms 192.168.0.17

Nmap scan report for 192.168.0.19 Host is up (0.087s latency).

All 1000 scanned ports on 192.168.0.19 are filtered

MAC Address: F0:7B:CB:80:41:FE (Hon Hai Precision Ind. Co.)

Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 87.00 ms 192.168.0.19

Skipping SYN Stealth Scan against 192.168.0.12 because Windows does not support scanning your own machine (localhost) this way.

Initiating Service scan at 02:57

Skipping OS Scan against 192.168.0.12 because it doesn't work against your own machine (localhost)

NSE: Script scanning 192.168.0.12.

Initiating NSE at 02:57

Completed NSE at 02:57, 0.00s elapsed
Nmap scan report for 192.168.0.12 Host is up.

7.7. ESTABLECER UN CONJUNTO DE CONTROLES QUE PERMITAN CONTRARRESTAR LAS FALENCIAS ENCONTRADAS EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN.

En el desarrollo del análisis y evaluación de riesgos en las oficinas de COMFAORIENTE de la seccional Pamplona se encontraron ciertas vulnerabilidades y riesgos que deben tener acciones correctivas para evitar pérdidas de información, filtración de información o afectaciones en el desarrollo del trabajo que se realiza.

Estas vulnerabilidades y riesgos se enlistan y se les da recomendaciones para evitar seguir cometiendo los mismos errores en la siguiente tabla.

7.7.1. Relación de las vulnerabilidades y amenazas detectadas. A través de las diferentes formas de encontrar la información en las de COMFAORIENTE Pamplona, mediante el análisis se evidenciaran y se identificaron las vulnerabilidades y las amenazas, las cuales forman parte de la matriz de riesgos en donde se clasifican los recursos estudiados, los cuales están conformados por los activos analizados de donde se derivan las vulnerabilidades.

Para la determinar la probabilidad de materialización de las amenazas y el impacto en consecuencia, se efectúan los siguientes pasos.

7.7.2. Matriz para el análisis de riesgo. La Probabilidad que se ejecute la amenaza y la Magnitud del daño pueden tomar los valores y condiciones respectivamente (1-4), por lo tanto la valoración de los riesgos resulta de los siguientes factores:

- Probabilidad. Tiene una escala de 1 a 4, siendo 1 una probabilidad muy baja de que se materialice la amenaza y 4 la más alta probabilidad.

- Impacto. Tiene una escala de 1 a 4, siendo 1 el menor impacto con mínimas consecuencias de afectación al activo y 4 un impacto con consecuencias graves, en relevancia del activo para la institución.

