Universidad de las Ciencias Informáticas

Facultad 9

Trabajo de Diploma para optar por el título de

Ingeniero en Ciencias Informáticas

Titulo: *"Documentación para la gestión de la seguridad informática del Centro de Datos de la Oficina Nacional de Recursos Minerales."*

AUTORES

Yuniesky Vázquez Figueredo

Yodelvis Rodríguez Arteaga

TUTOR

Ing. *Jorge L. Diéguez Escalona.*

ASESOR

Ing. *Cesar Rosales*

Ciudad de la Habana, julio 2 del 2008
"Año 50 de la Revolución"

"Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

Bruce Schneier.

DEDICATORIA

De Yodelvis:

A Ángela Arteaga, por haber cumplido el difícil papel de ser madre y padre a la vez, por ser además mi amiga y confidente, por dar la energía, entrega, amor y hasta parte se du vida para hacer de sus hijos hombres de bien.

A Rogelio, mi abuelo, abuelo por genética, padre incondicional por naturaleza y de corazón, por sus cuentos, sus consejos y apoyo, hoy no está entre nosotros y no va a poder ver físicamente mi resultado pero en mi corazón siempre habitará su presencia.

A Caridad mi abuelita, mi segunda madre, por escucharme siempre, por curar todos mis problemas, porque se que me quiere más que a ella misma.

A mis hermanos, que me esperan siempre con los brazos abiertos, Yudervis mi jimagua "el médico", con quien he compartido toda mi vida, Randy, quien hoy es un niño estudioso con muchas ganas de seguir nuestro ejemplo, Duniesky que desde pequeño siempre quiso estar junto a nosotros.

A mi familia y a todos los pobladores de La Lima que tanto confían en mí y esperan cada día que regrese siendo ingeniero.

De Yuniesky:

A Victoria Rosa, mi querida flor y madre por su amor incondicional, sus incontables desvelos, su apoyo en todo momento y por dedicarme además tantos sacrificios para que saliera adelante.

A mi querido padre Melanio, que no se queda atrás con sus innumerables consejos, la ayuda brindada en todos estos años y por su optimismo y fe depositada en mí.

A mis hermanos Yuviesky y Euliser por trasmitirme tanta energía positiva, el valor, la persistencia y la esperanza de salir adelante ante cualquier dificultad o barrera que nos ponga la vida.

A mi abuelita aunque ya no esté, por el amor que me dio y las tantas historias que me contó y por el cuidado paternal que me deba desde chiquito.

AGRADECIMIENTOS GENERALES

Quisiéramos agradecerle a nuestro Comandante en Jefe y a esta Revolución por brindarnos la oportunidad de que cumpliéramos nuestros sueños. A todos aquellos que nos brindaron su ayuda incondicional, a nuestras familias y amigos; así como a nuestro tutor y asesor por la guía, apoyo y ayuda que nos ofrecieron en el desarrollo de este trabajo.

Muchas gracias.

AGRADECIMIENTOS PERSONALES

De Yodelvis:

Quisiera agradecer a los maestros y profesores que participaron en mi formación como profesional. Agradecer también a aquellas personas que un día me dieron un consejo y hoy se sienten orgullosos de decir "aporté en la formación y educación de ese muchacho y hoy es como siempre esperé", gracias a todos por la confianza y apoyo.

De Yuniesky:

Quisiera agradecerles a mis padres y hermanos por todo el apoyo, sacrificio, amor y valor que me han brindado para poder salir adelante. Mi agradecimiento especial para Regla María por tanta paciencia, comprensión, cariño, ternura y amor en los últimos cuatro años y que tanta ayuda me brindó en incontables momentos. También les agradezco a mis amigos que ayudaron de forma incondicional a lograr mi meta con tantos consejos, sugerencias y que de una forma u otra hicieron posible que este trabajo se realizara.

DECLARACIÓN DE AUTORÍA.

Declaramos que somos los únicos autores de este trabajo y autorizamos a la Universidad de Ciencias Informáticas (UCI) a hacer uso del mismo en su beneficio.

Para que así conste firmamos la presente a los ____ días del mes de junio del año 2007.

_____	_____	_____
Firma del Autor	Firma del Autor	Firma del Tutor

OPINIÓN DEL USUARIO DEL TRABAJO DE DIPLOMA

El Trabajo de Diploma titulado “Documentación para la gestión de la seguridad informática del Centro de Datos de la Oficina Nacional de Recursos Minerales” fue realizado en la Universidad de las Ciencias Informáticas (UCI). Este centro considera que, en correspondencia con los objetivos trazados, el trabajo realizado le satisface:

- Totalmente
- Parcialmente en un ____ %

Los resultados de este Trabajo de Diploma le reportan a esta universidad los beneficios siguientes (cuantificar):

_____
_____
_____
_____
_____
_____
_____

Y para que así conste, se firma la presente a los ____ días del mes de junio del año 2007.

_____ _____
Representante de la entidad Cargo

_____ _____
Firma Cuño

OPINIÓN DEL TUTOR DEL TRABAJO DE DIPLOMA

Título: “Documentación para la gestión de la seguridad informática del Centro de Datos de la Oficina Nacional de Recursos Minerales”.

Autores: Yuniesky Vázquez Figueredo
Yodelvis Rodríguez Arteaga.

Como tutor del Trabajo de Diploma “Documentación para la gestión de la seguridad informática del Centro de Datos de la Oficina Nacional de Recursos Minerales”, luego de haber culminado la realización del mismo, considero que los autores Yuniesky Vázquez Figueredo y Yodelvis Rodríguez Arteaga han desarrollado un conjunto de habilidades que les permitirán darle solución adecuadamente a cualquier tipo de necesidad de informatización que se presente en su vida profesional.

Durante la realización del presente trabajo los estudiantes han demostrado un alto grado de preocupación y responsabilidad ante el cumplimiento en tiempo de las tareas que se les programaron. Han trabajado coordinadamente dando muestras de poseer responsabilidad y compromiso en la realización de su tesis. Su desempeño ha manifestado que han desarrollado un valioso nivel de asimilación e investigación, llegando a alcanzar un profundo conocimiento y una gran capacidad para la toma de decisiones correctas.

Los estudiantes manifestaron laboriosidad y preocupación a lo largo del cumplimiento de las tareas programadas, logrando que los resultados obtenidos estuviesen acorde con los objetivos trazados.

Por otra parte, el elemento investigativo del documento, estuvo desde el inicio muy bien orientado y estructurado, basado en una gran cantidad de bibliografía actualizada. Cada contenido se ha expuesto con claridad y aporta grandes conocimientos al lector. Vale destacar que el proceso realizado es una tarea completamente nueva en nuestra universidad e incluso en nuestro país por lo que han realizado un trabajo admirable que normalmente es objeto de mucho trabajo y poca planificación, logrando obtener resultados satisfactorios que serán de gran aporte a futuros procesos que puedan ser similares.

Por todo lo anteriormente expresado considero que el estudiante está apto para ejercer como Ingeniero Informático; y propongo que se le otorgue al Trabajo de Diploma la calificación de ____.

Ing. Jorge Luis Diéguez Escalona.

_____ _____

Firma Fecha

RESUMEN

Las relaciones entre la ONRM y la UCI dieron como fruto al Programa Nacional de Informatización del Conocimiento Geológico y que como bien dice su nombre se encargará de informatizar diferentes procesos de la geología. La digitalización de tantos mapas, la cantidad de aplicaciones e información a procesar generarán bases de datos que ocuparán una gran capacidad y que una vez se concluya el Programa se establecerán en un Centro de Datos que construirá la ONRM. Por su alta importancia es necesario preservar la integridad, confiabilidad y disponibilidad de la información por lo que esta investigación está centrada en el desarrollo de la documentación para la gestión de la seguridad informática del Centro de Datos de la ONRM.

El objetivo de este trabajo es la elaboración de un plan de seguridad informática para el futuro Centro de Datos de la Oficina Nacional de Recursos Minerales. Plan que contendrá el análisis de riesgos, las políticas de seguridad, medidas, procedimientos y un plan de contingencias en caso de que ocurra algún incidente. Incluso se realiza una propuesta de como deberá estar conformado el futuro sistema del centro.

PALABRAS CLAVES: Centro de Datos, Plan de Seguridad Informática.

INDICE

INTRODUCCIÓN 1

CAPÍTULO 1 "FUNDAMENTACIÓN TEÓRICA" 5

1.1 INTRODUCCIÓN 5
1.2 PRINCIPALES CONCEPTOS ASOCIADOS AL DOMINIO DEL PROBLEMA 5

1.2.1 Centro de Datos 6
1.2.2 Seguridad informática 6
1.2.2.1 Confidencialidad 6
1.2.2.2 Integridad 7
1.2.2.3 Disponibilidad 7
1.2.3 Plan de Seguridad Informática 7
1.2.4 Seguridad Física 7
1.2.5 Seguridad Lógica 8
1.2.6 Análisis de riesgos 8
1.2.7 Gestión de riesgos 8
1.2.8 Activos informáticos 8
1.2.9 Políticas de Seguridad 8
1.2.10 Amenazas 9
1.2.11 Riesgos 9

1.3 OBJETO DE ESTUDIO 9

1.3.1 Descripción General 9
1.3.2 Descripción actual del dominio del problema 12
1.3.3 Situación Problemática 13

1.4 ANÁLISIS DE OTRAS SOLUCIONES EXISTENTES 14

1.4.1 Principales aportes a nuestro problema 15

1.5 CONCLUSIONES PARCIALES 15

CAPÍTULO 2 SOLUCIÓN PROPUESTA 17

2.1 INTRODUCCIÓN 17
2.2 CARACTERIZACIÓN DEL SISTEMA 17

2.2.1 Flujo de la información: 20
2.2.2 Componentes del Sistema Informático 20
2.2.2.1 Router 21
2.2.2.2 Firewall 21
2.2.2.3 Switch 22
2.2.2.4 Servidor Proxy 22
2.2.2.5 Servidor DNS 23
2.2.2.6 Servidor Web 23
2.2.2.7 Servidor de Correo 23
2.2.2.8 Servidor FTP 24
2.2.2.9 Servidor de Aplicaciones 24
2.2.2.10 Servidor de Bases de Datos 25

2.3 ANÁLISIS DE RIESGOS 25

2.3.1 Identificación de los activos informáticos 25
2.3.2 Evaluación de los activos informáticos 27
2.3.3 Listado de las amenazas 28
2.3.4 Identificación de las amenazas por activos 29
2.3.5 Valoración de Riesgos 36
2.3.6 Resultado del Análisis 38

2.4 POLÍTICAS DE SEGURIDAD 39

2.4.1 Generales 39
2.4.2 Instalación de equipos de cómputo 41
2.4.3 Mantenimiento de equipo de cómputo 41
2.4.4 Reubicación del equipo de cómputo 41
2.4.5 Control de accesos 41
2.4.6 Control de acceso local a la red 42
2.4.7 Control de acceso remoto 42
2.4.8 Acceso a los sistemas administrativos 43
2.4.9 Sanciones 43