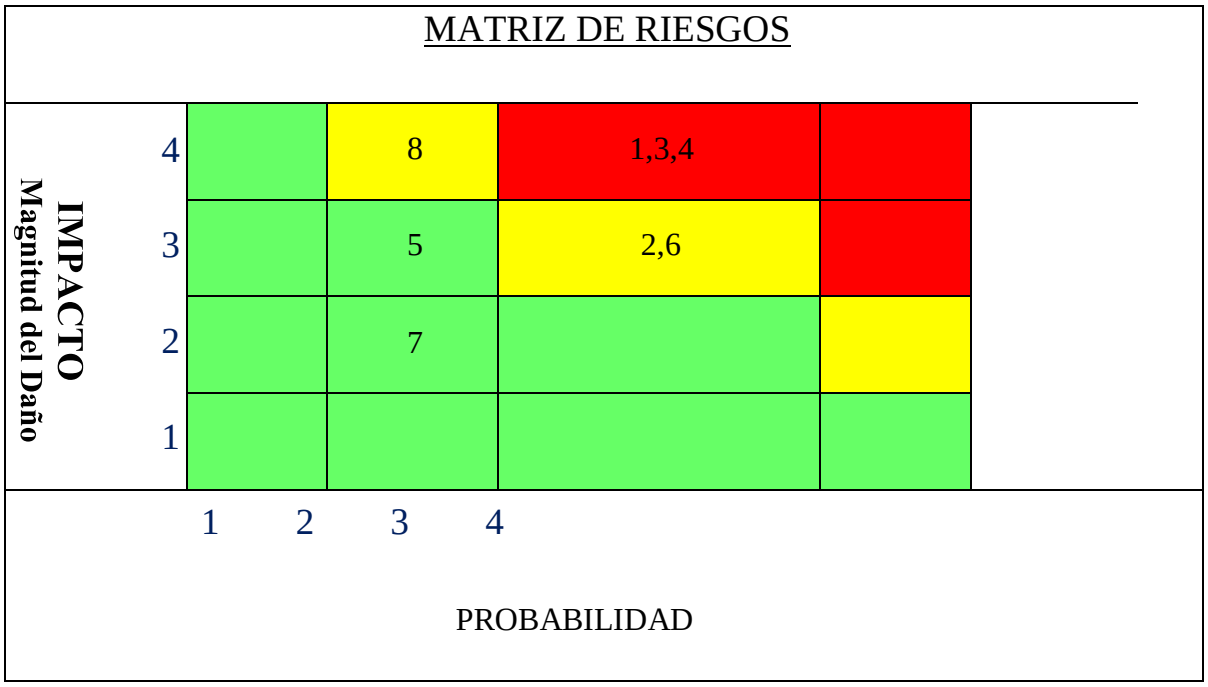
Calculo del riesgo total. Teniendo en cuenta los valores tomados respectivamente por la probabilidad y el impacto se multiplican y se obtiene un valor total del riesgo en la escala de 1-16.

- **Cuadro 1. Matriz para el análisis de riesgo**

Campo	Ítem	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valoración Total del Riesgo
					1	2	3	4	1	2	3	4	
Software	1	Mal manejo de las políticas de Backup	Pérdida de información	Pérdida de información			X					X	12
	2	Malas prácticas en el uso del internet	Acceso a correos electrónicos personales entre otras páginas web	Ataques informáticos y software malicioso			X				X		9
Hardware	3	Falta de seguridad física e infraestructura	Acceso a personal no autorizada	Robo de equipos y negación del servicio			X					X	12
	4	Mal funcionamiento de las UPS	Fallas eléctricas	Daño de equipos críticos			X					X	12
	5	Malas conexiones en los toma corrientes	Fallas eléctricas	Daño de equipos críticos		X					X		6
dispositivas de red Comunicaciones Inalámbricos	6	Fallos al cifrar la información	Desencriptar información para mejorar la seguridad	Robo de información			X				X		9
	7	Red de datos abierta	Escucha de paquetes por terceros	Robo de información		X				X			4
Seguridad	8	Falta de control de acceso	Accesos no autorizados	Pérdida de información o equipos		X						X	8

7.7.3. Matriz de clasificación del riesgo. Luego del análisis del riesgo realizado en la tabla anterior los valores calculados como “valor total del riesgo”, se deben clasificar para determinar su nivel de gestión y/o tratamiento, de acuerdo a los parámetros que estable la matriz de clasificación del riesgo, dicho proceso se muestra a continuación:

Cuadro 2. Matriz de clasificación del riesgo



7.7.4. Clasificación del riesgo. Con el resultado de la matriz anterior es posible distinguir y especificar los riesgos que requiere determinada gestión.

Cuadro 3. Clasificación de los riesgos encontrados

Ítem	Riesgo	Clasificación del riesgo
2	Malas prácticas en el uso del internet.	Riesgos que necesitan Investigación: Planes de actuación Preventivos. Mejorar condición.
6	Fallos al cifrar la información.	
8	Falta de control de acceso.	
1	Mal manejo de las políticas de Backup.	Riesgos que necesitan Mitigación: Planes de actuación correctivos, Gestión Urgente
3	Falta de seguridad física e infraestructura.	
4	Mal funcionamiento de las UPS.	
5	Malas conexiones en los toma corrientes.	Riesgos que necesitan Monitorización: Planes de

7	Red de datos abierta.	actuación Detectivos, Riesgo Aceptable

Gracias a los análisis realizados a los diferentes equipos y redes de las oficinas se pueden dar las siguientes recomendaciones, en donde se busca sensibilizar y contribuir al mejoramiento de las políticas de seguridad para disminuir las vulnerabilidades que están generando riesgo al óptimo funcionamiento y tratamiento de la información, dando algunas pautas y buenos manejos puntualizando en controles que disminuyan la probabilidad de los riesgos encontrados.

7.8. PLAN DE TRATAMIENTO DE RIESGOS

En adelante en el presente capítulo se adoptan los controles y/o políticas, con lo cual se busca sensibilizar y contribuir al saneamiento de las vulnerabilidades que están generando riesgo a los pilares de la seguridad informática (Integridad, confidencialidad y disponibilidad) de COMFAORIENTE Pamplona para el óptimo funcionamiento de los medios, recursos y gestión de la información, mejorando el espectro de la operación de los recursos físicos, dispositivos inalámbricos, orientación al recurso y optimización de la configuración de los sistemas operativos.

7.8.1. ISO 27002. Código de buenas prácticas. Publicado el 1 de julio de 2007. Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información. En cuanto a seguridad de la información. La ISO 27002, contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Esta norma se encuentra publicada en Español a través de la empresa AENOR y en Colombia NTCISO IEC 27002, así mismo se pueden encontrar en Perú, chile, entre otros países latinoamericanos, (Español, E. p. 2012).

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799 vigente, es un manual de prácticas para la seguridad de la información. Describe los controles y mecanismos, que pueden ser implementados, en base a la orientación proporcionada en la norma ISO 27001.

Los controles que figuran en esta norma están destinados a suplir las necesidades específicas identificadas a través de una evaluación formal de riesgos. La norma también tiene por objeto proporcionar una guía para el desarrollo de "normas de seguridad de la organización y las prácticas eficaces de gestión de la seguridad y para ayudar a construir la confianza en las actividades inter-organizacionales". En 2013 se publicó la versión actual. ISO 27002: 2013 contiene 114 controles, en comparación con el 133 documentado dentro de la versión 2005, (ISO 27000 Directory, 2013).

Toda organización que desee resguardar la información debe implementar un Sistema de Gestión de seguridad de la Información (SGSI), que constantemente esté evaluando la organización en busca de soluciones de seguridad de la entidad tratando con esto la mejora continua en para los sistemas. Un SGSI basado en la Norma NTC/ISO 27001 brinda las pautas para implementar un sistema de esta calidad así como también busca dirigir a la organización hacia un clima general de seguridad en todos los niveles.

Figura 33. DO tratamiento de los Riesgos

Fuente: http://www.iso27000.es/sgsi_implantar.html

En este paso se procede a seleccionar los objetivos de control y los controles del Anexo A de ISO 27001:2005 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo. Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI. Hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación final en cada revisión y/o acciones de tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

Definir una declaración de aplicabilidad también llamada SOA (Statement of Applicability) que incluya:

- Los objetivos de control y controles seleccionados y los motivos para su elección.

- Los objetivos de control y controles que actualmente ya están implantados.

- Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001:2005, en su segunda cláusula, en términos de "documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

Figura 34. Tratamiento de los riesgos

Fuente: http://www.iso27000.es/sgsi_implantar.html

7.8.2Controles. La definición que la norma ISO 31000:2011 da a conocer del concepto de "Control", el que se define en ésta norma como "Medida que modifica al riesgo" y además señala que "Los controles incluyen procesos, políticas, dispositivos, prácticas u otras acciones que modifican al riesgo". En este ítem se deben describir los controles existentes dentro del proceso o procedimiento, tendientes a mitigar el riesgo identificado. Para facilitar esta identificación se debe recurrir a la revisión de los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones. Pedagógica y metodológicamente, los controles existentes se clasifican en a)