2.5 MEDIDAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA 44

2.5.1 Seguridad física 44

2.5.1.1 Protección de áreas con tecnologías instaladas 44
2.5.1.1.1 Ubicación 44
2.5.1.1.2 Barreras Físicas 45
2.5.1.1.3 Sistema de Control de Acceso 46
2.5.1.1.4 Medios Técnicos de Detección de Intrusos 47
2.5.1.2 Protección Física de los Equipos 49
2.5.1.2.1 Ubicación 49
2.5.1.2.2 Dispositivos de Protección Física a Aplicar 49
2.5.1.2.3 Control de Acceso a las tecnologías informáticas 50
2.5.1.3 Soportes de información 52
2.5.1.3.1 Identificación 52
2.5.1.3.2 Conservación 52
2.5.1.3.3 Destrucción 54
2.5.1.3.4 Traslado 54

2.5.2 Seguridad Lógica 55

2.5.2.1 Identificación y autenticación de Usuarios 55
2.5.2.1.1 Identificación y Autentificación de Usuarios 55
2.5.2.1.1A Usuarios internos 56
2.5.2.1.1B Usuarios externos 57
2.5.2.2 Control de Acceso a los Activos y Recursos 59
2.5.2.2.1 Usuarios externos 59
2.5.2.2.2 Usuarios internos 60
2.5.2.2.2A Flujo de información entre activos informáticos 62
2.5.2.3 Integridad de los Ficheros y Datos 64
2.5.2.3.1 Firewall por hardware 65
2.5.2.3.2 Protección Contra Programas Dañinos 66
2.5.2.3.3 Ataques de red 68
2.5.2.3.4 Seguridad de Bases de Datos 69

2.5.3 Auditoría **71**

2.5.4 De Seguridad de Operaciones **73**

2.5.4.1 Salvaguardas 73
2.5.4.2 Instalaciones de Software 74
2.5.4.3 Mantenimiento y reparación de las Tecnologías de Información 76

2.5.5 De Recuperación Ante Contingencias **77**

2.5.5.1 Falla eléctrica por largo tiempo: 79
2.5.5.2 Falla en servidores del área desmilitarizada (DMZ): 81
2.5.5.2.1 Falla en el servidor Web: 82
2.5.5.2.2 Falla en el servidor de Aplicaciones: 82
2.5.5.2.3 Falla en el servidor de Directorios: 82
2.5.5.2.4 Falla en el servidor DNS: 82
2.5.5.3 Incendio: 83
2.5.5.4 Huracanes: 84

2.6 ANÁLISIS DE LOS BENEFICIOS QUE SE OBTIENEN CON EL RESULTADO DE LA SOLUCIÓN **86**

2.7 CONCLUSIONES PARCIALES **87**

CONCLUSIONES **89**

RECOMENDACIONES **90**

REFERANCIAS BIBLIOGRÁFICAS **91**

BIBLIOGRAFÍA CONSULTADA **93**

ANEXOS **94**

GLOSARIO **98**

INTRODUCCIÓN

El constante avance de las tecnologías de la información y comunicaciones ha llevado a cabo una revolución en el mundo entero. Su uso en las diferentes ramas existentes ha propiciado un elevado desarrollo en la economía, la política, la cultura y en sí en la sociedad. Nuestro país lucha por alcanzar la automatización e informatización en los sectores más importantes de nuestra sociedad en la que se destaca el Ministerio de la Industria Básica (MINBAS).

El Ministerio de la Industria Básica integra sectores estratégicos de la economía cubana, sus principales producciones y servicios se orientan tanto al mercado nacional como internacional. Tiene como misión garantizar el desarrollo de las ramas que la integran para hacer sostenible el resto de las ramas del país y lograr el bienestar del pueblo. Está constituido además por cuatro entidades independientes en la que se encuentra la Oficina Nacional de Recursos Minerales (ONRM) que es la rectora nacional para garantizar la racional explotación y utilización de los recursos minerales e implementar el marco jurídico para el desarrollo y control de la geología, la minería y el petróleo.

La dirección política del país ha definido al sector de las informáticas y las comunicaciones como un sector estratégico, siendo la Universidad de las Ciencias Informáticas (UCI) la principal impulsora de los programas de informatización.

A pesar de que la UCI es una institución totalmente nueva en el negocio de la producción de software, ya tiene un prestigio a nivel nacional e incluso internacional, con proyectos en realización en algunos países de América Central, pero fundamentalmente proyectos nacionales y con el hermano pueblo venezolano. Este prestigio le ha dado la oportunidad de poseer la patente de utilización de un grupo de software reconocido internacionalmente, además de buenas relaciones con representantes del mundo de la producción informática, principalmente los defensores de la producción de software de código abierto.

La ONRM y la UCI establecieron las relaciones al tomarse acuerdos sobre la realización de un sistema capaz de resolver las deficiencias existentes en el campo de la geología. Estas deficiencias están dada porque en la ONRM se maneja un elevado número de información y datos que hacen referencia al desarrollo geológico del país de sus últimos cuatro siglos, en su mayoría archivados en

papel o en un sistema gestor de información ineficiente, lo que provoca pérdida de información y atrasos en la localización y procesamiento de la misma, requerida por la ONRM y el resto de las entidades nacionales subordinadas a ella, así como las empresas tanto nacionales como internacionales interesadas en establecer relaciones de negocio en el país en la esfera geológica, ya que no poseen fácil acceso a la información referente a los temas de negocios geológicos en nuestro país, ni las vías para poder establecer los mismos, o se les hacen demasiado costosos los trámites.

El Programa Nacional de Informatización del Conocimiento Geológico (PNICG) llevado a cabo en la UCI, fruto de su relación con la ONRM fue dividido en módulos que se centran y resuelven determinados problemas en el campo de la geología, informatizando lo necesario; donde algunos de estos módulos generarán bases de datos con diferentes grados de capacidad y que llegarán a ocupar aproximadamente un total de hasta 46 Terabyte (TB) de información de datos geológicos. Para ello se construirá un centro de datos que contendrá a los servidores de dicha información.

La **situación Problemática** es la siguiente: El desconocimiento e inexperiencia a cerca de la gestión de la seguridad informática para el Centro de Datos que se construirá en la ONRM a medidas que los módulos del PNICG estén terminando y el volumen de información crítica aumente.

Por todo lo anteriormente expuesto el **Problema Científico** de esta investigación es:

¿Cómo gestionar la seguridad informática de un Centro de Datos?

Para lograr este propósito se identificó como **Objeto de Estudio** la seguridad informática en un Centro de Datos.

Por lo que el **Campo de acción** está centrado en la documentación para la gestión de la seguridad informática del Centro de Datos en la ONRM.

Como **Objetivo general** se ha planteado Elaborar un plan de seguridad informática de un Centro de Datos para la Oficina Nacional de Recursos Minerales.

A partir del análisis del objetivo general se derivaron los siguientes **objetivos específicos**:

- Realizar un estudio profundo sobre la gestión de la seguridad informática.
- Realizar un análisis de riesgos.
- Realizar la gestión de riesgos.
- Establecer las políticas de seguridad.
- Documentar las medidas y los procedimientos de la seguridad informática.

Para llevar acabo el desarrollo de la investigación, se plantea la siguiente **hipótesis*:*** Si se realiza un plan de seguridad informática para un centro de datos entonces se garantizará la integridad, confiabilidad, disponibilidad de la información y el funcionamiento eficiente del mismo en la Oficina Nacional de Recursos Minerales.

Para alcanzar los **objetivos específicos** propuestos, se llevarán a cabo las siguientes **tareas**:

- Entrevistar a personas especializadas en seguridad informática.
- Realizar propuesta de los activos informáticos que conformarán el centro de datos.
- Evaluar los activos informáticos.
- Identificar las amenazas potenciales que afecten los activos.
- Realizar una valoración de los riesgos que las amenazas implican.
- Elaborar las políticas de seguridad.
- Documentar las medidas y los procedimientos de la seguridad informática.

Para la realización de **las tareas** se emplearán los siguientes métodos:

Métodos Teóricos:

- Históricos lógicos, porque permite analizar la trayectoria del proceso brindándonos información relevante sobre el mismo.

- Análisis y síntesis, que permitirá dividir la situación en subtemas más simples para facilitar el estudio de las bibliografías y luego la reintegración de la información ya sintetizada enfocada a la

solución de la situación problemática.

- Modelación: Se representarán a través de diagramas los distintos procesos o actividades que se desarrollarán en la investigación para mejor comprensión del sistema.

Métodos empíricos:

- Entrevistas, porque mediante éstas se logrará obtener la información necesaria de lo que realmente quiere el cliente, además de la información que permitirá realizar este trabajo.

- Análisis de Documentos, mediante la cual se recogen, clasifican y se organiza la información concerniente que sirve de apoyo para el entendimiento y realización del documento científico.

A continuación se presenta un breve resumen de los capítulos en que fue distribuido el desarrollo de la investigación:

Capítulo 1: "Fundamentación Teórica". Se exponen un conjunto de conceptos asociados al dominio del problema planteado que ayudarán a familiarizarse con el entorno en el que se manifiesta la investigación, y con los que se espera que se comprenda la solución propuesta y la necesidad de la misma. Además se describen en detalles elementos relacionados al objeto de estudio que dio origen a este trabajo.

Capítulo 2: "Solución Propuesta". Se realiza la descripción de la solución propuesta del trabajo. Se caracteriza el futuro sistema y se proponen los componentes que lo integrarán. Se efectúa un análisis de los riesgos del sistema y se plantean las políticas de seguridad a establecer en el Centro de Datos; así como las medidas (físicas y lógicas), procedimientos y un plan de contingencias. Además se analizan los beneficios de la investigación.

CAPÍTULO 1 "FUNDAMENTACIÓN TEÓRICA"

1.1 Introducción

En este capítulo se abordará una serie de temas relacionados con el marco teórico y conceptual en que se desenvuelve la investigación para ayudar a comprender mejor el trabajo en general. En el mismo se hará una descripción del objeto de estudio planteado anteriormente en la introducción del trabajo, tratando temas relacionados con la entidad en la que se aplicará la seguridad informática, el por qué de su importancia y cuáles son los artefactos que la sustentan.

En el dominio del problema se describe la situación actual en la cual está enmarcada la investigación haciendo referencia a tres problemas fundamentales; el gran volumen de información a almacenar, hecho que tiene alta importancia por la sensibilidad de los datos geológicos, dando paso a la necesidad que existe de aplicar la seguridad informática para la protección de dicha información; otro de los problemas son los inconvenientes por la inexistencia de centros de datos en nuestro país y más aún por la falta de un plan de seguridad que responda a las particularidades de la organización.

La situación problemática argumentará brevemente cómo es que se irá realizando la integración de nuevos hardware y software cuando se construya el centro de datos de la Oficina Nacional de Recursos Minerales y según se vayan concluyendo los módulos del Programa Nacional de Informatización del Conocimiento Geológico, además de la necesaria seguridad de los mismos en todo momento. Lo más importante de este punto es la argumentación de la inexperiencia y el desconocimiento de la gestión del plan de seguridad para el centro de datos de esta organización.

En el último punto y no menos importante se hará un análisis de dos planes de seguridad: uno elaborado en nuestro país y otro en Argentina para una empresa de ventas de autos. Además, se argumentará sobre los aportes que estos planes de seguridad puedan ofrecer para la realización de este trabajo.

1.2 Principales conceptos asociados al dominio del problema

En la situación Problemática o marco del problema en sentido general, existen una serie de conceptos que, por su importancia y para mayor entendimiento de lo planteado, se explicará en que consiste

cada uno.

1.2.1 Centro de Datos

Con la revolución y el impacto provocado por el desarrollo de la Tecnología Informática (TI) en todas las esferas existentes de la sociedad, se ha informatizado gran parte de aquellas empresas y entidades que hoy cuentan tal desarrollo, aumentando así la cantidad de usuarios conectados a la gran red de redes: la Internet, lo que dificulta en muchas ocasiones los servicios brindados, e incluso la seguridad de la información crítica soportadas en las bases de datos. Se logra mayor eficiencia con el surgimiento de los Centro de Datos (Data Center) que son también conocidos por Centro de Procesos de Datos (CPD) por los beneficios y las ventajas que ofrecen.

Se denomina Centro de Datos a "aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de información de una organización"[1]. En el mismo se encuentra el personal especializado trabajando en los equipos electrónicos encargados del almacenamiento y seguridad de la información.

1.2.2 Seguridad informática

La seguridad informática es el conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la Información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información[2]. En la práctica está representada por un conjunto de procesos, tareas y actividades, implementados conjuntamente con elementos de computación y telecomunicaciones para controlar y proteger contra amenazas que pongan en riesgo los recursos informáticos[3].

1.2.2.1 Confidencialidad

Varias son las vías y los recursos que utiliza un atacante para hacer daño a una persona u organización, dentro de las que se encuentra la violación de la privacidad cuando se intercepta, se copia e incluso puede divulgar la información trasmitida por un medio y sin autorización del emisor o el remitente. Por lo que se denomina confidencialidad cuando los activos informáticos o la información son conocidos y accedida solo por las personas que están autorizadas[4].

1.2.2.2 Integridad

Otra vía por la cual el atacante puede cometer daños irreparables puede ser durante el envío de datos, pudiendo interceptar, alterar, borrar, etc., la información trasmitida.

Se denomina **integridad** a la seguridad de que la información trasmitida o los activos informáticos solo pueden ser modificados por las personas autorizadas y de la forma autorizada[4].

1.2.2.3 Disponibilidad

Aunque en cierto momento un atacante pueda bloquear, borrar o modificar la información, no solo ellos se convierten en los responsables de que las personas puedan acceder o no cuando quieran a los datos a los cuales están autorizados, sino que se debe también, por parte de la entidad que protege la información, evitar su pérdida y ser capaz de recuperarla en caso de un ataque o mala operación cuando se requiera.

Por lo que la disponibilidad es el aseguramiento de que los activos informáticos o la información sean accedidos por las personas autorizadas en el momento que lo requieran y deseen[4].

1.2.3 Plan de Seguridad Informática

El Plan de Seguridad Informática constituye una exigencia de la Resolución No. 6 de 1996 del Ministerio del Interior (MININT) que pone en vigor el Reglamento sobre la Seguridad Informática[5]. Es un documento básico que establece los principios organizativos y funcionales de la actividad de seguridad informática en un Órgano, Organismo o Entidad, a partir de las políticas y un conjunto de medidas aprobadas sobre la base de los resultados obtenidos en **el análisis de riesgos** previamente realizado que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo[2].

1.2.4 Seguridad Física

El concepto de Seguridad Física no es más que " la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"[6]. Representa toda acción a tomar para propiciar la protección de los medios informáticos que se encuentran en la organización; incluyendo los distintos tipos de controles y los diferentes dispositivos o mecanismos de seguridad, tanto internos como externos, para enfrentar problemas como: Desastres naturales en los que se incluyen las inundaciones, los incendios, terremotos, entre otros; además de robos, sabotajes, fraude, intrusión, etc.

1.2.5 Seguridad Lógica

La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo[7]. Se refiere a las técnicas y medidas que deben ser tomadas para asegurar que la información existente solo sea accedida, modificada o utilizada por las personas con autorización y que ante cualquier situación los responsables de la seguridad sepan que es lo que se debe hacer.

1.2.6 Análisis de riesgos

Para saber la atención que se le debe prestar a aquellos activos y recursos críticos en virtud de la función que realizan o los servicios que proporcionan, su valor y el riesgo a que están sometidos es necesario realizar un análisis de riesgos. El mismo no es más que el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización y los activos que en ella se encuentran[8].

1.2.7 Gestión de riesgos

Cuando se realiza un análisis de riesgos se debe seleccionar e implantar las salvaguardas, para conocer, prevenir, impedir, reducir o controlar los riesgos identificados en un análisis de riesgos y es a lo que llamamos gestión de riesgos[8].

1.2.8 Activos informáticos

Los activos informáticos son los recursos de un sistema de información o los que se relacionan con éste, necesarios para que la organización o entidad funcione correctamente y alcance los objetivos propuestos. Además de ser el objetivo principal a proteger de la seguridad informática[9].

1.2.9 Políticas de Seguridad

Existen varias definiciones de políticas de seguridad dentro de las que se encuentran que son “un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema”[6].

También se encuentra otra definición de la RFC (Request For Comments) 1244 que define como Política de Seguridad “una declaración de intenciones de alto nivel que cubre la seguridad de los

sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán"[10].

1.2.10 Amenazas

Las amenazas son la probabilidad de que un fenómeno de origen natural, humano o tecnológico se produzca en un determinado tiempo y espacio, constituyendo un peligro potencial al interferir en el funcionamiento adecuado de un ordenador personal o activo informático[11, 12].

1.2.11 Riesgos

Los riesgos son la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, indicando los daños o perjuicios que causaría a la Organización si no se protegieran adecuadamente[8].

1.3 Objeto de estudio

1.3.1 Descripción General

Anteriormente se planteó que el objeto de estudio para el desarrollo y elaboración del trabajo, sería el siguiente: La seguridad informática en un Centro de Datos. Este Centro de Datos será construido por la Oficina Nacional de Recursos Minerales, reafirmando que esta organización es una de las entidades independientes que integra al Ministerio de Industria Básica y que controla la racional explotación y utilización de los recursos minerales e implementa el marco jurídico para el desarrollo y control de la geología, la minería y el petróleo, lo que por ende tiene un volumen de información elevada que al digitalizarla, estos datos ocuparán una gran capacidad que puede llegar a alcanzar aproximadamente los 46 TB (Terabyte).

Para explicar lo que es la seguridad informática primeramente se impone conocer que es un centro de datos, el por qué de utilizar este sistema y no actuar como tradicionalmente se hace, donde cada empresa tenga en uno de sus departamentos instalado un conjunto de servidores que respondan a sus demandas particulares.

Ha sido y es preocupación de los disímiles usuarios de la tecnología, la seguridad tanto física como lógica de la información con que se trabaja y de la que se depende. En un inicio la tendencia fue concentrar los datos en las grandes y rudimentarias máquinas antiguas, que en aquellos momentos era lo más sofisticado que existía. En la generación de esos pesados ordenadores a válvulas se concentraba la información, no porque fuera lo ideal, sino porque no existía otra opción. Con la llegada de los pequeños y modernos ordenadores cambió la tendencia de almacenar los recursos de centralizados a descentralizados. Cada forma diferente de mantener controlada la información ha traído ventajas y desventajas que hacen que el usuario opte por una de ellas según sus posibilidades económicas o simplemente sus gustos. Las principales características que se miden a la hora de seleccionar la forma ideal en que serán almacenados los datos (centralizados o descentralizados) son:

- Disponibilidad.
- Confiabilidad.
- Integridad.
- Facilidad para hacer cambios.
- Accesibilidad.
- Costo.

Éstas características no significan que si se aplica una u otra técnica se corra el riesgo de que una de las condiciones no se cumplan, lo importante es que en cualquiera de los dos casos todas ellas estén presentes. La correcta elección no siempre es cuestión de gustos o posibilidades económicas. Es necesario aclarar cuando se está en presencia de información centralizada y cuando sería información descentralizada.

Información descentralizada:

Se está en presencia de la técnica de información descentralizada como forma de almacenar datos cuando se tiene la información o parte de ella distribuida en diferentes lugares físicos. Como ejemplo donde se refleja esta situación se puede tomar a una empresa ficticia que tiene diferentes sucursales en regiones geográficas distantes y cada una de estas entidades guarda información relevante que complementan al centro matriz.

Información centralizada:

Se está en presencia de la técnica de información centralizada como forma de almacenar los datos

cuando se tiene toda la información perteneciente a una entidad almacenada en un mismo local destinado para ello. Siguiendo con el mismo ejemplo anterior se tendría la empresa con sus sucursales distantes pero en este caso toda la información estaría concentrada en el centro matriz; si una sucursal necesita introducir información o consultarla, tendría que conectarse al centro matriz.

Ya vista la diferencia entre ambos conceptos solo queda analizar cuanto costaría económicamente elegir uno u otro sistema. Hasta aquí se ha hecho un poco de historia sobre los métodos de almacenamiento de grandes volúmenes de información, pero: ¿Cómo se comporta esto en la actualidad? ¿Cuál es la nueva tendencia?

La tendencia sobre el cómo almacenar los grandes volúmenes de información vuelve a ser centralizada y no precisamente por los mismos motivos. Esta vez se retorna a la concentración de los datos pero con la diferencia de que el lugar es un local especialmente destinado para tal fin llamado Centro de Datos, ubicado distante de la entidad que almacena la información.

¿Qué ventajas tendría guardar la información en un Centro de Datos?
El conjunto de razones que invitan a una empresa a optar por guardar su información en uno de estos sistemas es que son lugares donde se almacena gran cantidad de información de una empresa (pueden ser varias). Trabajan las 24 horas y los 365 días al año garantizando la máxima seguridad de los datos, esa es su función. Una vez que una empresa guarda su patrimonio en un centro de datos no tiene que preocuparse por la seguridad de ellos, de aquí la alta responsabilidad que asumen estos centros y la importancia de mantener la seguridad. Elegir uno de estos lugares para guardar los datos no siempre es una elección, en ocasiones, y a medidas que pasa el tiempo y crecen las bases de datos, resulta difícil del punto de vista económico mantener los servicios corriendo eficientemente en la entidad a la que pertenecen, siendo más factible pagar por el alquiler de un lugar donde, además de guardarlos, garantizan seguridad, accesibilidad, disponibilidad, confiabilidad y todo un conjunto de características que benefician a los clientes.

Ya explicado lo que es un centro de datos esta investigación propondrá como será la infraestructura física y lógica para crear el de la ONRM y dictará el conjunto de políticas, normas y procedimientos que garantizarán la seguridad acorde a las exigencias y requisitos que demanda uno de estos sistemas y la entidad a la cual pertenece, porque la evolución continua en el campo de las Tecnologías Informáticas y Comunicaciones (TIC) ha provocado un gran impacto en la sociedad, tanto para bien

como para mal, pues se ha incrementado el número de personas que interactúan con estos medios y con ellos los delitos informáticos (tales como: robos, sabotajes, fraude, intrusión, suplantación, etc., los cuales afectan de una forma u otra a la información u organización a la cual pertenece) por lo que es la razón principal del surgimiento de lo que hoy llamamos: **seguridad informática**.

La misma está sustentada por un Plan de Seguridad Informática que contiene componentes como: análisis de riesgo, políticas de seguridad, las medidas y los procedimientos tanto físicos como lógicos **[Anexo #1]**, donde este último punto se centra en la protección de las tecnologías y del activo de mayor importancia que contienen: la información.