Preventivos: Aquellos que actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización, y b) Correctivos: Aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia. Contribuyen a facilitar la mitigación del riesgo y así mismo se caracterizan porque se aplican continuamente en el respectivo proceso y procedimiento, deben ser evidenciables, medibles y concretos. Adicionalmente, esta es una variable de suma importancia, porque a través de ella se mitiga el riesgo potencial y de su correcta identificación y registro, permite contrarrestar los efectos negativos del riesgo residual.

7.8.3. Acción de mitigación del riesgo. Es el control de controles a implementarse en una vigencia. Es el conjunto de las principales actividades que se formularán y emplearán para mitigar el riesgo, pueden ser acciones preventivas o correctivas contra cada riesgo, definiendo acciones factibles y efectivas, tales como Ej.: la implantación de políticas, estándares, procedimientos y cambios físicos, entre otros, así mismo deben ser efectivas para evitar que éste se materialice; cada acción de mitigación debe ser pertinente teniéndose en cuenta la gobernabilidad y competencia de COMFAORIENTE.

7.8.4. Periodicidad de la acción de mitigación. Debe registrarse la periodicidad se llevará a cabo la acción de mitigación del riesgo, con una única asignación de periodicidad, así: diaria, semanal, mensual, bimestral, trimestral, cuatrimestral y semestral.

7.8.5. Seguimiento del riesgo. El responsable debe reportar el seguimiento del avance de las acciones de mitigación.

7.8.6. Por qué implementar controles. Las empresas, si bien están constituidas por activos físicos -edificios e infraestructura-, y activos de información contenido digital, muchas de las compañías administran los riesgos de seguridad físicos y de información como entidades separadas y distintas, lo que puede implicar pérdida de oportunidades. Adicionalmente, las empresas deben evitar una serie de riesgos de seguridad, entre los que incluyen robo de identidad, fuga de información, fraude y otros, por lo que es necesario contar con un marco de gobernabilidad en relación a la seguridad de la información (Burgos Salaza & Campos, 2009).

Figura 35. Modelo del plan para el tratamiento del riesgo

Fuente: http://www.iso27000.es/

7.8.7. Estructuración completa del plan de tratamiento. En este paso se consultan los controles y se adjudican a los riesgos de acuerdo al dominio en que se estos se presentan, en este sentido se parte de la vulnerabilidad y la amenaza que genera el riesgo, estos parámetros se analizaron en la Tabla 8. Matriz para el análisis de riesgo, en la cual cada riesgo está clasificado en un ítem, el plan de tratamiento se soportan en los dominios, objetivos de control y controles de la norma ISO 27002 y NTC-ISO-IEC 27001 (Primera actualización) ANEXO A (Tienda Icontec, 2006), cada uno de los riesgo tiene redactado su control como lo expresa el cuadro.

Cuadro 4. Controles

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
1	Malas prácticas en el uso del internet.	Riesgos que necesitan Investigación: Planes de actuación Preventivos. Mejorar condición.	Dominio: 14. Adquisición, desarrollo y mantenimiento de los sistemas de información. Objetivo de Control: 14.2. Seguridad en los procesos de desarrollo y soporte. Control: 14.2.2 Procedimientos de control de cambios en los sistemas.	Se realiza configuración para actualizaciones periódicas del sistema Operativas, programadas Cada Lunes, miércoles y viernes. En este proceso el sistema crea un archivo bitácora como seguimiento a las novedades y versiones.	La instalación la realiza el tecnólogo, encargado del soporte y mantenimiento de la infraestructura tecnológica del Centro.
2	Fallos al cifrar la información.		Dominio: 12. Seguridad en la operativa. Objetivo de Control: 12.6 Gestión de la vulnerabilidad técnica. Control: 12.6.2 Restricciones en la instalación de software.	Configuración local para que todos y cada uno de los equipos requieran autenticación de usuario con privilegios para la instalación de software autorizado.	Los privilegios de instalación los tiene la cuenta de usuario del tecnólogo, si se requiere determinada aplicación el funcionario solicita autorización a soporte.
3	Falta de control de acceso.		Dominio: 11. Seguridad física y ambiental. Objetivo de Control: 11.2 Seguridad de los equipos. Control: 11.2.1 Emplazamiento y protección de equipos.	Asegurar con cerradura Rack en puertas frontal y posterior reversibles y paneles laterales. Llaves se guardan bajo custodia del personal de seguridad quienes registran eventos al respecto en bitácora.	La solicitud de cerraduras la realiza el tecnólogo a cargo.