Dentro de la seguridad informática está comprendida, como antes expresaba, la seguridad física, pues es una de las formas en que se pueden prevenir o contrarrestar las acciones hostiles o contingencias que en cualquiera de los casos afectan los bienes informáticos, tanto al hardware como al software y la información contenida.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos en coordinación con los objetivos, estrategia y política de la Organización. El mismo proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento.

Luego del análisis de riesgos sigue la gestión de riesgos, que es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis. Las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta.

1.3.2 Descripción actual del dominio del problema

La gran cantidad de información referente al estudio y desarrollo geológico de los últimos cuatro siglos de nuestro país que se almacenará en el Centro de Datos de la Oficina Nacional de Recursos Minerales (ONRM) pasará a formar parte del patrimonio geológico; por el alto valor e importancia que poseen estos datos es necesario garantizar su seguridad ante adversidades de cualquier procedencia. Existen muchísimas empresas nacionales con potentes sistemas de seguridad implementados pero éstas no cuentan con la cantidad de información que almacenará la ONRM, haciéndose más difícil la

protección de los recursos a este nivel.

Precisamente el tema de la seguridad de los Centros de Datos contenedores de grandes volúmenes de información es algo que no se conoce a profundidad en nuestro país, por ser una de las estrategias que se usan en la informática moderna, además de muy costosas y poco difundidas; como ejemplo tenemos que en nuestro país solamente existe un centro de datos perteneciente a la Empresa de Telecomunicaciones de Cuba S.A (ETECSA) que por supuesto, su sistema informático se encuentra respaldado por un plan de seguridad informática. Es lógico que ese plan no esté expuesto para que otras personas fuera del centro lo conozcan porque les estarían dando la llave para que pudiesen acceder al sistema y realizar lo que les plazca con la información que allí se encuentra. Esta es la razón por la que no existe un plan de seguridad para un centro de datos por el cual este trabajo se pueda regir o guiar y que sea factible/consecuente a las necesidades y objetivos trazados por la institución los cuales son:

- Mantener correctamente funcionando el Centro de Datos que facilitará el trabajo de los geólogos cubanos a la hora de introducir los datos obtenidos en el terreno para procesar y almacenar esa información.

- Lograr la confidencialidad, integridad y disponibilidad la información que allí se almacena además de la protección de los activos que componen el sistema y garantizan los servicios.

1.3.3 Situación Problemática

Actualmente el Programa Nacional de Informatización del Conocimiento Geológico (PNICG) se encuentra en la fase de implementación. Una vez que se vaya terminando cada módulo, paulatinamente, y a medidas que el sistema lo permita, se irán actualizando sus bases de datos hasta alcanzar las capacidades previstas de información, los 46 TB que ocuparán en primera instancia, pero que en un futuro no muy lejano como los estudio en el campo geológico no han concluido, aclarar que estas bases de datos irán incrementando su información. Las aplicaciones también se insertarán en los servidores gradualmente por lo que estos deben ser escalables y soportar, de manera eficiente, la incorporación de nuevas tecnologías y nuevos software permitiendo en todo momento una seguridad completa del Centro de Datos y de los activos informáticos que en él se encuentran, dentro de los que se incluye el más importante: la información.

La ONRM planea en un futuro, cuando el PNICG haya terminado un prototipo funcional, la construcción de un Centro de Datos. Como actualmente no existe por ende tampoco existe el plan de seguridad informática para el mismo y que además responda a los objetivos de esta entidad y contenga el análisis de riesgos para tener en cuenta: de qué se desean proteger; de qué es necesario protegerlos y cómo se protegerán todos los activos informáticos que allí se encuentran. No existen las medidas ni las políticas de seguridad en las que se incluyan la seguridad física y lógica; ni los procedimientos y acciones a realizar para prevenir o actuar en caso de que ocurra algún incidente de cualquier procedencia.

Es precisamente esto lo que da paso a la situación problemática planteada: el desconocimiento e inexperiencia acerca de la gestión de la seguridad informática en un Centro de Datos. Una vez que los datos geológicos se encuentren almacenados en los grandes servidores brindando los diferentes tipos de servicios a la cual podrán acceder tanto geólogos como usuarios de cualquier índole, será de vital importancia protegerlos tanto interna como externamente garantizando el acceso y la manipulación correcta de la información almacenada; como también se hace necesaria la protección física del hardware que compone al sistema.

1.4 Análisis de otras soluciones existentes

La existencia de otros planes de seguridad informática en el mundo es imposible de cifrar por la cantidad que hay hoy en día, incluso en nuestro país, aunque también son poco difundidos por su importancia en una entidad y porque además comprometerían la seguridad del sistema y con ello la información que pueda contener. A pesar de que todos persiguen un mismo objetivo como es la seguridad de los activos informáticos, ninguno es igual porque cada organización o entidad tiene sus particularidades a las que son ajustados. Se pueden citar algunos como: El plan de Seguridad Informática y Contingencia del Organismo Central del Ministerio de Educación Cubana y el Plan de seguridad Informática de una Empresa de venta de automotores realizado por María Dolores Cerini y Pablo Ignacio Prá.

El primer plan de seguridad que se citó fue desarrollado por María de los Ángeles Novo, responsable de la seguridad informática en las Oficinas Centrales del Ministerio de Educación (MINED). La misma realiza una caracterización del sistema y hace un análisis de todos los bienes informáticos y de

comunicación que se encuentran en las áreas del edificio del Organismo Central del MINED para confeccionar el plan abarcó todas las tecnologías informáticas instaladas en cada área de la entidad. Basándose en el análisis de riesgos que realizó, refleja las medidas de seguridad a tomar ante cualquier situación para garantizar la continuidad de los procesos informáticos. Así como las políticas de seguridad, los procedimientos tanto físicos como lógicos y por último en caso de la ocurrencia de alguna actividad delictiva con éxito o de una contingencia, el plan de contingencia ante las mismas.

En el segundo plan de seguridad se desarrolla una auditoría de seguridad informática y un análisis de riesgos en una empresa de venta de automotores, con el fin de relevar la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas, operaciones, y el cumplimiento de los reglamentos y normas prescritas. En él se detallan las debilidades encontradas y se proponen soluciones con vista a mejorar la seguridad informática. Este proceso desembocó en un plan de seguridad informática con el propósito de proteger la información y los activos de la organización, tratando de garantizar la confidencialidad, integridad y disponibilidad de los datos; y enmarcando las responsabilidades que debe asumir cada uno de los empleados de la organización.

1.4.1 Principales aportes a nuestro problema

El análisis de los planes de seguridad que se citaron anteriormente brinda de alguna manera la respuesta al problema científico planteado porque ofrecen una línea o guía de trabajo por la cual estará encaminada la investigación, especialmente el primer plan de seguridad, que regirá el desarrollo de este trabajo. La razón es que fue realizado según la **Metodología para la Elaboración del Plan de Seguridad Informática [Anexo #1]** y es por esta metodología que se realizará el plan de seguridad informática.

Ofrecen además una serie de políticas de seguridad, medidas y procedimientos comunes a realizar para prevenir y contrarrestar actividades ilícitas o contingencias y en el caso de que alguna tenga éxito, las acciones a tomar para realizar la recuperación en el menor tiempo posible.

1.5 Conclusiones Parciales

En este primer capítulo se ha hecho un acercamiento general al entorno en el que se encuentra enmarcada la investigación. En forma de conceptos se dan a conocer las terminologías necesarias para entender el trabajo y que se utilizarán a lo largo de su trayectoria. Los puntos abordados ubican al lector en la situación particular en que se desenvuelve la investigación. Se planteó como objetivo principal a desarrollar, la gestión de la seguridad informática en un centro de datos. Para esto, de diferentes formas, se explica la importancia que tiene, tanto para la Oficina Nacional de Recursos Minerales como para el país el desarrollo de un plan de seguridad para mantener la información segura, confiable y disponible en todo momento.

Dentro de los puntos tratados se pueden encontrar temas de mayor importancia: una Descripción General, Descripción actual del dominio del problema y Situación Problemática. Ya en la introducción se habló de estos temas, la diferencia es que en este capítulo se explica más detalladamente en que consisten, dando elementos que enriquecen el significado de lo que se plantea. Casi al final, y no por ser menos importante, se muestran otras soluciones que, de alguna manera, sus objetivos coinciden con esta investigación. Esas soluciones han servido como guía y bibliografía de obligada referencia para comprender mejor el entorno relacionado con los sistemas de gestión de la seguridad informática en el mundo actual.

CAPÍTULO 2: SOLUCIÓN PROPUESTA

2.1 Introducción

En este capítulo se comienza a dar solución al plan de seguridad informática. El marco en que se desenvuelve la investigación es un poco atípico comparado con el proceso que comúnmente se presenta en estos casos. Normalmente para la realización de un plan de seguridad se cuenta con una infraestructura informática desplegada con diferentes niveles de vulnerabilidad en cada uno de sus activos. A partir de ese sistema existente el especialista comienza su trabajo en aras de garantizar una protección óptima y consecuente con la realidad que se presenta. En este caso no se cuenta con dicha infraestructura por lo que forma parte de la investigación tal propuesta asumiendo la responsabilidad de que el despliegue quede conformado tal y como exige el desarrollo de las tecnologías en la actualidad. Aquí se hace una descripción del diagrama de red implementado caracterizando cada activo así como el flujo de información entre estos. También son analizadas todas las amenazas a las que están expuestos los activos, proceso que refleja claramente los diferentes niveles de vulnerabilidad existentes en el sistema. Mediante tablas se realiza el análisis de riesgos que implica el examen de cada uno de ellos y su clasificación por niveles, a partir de la probabilidad de ocurrencia y la severidad del impacto que puedan producir, incluyendo la toma de decisiones sobre la base de criterios de los activos. En esta etapa la investigación está centrada en un estudio detallado de la futura organización que será el Centro de Datos, para ello se destaca como objetivos fundamentales: caracterizar el sistema informático, identificar las amenazas potenciales y estimación del riesgo sobre los activos.

2.2 Caracterización del sistema

Para llevar a cabo la tarea de realizar la gestión de la seguridad informática en cualquier centro hay que tener un domino pleno del funcionamiento y flujo de activos con que se cuenta. Una vez comprendido el entorno de trabajo se estará listo para desplegar todo el conjunto de medidas y políticas que garantice una correcta seguridad. El primer paso del que se habla no es más que una Auditoria Informática. Este término no va ha ser tratado a profundidad en la investigación pero si es necesario comprenderlo por su importancia. La auditoria informática es un proceso de revisión de inventariado, usualmente se usa como información de retroalimentación, para analizar en que medida el sistema garantiza la seguridad informática, pero no ofrece una visión general del sistema, solo

puede detectar puntos de fallos concretos sobre cada activo. Explícitamente se deduce que para poder realizar una auditoria de este tipo, tiene que existir una entidad con cierto nivel de desarrollo tecnológico. Esta entidad, tenga o no un sistema de seguridad informático implementado, brinda una base al especialista para su futuro trabajo.

En el caso particular de la presente investigación se trabajará para un Centro de Datos que será instalado en el futuro. La empresa encargada de hacer la inversión, como ya se ha mencionado con anterioridad, será la Oficina Nacional de Recursos Minerales y serán también esta empresa el principal usuario. Los activos seleccionados en el estudio forman una propuesta lo más cercana posible al despliegue final, y la investigación en general se considerará una guía o herramienta de trabajo una vez comience a funcionar el centro.

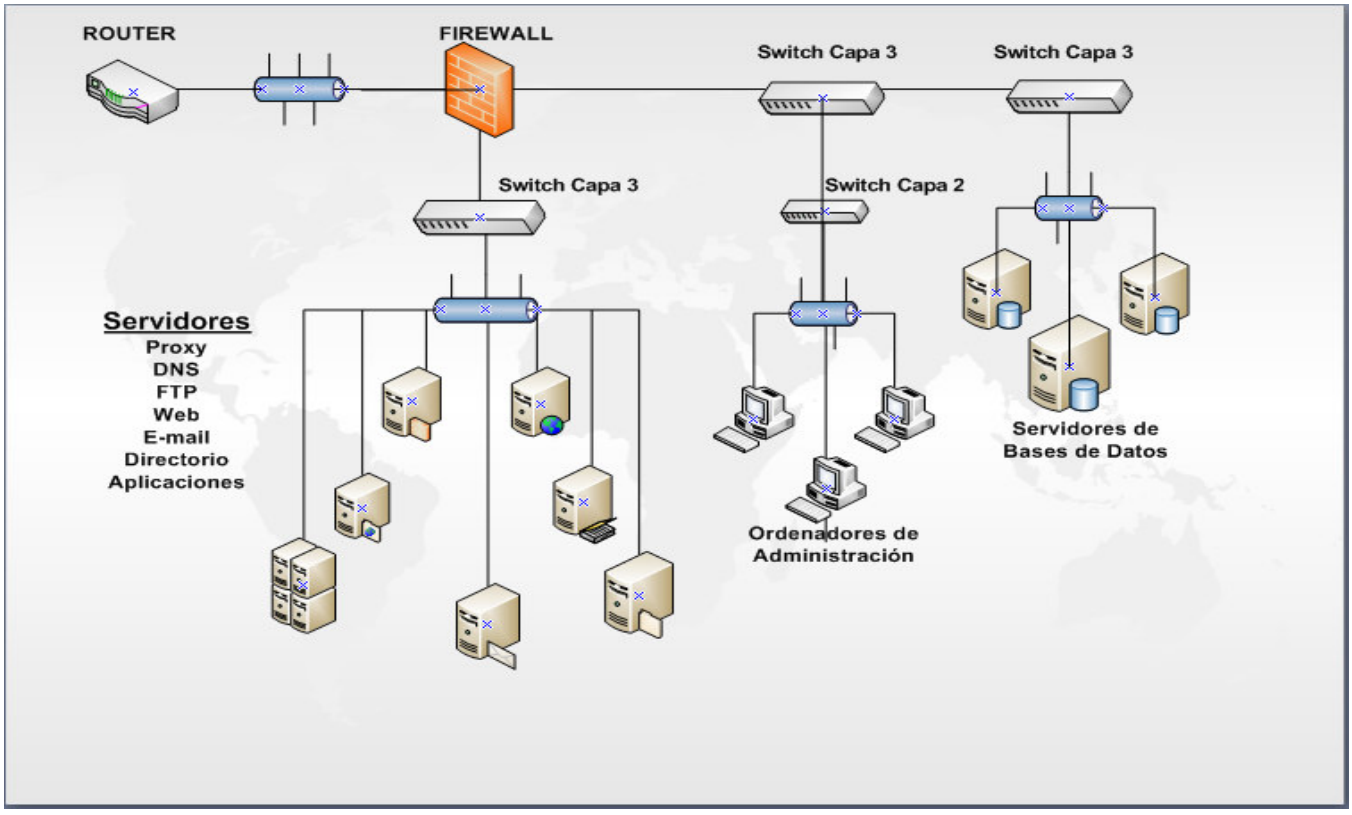
Los activos estarán ubicados por áreas de trabajo según las funciones que prestan. La idea de formar áreas ayuda a la comprensión del sistema y mejora el proceso de instalación y mantenimiento de la tecnología desplegada y la información contenida. Las áreas indican también el uso de locales con características físico ambiental, adecuadas a cada caso. A continuación se muestra la relación de estas áreas:

Área 1	Router Wan, Firewall por hardware, Switch Core capa tres, Switch de la DMZ capa tres, Switch capa tres, servidores de comunicación, servidor de Directorios de Usuarios, servidor de Aplicaciones y servidores de Base de Datos.
Área 2	Switch capa dos y ordenadores de administración.

Después de un análisis riguroso de documentos, búsqueda en Internet, entrevistas y conocimientos propios quedó conformada la red. No se está hablando de un local pequeño con características tradicionales donde la seguridad se resuelve, en muchos casos, con la buena configuración de un Firewall. Dado la gran cantidad de información sensible, de la cual el centro será responsable, los sistemas y componentes que conforman la red tienen características muy superiores a las que comúnmente existen en las diferentes empresas. Si bien las dimensiones físicas de este centro no son tan amplias, el tráfico de información que va a entrar y salir constantemente sí lo será, lo que conlleva al uso de hardware con características que permitan el funcionamiento óptimo de la red. Seguidamente se explica la propuesta que se realizó de como quedará conformada la red con todos sus componentes y el flujo dentro de ella.

Mediante un Router es conectado el centro directamente a la Internet. Este flujo de información es analizado rigurosamente por el Firewall (cortafuego) principal encargado de la protección contra intrusos y del análisis de cada paquete que entra y sale de la red. Este Firewall será de tipo WAN por hardware. Los servidores de comunicación: servidor DNS, servidor FTP, Servidor Web, servidor de Aplicaciones y servidor de Directorio de Usuarios están ubicados en una Zona Desmilitarizada (DMZ) para mayor seguridad. Esta configuración se hace en el Firewall con el objetivo de lograr la mayor seguridad posible dado que los servidores implicados son los que están expuestos directamente a la red externa mediante los servicios que prestan. Conectado también al cortafuego se encuentra un Switch Core capa tres, correctamente configurado, encargado de distribuir la red en dos subredes. Una de estas, formada por los servidores de Bases de Datos, conectados a otro Switch capa tres y la otra con las máquinas de administración conectadas a un Switch capa dos. Tanto la red desmilitarizada como la subred que contiene los servidores de Bases de Datos requieren de cableado de tipo fibra óptica para garantizar la velocidad de la red así como el tráfico de información que circulará por ella. Seguidamente se muestra el diagrama de red resultante de la entrevista realizada al compañero Dixan Mastrapa (**Anexo #2**) para mejor comprensión.

Diagrama de red:



Dada la configuración de la red y la cantidad de activos, se pueden conformar dos locales. Los diferentes departamentos del centro están en correspondencia con las áreas definidas anteriormente. La seguridad física de cada uno de los locales también depende del valor de los activos que contiene.

El recinto estará dividido en dos partes fundamentales; en una división se encuentran el Switch capa dos y varias computadoras para el control y administración del centro. En la otra división se encuentran los servidores de comunicación: servidor DNS, servidor FTP, Servidor Web, servidor de Aplicaciones, además se encuentran otros activos como: Router Wan, Firewall por hardware, Switch Core capa tres, el Switch capa tres de la DMZ, Switch capa tres para los servidores de Bases de Datos, servidores de Bases de Datos y servidor de Directorios. También se dispondrá del uso de un circuito cerrado de televisión para observar constantemente lo que está sucediendo en todo el local y dejar grabadas las imágenes para ser usadas en caso de algún acto ilícito que afecte el sistema, así como el uso de puertas con acceso restringido.

2.2.1 Flujo de la información

Publicado en Internet estarán los diferentes servicios que se prestarán por parte del centro de datos. Existen diferentes niveles de privilegios para los usuarios que accedan al sistema. Si solo se quiere ver la presentación del sitio web o algún dato general, se puede acceder como invitado, solo que de esa forma no podrá acceder a ningún servicio importante. Una vez que el usuario es registrado se le asigna un nivel de privilegio mediante el cual podrá navegar y realizar las operaciones que le sean permitidas. Todo el intercambio externo se realiza directamente mediante el servidor Web. En el caso de que el usuario sea de tipo invitado, este servidor podrá brindar información sin tener que conectarse a otro servidor. Por el contrario, si el usuario tiene algún privilegio, la primera operación será la autenticación y asignación del privilegio, comprobando esa información en el servidor de Directorio de Usuarios. Para dar respuesta a las diferentes consultas de los servicios prestados, el servidor Web se conectará al servidor de Aplicaciones y éste es el que buscará la información en los servidores de Bases de Datos. De esta manera se llevará cabo el proceso de flujo de la información en el centro resaltando que el control de todas las aplicaciones y activos se realizará mediante las máquinas de administración por los administradores del sistema.

2.2.2 Componentes del Sistema Informático

Para mayor comprensión se realizará a continuación una breve descripción de los componentes de

hardware que se propusieron para conformar el sistema informático, así como las tareas y funciones que cumplirán en dicho sistema y por el cual fueron seleccionados.

2.2.2.1 Router

"En términos simples, un Router es un dispositivo algo más grande que un módem con capacidad para hacer muchas cosas que normalmente realiza un computador. Es como una especie de mini-computador que logra unir ordenadores entre sí, conectarlos a Internet y poner una barrera de seguridad entre la Red y la PC. En otras palabras, son un puente entre varios dispositivos informáticos que se comunican. A diferencia de un Hub o un Switch del tipo capa 2, un Router inspecciona cada paquete de información para tomar decisiones a la hora de encaminarlo de un lugar a otro. Un Switch del tipo capa 3 sí tiene también esta funcionalidad. Profundizando más en su funcionamiento, un Router es un dispositivo que encamina tráfico desde una red conectada a uno de sus puertos hacia otra red conectada en otro de sus puertos. Para ello necesita:

- Saber la dirección de destino: ¿Dónde va la información que necesita ser encaminada?
- Identificar las fuentes de la información a ser encaminada: ¿Cuál es el origen de la información?
- Descubrir las rutas: ¿Cuáles son las posibles rutas iníciales o caminos, a los destinos de interés?
- Seleccionar rutas: ¿Cuál es el mejor camino para el destino que se requiere?
- Mantener y verificar la información de routing: ¿Está la información sobre el camino hacia el destino, actualizada?" [13].

2.2.2.2 Firewall

"Un Firewall/Cortafuegos es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet). El Muro Cortafuegos, sólo sirve de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer

protección una vez que el intruso lo traspasa.

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "No es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir password(s) o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta. El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados"[14].

2.2.2.3 Switch

Los Switch(s) son otro tipo de dispositivo utilizados para enlazar LAN(s) separadas y proveer los paquetes entre ellas. Un Switch es un dispositivo con múltiples puertos, cada uno de los cuales puede soportar una simple estación de trabajo o bien toda una red Ethernet o Token Ring con una LAN diferente conectada a cada uno de los puertos del Switch, este puede conmutar los paquetes entre ellas, como sea necesario. Se utilizan para aumentar el rendimiento en las redes de las organizaciones, segmentando las grandes en varias más pequeñas lo que disminuye la congestión a la vez que sigue proporcionando la ínter conectividad necesaria.[15]

2.2.2.4 Servidor Proxy

Un Servidor Proxy permite la conexión de la red privada o LAN a una red pública como Internet, actuando como puerta de enlace para las computadoras de los clientes internos a Internet. Proxy Server es una puerta de enlace de seguridad que se puede utilizar para proporcionar conectividad a Internet para IP y redes basadas en IPX. Una puerta de enlace es un ordenador que permite a las dos redes de comunicación intercambiar información. "El Proxy es un sistema pensado para establecer una política de acceso de salida, es decir, sirve para determinar que páginas de Internet pueden ser visitadas y además por quién. Dispone de informes sobre los accesos a Internet y de caché para acelerar la navegación de páginas ya visitadas"[16].