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
4	Mal manejo de las políticas de Backup.	Riesgos que necesitan Mitigación: Planes de actuación correctivos, Gestión Urgente	Dominio: 12. SEGURIDAD EN LA OPERATIVA. Objetivo de Control: 12.3 Copias de seguridad. Control: 12.3.1 Copias de seguridad de la información.	Realización de copias de seguridad de los servidores de archivos del centro, copiando la información en el servidor de respaldo, de acuerdo a la técnica implementada y sugerida por la central.	El proceso de copias de seguridad lo ejecuta el tecnólogo a cargo del mantenimiento de los equipos.
5	Falta de seguridad física e infraestructura.		Dominio: 12. SEGURIDAD EN LA OPERATIVA. Objetivo de Control: 12.2 Protección contra código malicioso. Control: 12.1 Controles contra el código malicioso.	Revisión y despliegue programada para Instalación, actualización de base de datos de virus, y de programa desde el servidor de antivirus de la, con última versión desplegada del antivirus.	La revisión y despliegue se hará paulatinamente.
6	Mal funcionamiento de las UPS.		Dominio: 11.SEGURIDAD FÍSICA Y AMBIENTAL. Objetivo de Control: 11.2 Seguridad de los equipos. Control: 11.2.4 Mantenimiento de los equipos.	Mantenimiento preventivo y correctivo de la UPS, Cada 3 meses. Limpieza interna y externa, con herramientas adecuadas. Abertura y limpieza de ranuras de ventilación desmonte y limpieza se sistema de ventilación.	La reparación la realiza el tecnólogo a cargo del mantenimiento de los equipos en la institución.

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
7	Malas conexiones en los toma corrientes.	Riesgos que necesitan Monitorización: Planes de actuación Detectivos, Riesgo Aceptable	Dominio: 11.SEGURIDAD FÍSICA Y AMBIENTAL. Objetivo de Control: 11.2 Seguridad de los equipos. Control: 11.2.4 Mantenimiento de los equipos.	Mantenimiento preventivo y correctivo de los toma corrientes, Cada 3 meses. Limpieza interna y externa, con herramientas adecuadas. Abertura y limpieza de ranuras de ventilación desmonte y limpieza se sistema de ventilación.	La reparación la realiza el tecnólogo a cargo del mantenimiento de los equipos en la institución.
8	Red de datos abierta.		Dominio: 9. CONTROL DE ACCESOS. Objetivo de Control: 9.4 control de acceso a sistemas y aplicaciones Control: 9.4.1 restricción del acceso a la información	Se realiza y se ejecuta el plan para verificar en los equipos involucrados, el puerto NetBios habilitado y se procede a deshabilitar. Se realiza copias de seguridad y activa las cuentas en cada equipo de usuarios, docentes y administrativos para asignarles privilegios	El proceso de revisión de NetBios lo ejecuta el tecnólogo a cargo.

8. PROPONENTES

8.1. PROPONENTES PRIMARIOS.

Jorge Enrique Araque Isidro, Ingeniero en Mecatrónica, Candidato a Especialista en Seguridad Informática, Candidato a Magister en Controles Industriales, Docente de la Universidad de Pamplona, 5 años como docente universitario.