"Algunas características de este tipo de servidor son:

a. Proporciona una capa extra de seguridad.

b. Aísla a los usuarios de la Intranet.

c. Un Proxy actúa como un 'cache', es decir un almacenamiento dinámico de información con mayor acceso.

d. Se realiza una vigilancia, control y acceso transparente para el usuario.

e. Se pueden hacer usos de las características que ofrece para definir listas de control de acceso, tanto para usuarios, como para URL(s).

f. Permite el control de acceso a diferentes sitios Web"[17].

2.2.2.5 Servidor DNS

Los servidores de Sistemas de Nombres de Dominio (DNS, Domain Name System) alojan registros de una base de datos DNS distribuida y los utilizan para resolver consultas de nombres DNS enviadas por equipos clientes DNS, por ejemplo, consultas de nombres de equipos o sitios Web de la red o Internet. "Un servidor DNS se utiliza para proveer a las computadoras de los usuarios (clientes) un nombre equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios cuando éste está bien configurado. Cada Red de Área Local (LAN) debería contar con un servidor DNS. Estos servidores trabajan de forma jerárquica para intercambiar información y obtener las direcciones IP de otras LAN(s)"[18].

2.2.2.6 Servidor Web

"El servidor Web es un programa que corre sobre el servidor que escucha las peticiones HTTP que le llegan y las satisface. Dependiendo del tipo de la petición, el servidor Web buscará una página Web o bien ejecutará un programa en el servidor. De cualquier modo, siempre devolverá algún tipo de resultado HTML al cliente o navegador que realizó la petición. El servidor Web va a ser fundamental en el desarrollo de las aplicaciones del lado del servidor, server side applications, que vayamos a construir, ya que se ejecutarán en él".[19]

2.2.2.7 Servidor de Correo

Un servidor de correo es una aplicación informática que permite enviar mensajes de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando. Entre los más usados se

encuentran send mail y Exim, este último predeterminado en la distribución GNU/Linux Debian.
Para lograr la conexión se definen una serie de protocolos, cada uno con una finalidad concreta:
SMTP (Simple Mail Transfer Protocol): Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

POP (Post Office Protocol): Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

IMAP (Internet Message Access Protocol): Su finalidad es la misma que la de, POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP, que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

2.2.2.8 Servidor FTP

"Un servidor FTP es un programa especial que se ejecuta en un servidor conectado normalmente en Internet (aunque puede estar conectado en otros tipos de redes, LAN, MAN, etc.). La función del mismo es permitir el desplazamiento de datos entre diferentes servidores / ordenadores.

Algunos ejemplos del uso que se le puede dar a este tipo de servidores son:
Como servidor de backups (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación FTP para que los datos viajen encriptados, como el SFTP (Secure File Transfer Protocol).

Como servidor para compartir archivos de imágenes, información o software(s) para los trabajadores de la empresa según los permisos de acceso que se les hayan otorgado; de esta manera se ahorran tener que ir hasta la entidad para obtener o depositar los útiles de trabajo". [20]

2.2.2.9 Servidor de Aplicaciones

"Proporciona servicios que soportan la ejecución y disponibilidad de las aplicaciones desplegadas. Es el corazón de un gran sistema distribuido"[21]. "Un servidor de aplicaciones no es más que un cambio de nombre, para algunos servidores Web de nueva generación que proporcionan la lógica de negocio

sobre la que construir aplicaciones. Suelen asociarse con servidores de alto rendimiento pensados para dar servicio a sitios Web (Web Sites) con grandes necesidades: afluencia de visitas, movimiento de datos, atención de transacciones hacia bases de datos, etc. Generalmente los fabricantes del sector tienen a disposición del público un servidor Web básico y otro con multitud de extensiones fuertemente integradas al que llaman servidor de aplicaciones"[22].

2.2.2.10 Servidor de Bases de Datos

"Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modo cliente-servidor. También puede hacer referencia a aquellas computadoras dedicadas a ejecutar esos programas, prestando el servicio. Los sistemas de administración de bases de datos (SGBD) generalmente proveen funcionalidades para servidores de bases de datos, en cambio otros (como por ejemplo, MySQL) solamente proveen construcción y acceso a la base de datos"[23].

2.3 Análisis de Riesgos

Un sistema de medidas para la Seguridad Informática incluye el establecimiento de las políticas y procedimientos que conforman una estrategia de cómo tratar los aspectos de seguridad donde la base de este proceso radica en la realización de un **análisis de riesgos** lo que implica determinar las necesidades de protección del sistema informático objeto de análisis.

2.3.1 Identificación de los activos informáticos

El primer paso consiste en la identificación de los activos y recursos informáticos que necesitan ser protegidos. En esta primera tabla (**Tabla 1**) se muestra la propuesta oficial de todos los activos que compondrán al futuro sistema informático indicando rasgos que facilitan el proceso de caracterización como los que se encuentran a continuación:

Según el **Tipo** de activo:

Hardware (HD): computadoras personales, servidores, estaciones de trabajo, soportes magnéticos, líneas de comunicaciones, módems, Router, concentradores, etc.

Software (SW): programas fuentes, programas ejecutables, programas de diagnóstico, utilitarios, sistemas operativos, programas de comunicaciones, etc.

Datos (DT): durante la ejecución, almacenados en discos, backup(s), bases de datos, rastros de auditoría, en tránsito por los medios de comunicaciones, etc.

Según el Área de **Ubicación**:

Área # 1: Área de Servidores.

Área # 2: Área de Administración.

En cuanto al No. de Serie, cuando se realice el inventario se registrará el número de serie que el activo posee de fabricación o se le asignará uno nuevo durante la acción.

Tabla #1: Identificación de Activos Informáticos

No.	Descripción	Tipo	No. Serie	Ubicación
1	Servidor de Datos Geológicos	HW	10001	Área #1
2	Datos geológicos	DT	10002	Área #1
3	Servidor de Aplicaciones	HW	10003	Área #1
4	Aplicaciones	SW	10004	Área #1
5	Servidor de Salvaguardas	HW	10005	Área #1
6	Salvaguardas	DT	10006	Área #1
7	Servidor para datos de usuarios	HW	10007	Área #1
8	Datos de usuarios	DT	10008	Área #1
9	Servidor de Correos	HW	10009	Área #1
10	Servidor Web	HW	100010	Área #1
11	Servidor FTP	HW	100011	Área #1
12	Switch Principal capa 3	HW	100012	Área #1
13	Ordenadores de Administración	HW	100013	Área #2
14	Switch capa 3 (DMZ)	HW	100014	Área #1
15	Servidor Proxy	HW	100015	Área #1
16	Servidor DNS	HW	100016	Área #1
17	Firewall Principal	HW	100017	Área #1
18	Router	HW	100018	Área #1
19	Switch capa 3(Para servidores de BD)	HW	100019	Área #1
20	Switch capa 2	HW	100020	Area #2
21	Cableado, aire acondicionado, sistema cerrado de tv.	HW	100021	Área #1 Área #2

2.3.2 Evaluación de los activos informáticos

Una vez obtenido el resultado de la caracterización con el listado de la relación de los activos y recursos identificados. Se muestra en la **Tabla 2** la forma de valorar la importancia de los activos que componen el sistema informático, a partir del papel que juegan dentro del mismo.

Tabla #2: Evaluación de Activos Informáticos

No.	Dom.	Función	Costo	Imagen	CONF	INTEG	DISP	Valor (Wi)
1	Área #1	10	10	10	10	10	10	10.00
2	Área #1	10	10	10	10	10	10	10.00
3	Área #1	9	9	9	8	10	10	9.17
4	Área #1	9	10	8	7	8	10	8.67
5	Área #1	6	8	6	10	9	8	7.83
6	Área #1	6	8	6	10	9	7	7.67
7	Área #1	8	8	9	10	8	10	8.83
8	Área #1	8	8	9	10	8	10	8.83
9	Área #1	6	8	5	9	8	7	7.17
10	Área #1	8	8	9	10	9	10	9.00
11	Área #1	9	8	8	9	8	9	8.50
12	Área #1	10	10	9	10	10	10	9.83
13	Área #2	9	8	9	7	7	8	8.00
14	Área #1	10	10	9	10	10	10	9.83
15	Área #1	8	8	8	7	8	9	8.00
16	Área #1	9	9	8	10	9	9	9.00
17	Área #1	10	10	10	10	10	10	10.00
18	Área #1	10	10	9	7	7	10	8.83
19	Área #1	10	10	9	10	9	10	9.67
20	Área #2	8	8	8	9	9	9	8.5
21	Área #1 Área #2	10	10	10	5	5	10	8.33

La determinación de la importancia de cada activo y recurso se realiza de forma numérica. A las columnas de la 3 a la 8 se le asignaron valores entre 0 y 10, a partir de la estimación que se hizo de la importancia de cada uno de estos factores sobre los activos informáticos (0 sin importancia y 10 máxima). Pudiendo guiarse por la siguiente escala:

Nula	Baja			Media			Alta			Máxima
0	1	2	3	4	5	6	7	8	9	1

Donde No.: es el Número de Orden consecutivo (se obtiene de la **Tabla 1** según le fue asignado al activo).

Dominio: Identificación para agrupar los activos afines por las funciones que realizan y/o por la administración sobre ellos. (Área1, Área2,... Área N según la cantidad que se cree).

Función: Importancia de la tarea que cumple el activo.

Costo: Valor y valor de uso del activo.

Imagen: Repercusión interna y/o externa que ocasionaría la pérdida del activo.

Confidencialidad: Necesidad de proteger la información que del activo se pueda obtener.

Integridad: Necesidad de que la información no se modifique o destruya.

Disponibilidad: Que los servicios que de los activos se esperan puedan ser obtenidos en todo momento de forma autorizada.

Valor (**Wi**): **Importancia del activo**

Wi = Promedio de los valores asignados al activo.

2.3.3 Listado de las amenazas

Resumiendo la búsqueda en Internet y todo tipo de documentos relacionados con el tema, se realizó una lista enumerada con las amenazas que podrían poner en riesgo a cada uno de los activos y en sí al sistema informático completo. Las mismas serán utilizadas en la Tabla No. 3 y posteriormente en la realización de la Tabla No. 4 donde las identificará el número asignado.

El listado es el siguiente:

1- Acceso no autorizado.
2- Fallo de Energía eléctrica.
3- Fallo de Hardware.
4- Incendios.
5- Error de configuración.
6- Hurto de activos y/o recursos.
7- Mal funcionamiento o carencia de aire acondicionado.
8- Mal mantenimiento.
9- Límite de vida útil.
10- Abuso de privilegios de acceso.
11- Manipulación de la configuración del firewall interno.

12- Falla en los medios externos.
13- Perdida de confidencialidad en datos sensibles y del sistema.
14- Virus.
15- Copia no autorizada de datos en medios de almacenamientos.
16- Errores de software.
17- Transferencia de datos incorrectos.
18- Pérdida de datos en tránsito.
19- Mala integridad de los datos.
20- Spoofing y sniffing.
21- Denegación de servicio.
22- Errores de los usuarios en la introducción de datos.
23- Suplantación de identidad.
24- Reducción de velocidad de transmisión.
25- Ancho de banda insuficiente.
26- Robo de contraseñas.
27- Destrucción negligente de los equipos.
28- Falta de confidencialidad.
29- Software desactualizado.
30- Acceso pirata en la red interna.
31- Fallo de servicios de comunicaciones.
32- Errores de monitorización (Log).
33- Manipulación de la configuración.
34- Daño de cables inadvertido.
35- Conexión de cables inadmisibles.

2.3.4 Identificación de las amenazas por activos

Luego de calcular la importancia de cada activo (Tabla No. 2) se desarrolló la Tabla No. 3 donde se muestra el análisis a partir de la identificación de las amenazas que pueden afectar el sistema informático y su incidencia sobre cada uno de los activos que lo componen. Se abrió una columna con el número y otra para el nombre de cada activo identificado en la Tabla No. 1 y por último una columna con el nombre de las amenazas que pueden afectarlo.

Tabla #3: Identificación de las Amenazas por Activos Informáticos		
No.	**Nombre del Activo**	**Amenazas**
1	**Servidor de Datos geológicos:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Error de configuración
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Límite de vida útil
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno
2	**Datos geológicos:**	Acceso no autorizado
		Falla en los medios externos
		Perdida de confidencialidad en datos sensibles y del sistema
		Virus
		Copia no autorizada de datos en medios de almacenamientos
		Errores de software
		Transferencia de datos incorrectos
		Perdida de datos en tránsito
		Mala integridad de los datos
		Spoofing y sniffing
		Denegación de servicio
		Abuso de privilegios de acceso
		Errores de los usuarios en la introducción de datos
3	**Servidor de Aplicaciones:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Límite de vida útil
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno

No.	Nombre del Activo	Amenazas
4	**Aplicaciones:**	Acceso no autorizado
		Falla en los medios externos
		Perdida de confidencialidad en datos sensibles y del sistema
		Virus
		Errores del software
		Denegación de servicio
		Abuso de privilegios de acceso
		Spoofing y sniffing
5	**Servidor de Salvaguardas:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Error de configuración
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Límite de vida útil
		Manipulación de la configuración del firewall interno
6	**Salvaguardas:**	Acceso no autorizado
		Falla en los medios externos
		Perdida de confidencialidad en datos sensibles
		Virus
		Copia no autorizada de datos en medios de almacenamientos
		Errores de software
		Transferencia de datos incorrectos
		Spoofing y sniffing
		Perdida de datos en tránsito
		Abuso de privilegios de acceso
7	**Servidor para datos de usuarios:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Error de configuración
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Límite de vida útil
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno

No.	Nombre del Activo	Amenazas
8	**Datos de usuarios:**	Acceso no autorizado
		Falla en los medios externos
		Perdida de confidencialidad en datos sensibles
		Virus
		Suplantación de identidad
		Copia no autorizada de datos en medios de almacenamientos
		Errores de software
		Transferencia de datos incorrectos
		Perdida de datos en tránsito
		Mala integridad de los datos
		Abuso de privilegios de acceso
		Spoofing y sniffing
9	**Servidor de Correos:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Error de configuración
		Límite de vida útil
		Manipulación de la configuración
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno
10	**Servidor Web:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Error de configuración
		Mal mantenimiento
		Límite de vida útil
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno

No.	Nombre del Activo	Amenazas
11	**Servidor FTP:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Error de configuración
		Límite de vida útil
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno
12	**Switch CORE capa 3:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Error de configuración
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Reducción de velocidad de transmisión
		Límite de vida útil
		Ancho de banda insuficiente
		Destrucción negligente de los equipos
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno
13	**Ordenadores de Administración:**	Acceso no autorizado
		Robo de contraseñas
		Hurto de activos y/o recursos
		Destrucción negligente de los equipos
		Suplantación de identidad
		Virus, gusanos y caballos de Troya
		Falta de confidencialidad
		Software desactualizado
		Acceso pirata en la red interna
		Fallo de servicios de comunicaciones

No.	Nombre del Activo	Amenazas
14	**Switch capa 3 (DMZ):**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Error de configuración
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Destrucción negligente de los equipos
		Reducción de velocidad de transmisión
		Límite de vida útil
		Ancho de banda insuficiente
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno
15	**Servidor Proxy:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Hurto de activos y/o recursos
		Errores de monitorización (log)
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Error de configuración
		Manipulación de la configuración
		Límite de vida útil
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno
16	**Servidor DNS:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Error de configuración
		Límite de vida útil
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno

No.	Nombre del Activo	Amenazas
17	**Firewall Principal:**	Acceso no autorizado
		Incendios
		Mal funcionamiento o carencia de aire acondicionado
		Límite de vida útil
		Manipulación de la configuración
		Error en la configuración
		Mal mantenimiento
		Fallo de Energía eléctrica
		Fallo de Hardware
18	**Router:**	Acceso no autorizado
		Fallo de Hardware
		Fallo de Energía eléctrica
		Error en la configuración
		Manipulación de la configuración
		Incendios
		Abuso de privilegios de acceso
		Mal mantenimiento
		Mal funcionamiento o carencia de aire acondicionado
		Límite de vida útil
19	**Switch Capa 3(Servidores de BD):**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Error de configuración
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Destrucción negligente de los equipos
		Mal mantenimiento
		Reducción de velocidad de transmisión
		Límite de vida útil
		Ancho de banda insuficiente
		Abuso de privilegios de acceso
		Manipulación de la configuración del firewall interno

No.	Nombre del Activo	Amenazas
20	**Switch capa 2:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Error de configuración
		Hurto de activos y/o recursos
		Mal funcionamiento o carencia de aire acondicionado
		Mal mantenimiento
		Reducción de velocidad de transmisión
		Límite de vida útil
		Ancho de banda insuficiente
		Abuso de privilegios de acceso
		Manipulación de la configuración
21	**Cableado, aire acondicionado, sistema cerrado de tv:**	Acceso no autorizado
		Fallo de Energía eléctrica
		Fallo de Hardware
		Incendios
		Mal mantenimiento
		Daño de cables inadvertido
		Conexión de cables inadmisibles
		Límite de vida útil
		Abuso de privilegios de acceso

2.3.5 Valoración de Riesgos

A partir de la Tabla No. 3 donde se identificaron las amenazas que ponen en peligro la seguridad de cada uno de los activos, se cuantificó el riesgo de que cada una de ella se materialice llegando a afectarlos. Esto se refleja en la **Tabla No. 4** donde se organizó de la forma siguiente:

No. y Dom. (Número consecutivo y Dominio) correspondiente en la **Tabla No. 2**

R1, R2...Rn Reflejan la posibilidad de que se materialicen las amenazas identificadas en la **Tabla No. 3** sobre cada activo, a los que se les asignó valores entre 0 y 1 de acuerdo a las probabilidades de ocurrencias que se estimaron según la siguiente tabla de valores:

Nula	Baja			Media			Alta			Máxima
0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1

También se realizaron los cálculos siguientes:

La Valoración de riesgos (**Ri**) donde:

Ri = Promedio de las Amenazas o riesgos marcados que pueden afectar al activo.

La importancia del Activo (**Wi**)

Wi = Se obtiene de los valores estimados en la Tabla No. 2.

El peso del riesgo de cada Activo (**P**)

P= Ri * Wi

Tabla4

VALORACION DE RIESGOS

	NO ->	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21		
Riesgos	Dom.->	A#1	A#1	A#1	A#1	A	A#1	A#1	A#1	A#1	A#1	A#1	A#1	A#2	A#1	A#1	A#1	A#1	A#1	A#1	A#:	A#1	Suma	Promedio
R1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	21	1
R2		0,7		0,7		0,7		0,7		0,7	0,7	0,7	0,7		0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	11,2	0,7
R3		0,4		0,5		0,6		0,6		0,5	0,5	0,5	0,6		0,6	0,7	0,7	0,5	0,5	0,6	0,6	0,6	9	0,5625
R4		0,3		0,3		0,3		0,3		0,3	0,3	0,3	0,3		0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	4,8	0,3
R5		1				1		1		1	1	1	1		1	1	1	1	1	1	1		14	1
R6		0,4		0,4		0,3		0,4		0,4	0,4	0,4	0,3	0,4	0,3	0,3	0,3			0,3	0,3		4,9	0,35
R7		0,4		0,4		0,4		0,4		0,4	0,4	0,4	0,4		0,4	0,4	0,4	0,4	0,4	0,4	0,4		6	0,4
R8		0,6		0,7		0,7		0,6		0,6	0,6	0,6	0,7		0,7	0,6	0,6	0,6	0,6	0,7	0,7	0,7	10,3	0,64375
R9		0,5		0,5		0,5		0,5		0,5	0,5	0,5	0,5		0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	8	0,5
R10		0,8	0,9	0,7	0,8		0,8	0,9	0,9	0,8	0,8	0,8	0,8		0,8	0,9	0,9		1	0,8	0,8	0,8	14,7	0,816667
R11		0,9		0,8		0,7		0,9		0,7	0,7	0,7	0,8		0,8	0,7	0,7			0,8	0,8		9,65	0,742308
R12			0,6		0,6		0,6		0,6														2,4	0,6
R13			0,8		0,8		0,9		0,9														3,4	0,85
R14			1		1		1		1					1									5	1
R15			0,7				0,8		0,9														2,3	0,766667
R16			0,5		0,7		0,5		0,4														2,1	0,525
R17			0,4				0,5		0,4														1,3	0,433333
R18			0,4				0,4		0,4														1,2	0,4
R19			0,5						0,5														1	0,5
R20			0,6				0,6		0,6														1,8	0,6
R21			0,4		0,7																		1,05	0,525
R22			0,5																				0,5	0,5
R23									0,9					0,9									1,7	0,85
R24													0,5		0,5					0,5	0,5		2	0,5
R25													0,3		0,3					0,3	0,4		1,3	0,325
R26														0,6									0,6	0,6
R27													0,5	0,5	0,5					0,5	0,5		2,5	0,5
R28														0,5					1				1,5	0,75
R29														0,4									0,4	0,4
R30														0,6									0,6	0,6
R31														0,5									0,5	0,5
R32																1							1	1
R33													0,9		0,9	0,9		0,8	0,9	0,9	0,9		5,95	0,85
R34																						0,7	0,7	0,7
R35																						0,9	0,85	0,85
Ri		0,6	0,6	0,6	0,8	0,6	0,7	0,7	0,7	0,6	0,6	0,6	0,6	0,6	0,6	0,7	0,6	0,6	0,7	0,6	0,6	0,7	13,65	0,64997
Wi		10	10	9,2	8,7	7,8	7,7	8,8	8,8	7,2	9	8,5	9,8	8	9,8	8	9	10	8,8	9,7	8,5	8,3	185,7	8,840952
P		6,4	6,4	5,5	6,8	4,9	5,4	5,9	6,2	4,4	5,6	5,3	6	5,1	6	5,5	5,8	6,4	6,3	5,9	5,3	5,5	120,5	5,738314

2.3.6 Resultado del Análisis

Realizado el análisis de riesgos ya se tiene el listado de los recursos que se desean proteger (Tabla 1) además de saber cuales son los más importantes, siendo este uno de los objetivos del análisis de riesgos. También se encuentran definidas muchas de las amenazas a las que pueden estar expuestos los activos que componen el sistema informático y las probabilidades de que estas se materialicen.