8.2. PROPONENTES SECUNDARIOS.

Jorge Enrique Ramírez, Ingeniero de Sistemas, Especialista en Seguridad Informática, Magister en Gestión de Tecnología de Información, Docente de la UNAD seccional Pamplona.

Juan Miguel Gelvez Araque, Contador público, Gerente de COMFAORIENTE.

9. RECURSOS DISPONIBLES

9.1. RECURSOS

9.1.1. Recursos Materiales. Son los siguientes. Computador portátil hp Pavilion dv5, Memoria RAM de 4GB, procesador Intel Core i5 de 2.27 GHz, Disco Duro de 1TB.

SO Windows 7 Ultimate 32 bits.

Conexión a Internet de 2Mbps.
Resmas de papel.

Material Bibliográfico de la Biblioteca virtual de la Universidad Nacional Abierta y a Distancia.

9.1.2. Recursos Institucionales. Se tuvieron en cuenta los siguientes:

Oficinas de COMFAORIENTE seccional Pamplona.
Equipos de cómputo de las oficinas de COMFAORIENTE seccional Pamplona.
Instalaciones eléctricas de las oficinas de COMFAORIENTE seccional Pamplona.

9.1.3. Presupuesto.

10. CRONOGRAMA PROPUESTO INICIAL

Tabla 6. Cronograma

Actividad	SEMANA															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Hacer un inventario de los equipos y recursos relacionados con el manejo del sistema de información.																
Describir la infraestructura tecnológica presente en la organización.																
Realizar hacking ético a los sistemas de información para establecer vulnerabilidades.																
Establecer un conjunto de controles que permitan contrarrestar las falencias encontradas en la infraestructura tecnológica de la organización.																

11. RESULTADOS ESPERADOS

Con el desarrollo del trabajo de grado terminado se espera que la empresa COMFAORIENTE seccional Pamplona tome en consideración el análisis y evaluación de riesgos a los activos informáticos, que tomando en cuenta el resultado del mismo aplique las acciones de control que se proponen para mitigar de esta forma los riesgos de los cuales algunos son altos y deben tener acciones correctivas que deben ser atendidas lo más pronto posible.

Se espera que se puedan cambiar algunos comportamientos a nivel institucional que permitan a los administrativos adoptar prácticas seguras para evitar aumentar los niveles de los diferentes riesgos que se pueden llegar a presentar en los activos informáticos.

12. CONCLUSIONES

Con el análisis hecho a la infraestructura tecnológica de las oficinas de COMFAORIENTE de la sede de Pamplona de vulnerabilidades y riesgos se pudo identificar ciertos fallos de seguridad en la red de la institución, ante lo encontrado en estos análisis se realizan una serie de recomendaciones y controles para disminuir estos fallos, por esto se concluye.

- Se realizó una revisión de activos de las oficinas para de esta forma hacer las pertinentes observaciones para tabular el inventario de equipos con sus respectivas características técnicas para de esta forma categorizar e identificar posibles riesgos o vulnerabilidades.

- Se realizó un análisis de la infraestructura tecnológica en donde se identificaron los activos y se pudo describir la forma en que funciona la red de las oficinas de COMFAORIENTE.

- Se utilizó algunos software para hacer el haking ético, cabe resaltar que este fue una simulación debido a que no se permitió por parte de la empresa realizarlo directamente en los equipos y la red pero aun así se detectaron las posibles vulnerabilidades y riesgos por las características de los equipos obtenidos en el inventario realizado.

- Al tener todos los datos recogidos en las acciones hechas de análisis de vulnerabilidades y riesgos de los activos de las oficinas de COMFAORIENTE se realizan las recomendaciones respectivas a través de la matriz de control para que se apliquen buenas prácticas de seguridad de la información.

RECOMENDACIONES

Crear y mantener una base sólida de seguridad con soluciones interconectadas que abarquen toda la empresa. Desde el punto final al centro de datos a la nube, estas soluciones reducen los riesgos y la complejidad para que la empresa pueda avanzar.

Los proyectos de informatización de la empresa junto a la infraestructura TI, también deben incluir un sistema que permita conservar y mantener los datos y los documentos que los contienen durante, al menos, su período de vigencia legal.
Utilizar la automatización para atenuar tareas de seguridad, disminuyendo los errores manuales.

Invertir tiempo y recursos suficientes en el mantenimiento de los sistemas para que se mantengan siempre actualizados.

Cada usuario del sistema debe acceder solamente a aquello que requiera. De la misma forma en que es importante limitar el acceso a determinados archivos, también es necesario que haya un bloqueo de aplicaciones, programas y sistemas que permitan la salida de información de la empresa. Así como nubes públicas, en las que son posibles cargar millones de archivos en diferentes formatos.

Es importante diferenciar en la red, los datos más relevantes y estratégicos de la empresa y sobre ellos hacer una barrera diferenciada de protección. Puede ser criptografía, contraseñas o inclusive firewalls para limitar el tránsito en esa parte de la red.

Es fundamental que el coordinador de la red tenga una visión general sobre lo que está pasando con todo el sistema. Asegurarse de que está realizando un barrido completo por toda el área y mantenga un monitoreo constante y sistemático.

Una política de seguridad reside en permitir que administradores de la red, personal de seguridad en TI y otros técnicos puedan entender las reglas y aplicarlas en la red, colaborando también con la divulgación de éstas entre los usuarios.

Los equipos de seguridad deben estar alineados con los otros equipos de la empresa ligados a las operaciones y procesos de sus tareas. Todos deben saber que existen reglas, y que esas reglas son para la seguridad de la empresa y que deben ser cumplidas. Al estar todos alineados no existen disculpas futuras y existe la posibilidad de mejoras a partir de feedbacks que pueden surgir de otras áreas que no se relacionen con la TI.

Es necesario precisar métricas y datos capaces de evaluar su trabajo en seguridad de la información a lo largo del tiempo. Con tan frecuentes cortes de presupuesto, poder demostrar la importancia de su trabajo es algo fundamental.

La empresa necesita encontrar una solución sistemática con la que puedan asegurar su información con un enfoque basado en la gestión, que al mismo tiempo cumpla con las exigencias jurídicas. El cumplimiento con las leyes relativas a seguridad es un paso importante, pero no garantiza la cobertura internacional de los proyectos y la apertura de la empresa.

BIBLIOGRAFIA

Álvarez Jerzon. Diseño de un sistema de gestión de seguridad de la información - SGSI basado en la norma iso27001 para el Colegio Procolombiano de la ciudad de Bogotá, que incluye: asesoría, planeación.
Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia. 2016.

Arévalo o, Escalante K, Guevara N, Jiménez, M Montoya A y Orellana J. (2009) Metodología de análisis de riesgo de la empresa la casa de las baterías S.A de C.V". Universidad Tecnológica del Salvador.

Bojaca Garavito Edgar. Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco De Gachetá. . Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. 2016.

Bueno Shirley. Diseñar un Sistema de Gestión de Seguridad de la Información mediante la Norma ISO 27001 en el Instituto Colombiano de Bienestar Familiar Centro Zonal Virgen y Turístico de la Regional Bolívar. Universidad Nacional Abierta y a Distancia UNAD Cartagena. Colombia. 2015.

Cordero J y García Y. (2016) Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. san Bartolomé de Capitanejo, Santander. Universidad Nacional Abierta y a Distancia. UNAD.

Cordero Liñán Ronal.Diagnóstico del estado actual de la seguridad de la información basado en la norma ISO 27001:2013, de la IPS Medicsalud de la ciudad de Valledupar – Cesar. Universidad Nacional Abierta y a Distancia "UNAD". Valledupar Colombia. 2017.

Francisco N, Solarte E, Rosero, M. (2015) Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de Pamplona - Norte De Santander.

García Vivian & Ortiz Jhon. Análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial. Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia. 2017.

García Ramírez German & Castro Jaime. Diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) a la Empresa Unitransa S.A. Ubicada en la Ciudad de Bucaramanga. Universidad Nacional Abierta y a Distancia UNAD. Bucaramanga. Colombia- 2017.

Henao Rodríguez Jaime.Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 para la empresa USOMET LTDA. en la ciudad de Ibagué. Universidad Nacional Abierta y a Distancia
UNAD. Bogotá D.C. Colombia. 2016

Hernández Sampier. (2003) Metodología de la investigación. Editorial Mac Graw Hill. España

Maureira Daniel Norma Iso/Iec 27001 Aplicada a una Carrera Universitaria. Universidad Andres Bello. Santiago de Chile. 2017.

Presidencia de la Republica. (2017)Guía para la calificación de la información de acuerdo con sus niveles de seguridad.

Perafan Jairo y Caicedo Mildred. (2014) Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Universidad Nacional Abierta y a Distancia. Popayán.

SGSI. Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC..2015 Recuperado de_
http://openaccess.uoc.edu/webapps/o2/bitstream/10609/42965/7/mmanozTFC0615memoria.pdf

Solarte Francisco, Enríquez Edgar & Benavidez Miriam. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la

norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, (Diciembre 2015)

Sossa Johanna (2012) Análisis de Riesgos Estándares para la administración de riesgos. Universidad Javeriana Recuperado de. http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

Suarez Padilla Yomay. análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & CÍA. LTDA, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Universidad Nacional Abierta y a Distancia UNAD. Bogotá D.C. Colombia. 2015.

ANEXOS

SOLICITUD DE PERMISO PARA DESARROLLAR MI TRABAJO DE GRADO EN COMFAORIENTE SECCIONAL PAMPLONA.

UN
Universidad Nacional
Abierta y a Distancia

532-24-173
Pamplona, 25 de septiembre de 2015

Doctor
JUAN MIGUEL GELVEZ ARAQUE
COMFAORIENTE
Ciudad

ASUNTO: CARTA DE INTENCIÓN PARA DESARROLLAR PRÁCTICA PROFESIONAL DE ESPECIALIZACION.

Respetado Doctor,

Con el propósito de fortalecer el proceso de aprendizaje de los estudiantes de los últimos semestres del programa ESPECIALIZACION EN SEGURIDAD INFORMATICA, la Universidad Nacional Abierta y a Distancia, busca establecer su apoyo y colaboración en el àrea de Redes e Informática, en las cuales nuestros estudiantes tengan la oportunidad de validar y fortalecer los conocimientos adquiridos durante su formación académica mediante la ejecución del proyecto de grado en el área mencionada.

Dicha validación se convertiría en una gran oportunidad para las dos instituciones puesto que para nuestros estudiantes el tener un centro de práctica le permite afianzar su desempeño como futuros profesionales y para su entidad el beneficio se verá reflejado en la optimización de los servicios que gestiona el área de Redes y Sistemas de la Caja de Compensación COMFARIENTE, seccional Pamplona.

Es así como presentamos a nuestro estudiante JORGE ENRIQUE ARAQUE ISIDRO, identificado con la cédula de ciudadanía 1094249080.

La práctica se establecerá de acuerdo al cronograma establecido en el proyecto presentado por el estudiante

Agradecemos su valiosa colaboración,

Atentamente,

SANTIAGO BURBANO RODRIGUEZ
DIRECTOR UNAD
Centro Comunitario de Atención Virtual CCAV Pamplona

COMFAORIENTE
JEFE
SECCIONAL PAMPLONA

Universidad Nacional Abierta y a Distancia UNAD
CEAD Pamplona Av. Santander 11 42 la Salle
Teléfono: 5686688 – 3112815599
Pamplona@unad.edu.co