Mediante la **Tabla 4** se determinó el Riesgo Total del Sistema (W_R), siendo este de 0,65 y que se obtuvo dividiendo la suma total de los valores del peso del riesgo de cada activo (**P**) por la suma total de la importancia de los activos (**Wi**). La fórmula seria la siguiente:

$$w_R = \sum_{i=1}^{21} R_i \times w_i \Big/ \sum_{i=1}^{21} w_i$$

De forma análoga se pudieron obtener el riesgo total de cada una de las áreas, en la que se determinó mediante los cálculos siguientes que el **Área #1** implicaba un riesgo de 0,65 y el **Área #2** de 0,64 respectivamente:

$$w_{R_1} = \sum_{i=1}^{19} R_i \times w_i \Big/ \sum_{i=1}^{19} w_i$$

,

$$w_{R_2} = \sum_{i=1}^{3} R_i \times w_i \Big/ \sum_{i=1}^{3} w_i$$

El resultado entre la comparación de los riesgos por área determinó que el Área de los servidores que contendrá los activos y recursos de mayor importancia y que por la cantidad de amenazas a los que pueden estar expuestos los mismos, tiene mayor peso de riesgo que el **Área #2,** área donde se encontrarán ubicados los ordenadores de administración.

En caso de que se materialice alguna de las amenazas anteriormente expuestas en la **Tabla No. 3** sobre algún activo, el impacto en la entidad podría ser la perdida física tanto del componente en específico como la información que pueda estar contenida en él incluyendo todas las tareas dependientes según su función. En resumen, lo que podría originarse en cualquiera de los casos sería la falta de confidencialidad, integridad o disponibilidad de la información, lo que afectaría la toma de decisiones de nuestro país en el campo de la geología y en las demás ramas que dependen de esta,

al mismo tiempo que afecta los estudios geológicos que llevan a cabo los especialistas.

2.4 Políticas de seguridad

El actual cambiante mundo de las informáticas y las comunicaciones trae nuevos retos a todas aquellas instituciones que desean o necesitan proteger sus bienes y garantizar la supervivencia. Estar conectado a la red implica convivir en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., que, ya sea por diversión personal, desconocimiento de medidas penitenciarias o simplemente con toda la intención, buscan una vía de entrada a los sistemas de seguridad y en muchos casos dejan irreparables daños. Todo este incremento de las amenazas viene dado por el uso masivo y universal de la Internet y el desarrollo tecnológico actual.

En muchos casos las políticas de seguridad son ignoradas por ser difíciles de llevar a cavo o porque no se entienden por la ambigüedad con que fueron elaboradas. A continuación se presentan el conjunto de políticas que regirán el comportamiento del Centro de Datos. Éstas han sido desarrolladas lo más general posible tratando en todo momento de proporcionar las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán. Es altamente importante que estas políticas sean del conocimiento de todos los trabajadores y usuarios finales, así como aquellas personas que de alguna manera interactúen con el centro.

En la Administración de Redes o Administración del Sistema se encontrarán los responsables del Centro de Datos, quienes se encargarán de hacer cumplir las políticas de seguridad implantadas y de llevar a cabo todo el proceso de cumplimiento de las mismas.

2.4.1 Generales

1. Todos los activos tangibles del centro deben estar controlados por un número de inventario, además un sello de seguridad para aquellos equipos que lo permitan.

2. Los usuarios que accedan desde el exterior (Internet) al centro, se comunican solo con los servidores Web, de correo y servidor FTP en caso autorizado.

3. Los servidores de Bases de Datos tendrán comunicación sólo con el servidor de Aplicaciones y con las máquinas de administración, no así con la red externa.

4. Cada equipo de cómputo tendrá correctamente configurado su Firewall interno.

5. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).

6. Corresponde al departamento de Administración de Redes autorizar cualquier adquisición y actualización del software.

7. Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

8. La contraseña empleada por los usuarios para acceder a los servicios telemáticos tendrá una longitud de 8 caracteres como mínimo y debe cumplir con varios requerimientos de complejidad como empleo de números, caracteres especiales, letras mayúsculas y minúsculas.

9. Debe existir un grupo de administración que permanecerá en el grupo de administradores de cada máquina de trabajo y servidores con vista a facilitar las tareas de soporte técnico o la realización de auditorias.

10. Todo el tráfico de información entre el interior y el exterior del centro debe pasar a través del Firewall por hardware donde quedará constancia de esas acciones mediante los Log(s) que se generarán.

11. Debe llevarse un registro de toda la actividad dentro de la red interna a través del Proxy.

12. Para la protección contra virus se utilizarán los programas antivirus de producción nacional u otros autorizados oficialmente para su uso en el país, debidamente actualizados.

13. Los ficheros adquiridos por cualquier vía deberán pasar por un proceso exhaustivo de descontaminación que garantice la eliminación de cualquier virus informático o programa maligno.

2.4.2 Instalación de equipos de cómputo

1. Tanto los ordenadores de administración, servidores de comunicación para Internet, servidores de Bases de Datos, así como cualquier dispositivo que se conecte a la red interna, sea propiedad del centro o no, debe sujetarse a las normas y procedimientos de instalación que emite el departamento de Dirección de Redes.

2. La Dirección de Redes deberá tener un registro de todos los activos propiedad del centro.

3. La protección física de los equipos corresponde, en un principio, a los trabajadores del centro, en este caso a los administradores de red.

2.4.3 Mantenimiento de equipo de cómputo

1. Al departamento de Administración de Redes le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a como tenga lugar.

2. En el caso de que haya que atender algún equipo por parte del personal especializado ajeno al centro, la Dirección de Redes deberá normar al respecto y generar los informes correspondientes.

3. El mantenimiento a los equipos, así como los posibles cambios y actualizaciones en software(s) deberán ser registrados en informes correspondientes.

2.4.4 Reubicación del equipo de cómputo

1. La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que el departamento de Administración Redes emita para ello.

2. En caso de efectuarse alguna modificación en la ubicación de los equipos de cómputo por parte del personal especializado ajeno al centro, se deberá trabajar en coordinación con los administradores de red y deberá quedar la tarea reflejada en informes, todo esto con la debida autorización.

2.4.5 Control de accesos

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta el departamento de Administración de Redes.
2. El control de acceso al área de administración se hará de forma permanente, permitiendo, en caso excepcional, el acceso de personal ajeno con la debida autorización.

3. Al área de servidores solo podrá entrar la dirección del centro y personal especializado externo con la debida autorización, en todo caso se registrará en un informe.

4. El acceso al área de servidores tendrá solo un representante que será el encargado directo de controlar el acceso y los cambios al local.

5. Bajo condiciones de emergencia o de situaciones de urgencia extrema, el acceso a las diferentes áreas estará sujeto a las normas que especifiquen las autoridades superiores a la institución.

6. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

2.4.6 Control de acceso local a la red

1. El departamento de Administración de Redes es el responsable de que todo usuario que haga uso de algún servicio esté registrado con cierto nivel de privilegios.

2. Dado la gran cantidad de usuarios que podrán hacer uso de los servicios del centro, el departamento de Administración y Redes verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.

3. El acceso lógico a equipos especializados de cómputo (servidores, enrutadores, bases de datos, Switch, etc.) conectados a la red es administrado por el departamento de Administración de Redes.

2.4.7 Control de acceso remoto

1. El departamento de Administración de Redes es el responsable de proporcionar el acceso de los usuarios a los diferentes servicios disponibles.

2. Ningún tercero podrá hacer uso de los equipos de cómputo desde la red externa, esto le es permitido solo a los administradores desde dentro del centro y con el debido control.

3. El acceso remoto que realicen los usuarios deberá cumplir las normas que emite el departamento de Administración de Redes.

4. Los usuarios son responsables del uso de su acceso autorizado.

5. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista, ni al alcance de terceros.

6. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

7. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y contactar con los administradores del centro para notificar la incidencia.

2.4.8 Acceso a los sistemas administrativos

1. Tendrá acceso a los sistemas administrativos sólo el personal del centro perteneciente al departamento de Administración de Redes.

2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

3. La instalación de nuevas aplicaciones y sistemas de información se rigen por las normas y procedimientos establecidos por el departamento de Administración de Redes.

2.4.9 Sanciones

1. Cualquier violación de las políticas y normas de seguridad deberá ser sancionada de acuerdo al

reglamento emitido por el departamento de Administración de Redes.

2. Las sanciones pueden ser desde una llamada de atención o informar al usuario, hasta la suspensión del servicio, dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

3. Corresponderá al departamento de Administración de Redes hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.

4. Todas las acciones en las que se comprometa la seguridad del Centro y que no estén previstas en esta política, deberán ser revisadas por el departamento de Administración de Redes para dictar una resolución sujetándose al estado de derecho." [24]

2.5 Medidas y procedimientos de seguridad informática

2.5.1 Seguridad física

2.5.1.1 Protección de áreas con tecnologías instaladas

El centro de datos deberá estar dividido en dos áreas que se protegerán mediante este plan de seguridad. Se recordarán que éstas son:

1. El área de servidores: estarán ubicados todos los servidores, fundamentalmente los de base de datos que almacenarán la información geológica.

2. El área de administración: estarán ubicados el switch capa dos y los ordenadores que se encargarán de monitorear los servicios, el ancho de banda, etc.

2.5.1.1.1 Ubicación

La ONRM no ha definido donde estará ubicado geográficamente el Centro de Datos. Para la elección del lugar donde se construirá se deberán tener en cuenta medidas como:

1. Su ubicación deberá estar lejos de lugares como: almacenes de materiales inflamables, plantas eléctricas, gasolineras, etc.

2. La ubicación se deberá encontrar en lugares altos para evitar que el local se pueda inundar.

2.5.1.1.2 Barreras Físicas

1. El local donde se vayan a instalar los activos informáticos deberá ser capaz de mantenerse seguro ante adversidades.

   - La construcción deberá ser sólida, preferentemente de mampostería, resistente a ráfagas de vientos huracanados.

   - Todos los materiales usados en la construcción deberán ser incombustibles.

   - Las paredes deberán ser resistentes al fuego.

   - Para evitar los problemas de filtraciones la azotea deberá estar protegida por tela asfáltica (asfaltex).

2. Las ventanas y las puertas que dan entrada o salida al centro deberán estar protegidas por rejas y métodos que impidan la visión hacia dentro.

   - Las rejas deberán ser del tamaño de las ventanas y puertas, además de tener un candado que se le pondrá cuando termine la jornada laboral, siendo responsable el administrador del sistema o una persona designada por él.

   - Para evitar la visión hacia dentro, las ventanas o rendijas deberán estar cubiertas por cortinas.

   - Esta medida se aplicará al área de servidores colocando un candado electrónico en la puerta, con el fin de permitir el acceso solo a personas autorizadas por el administrador del sistema.

3. En caso de que la empresa quiera expandirse, el espacio físico del local deberá permitir la instalación o reinstalación de nuevos hardwares, así como la conservación de recursos redundantes.

4. Deberá existir un sistema detector de incendio y humo con alarma sonora, que pueda ser activado

tanto manual como automáticamente, además de extintores de incendio en cada área del local.

- Los extintores manuales contra el fuego deben ser de dióxido de carbono u otros gases con agentes de extinción.

- No deben existir extintores, que dentro, la química sea polvo seco en el área de ordenadores o servidores.

- Se deberá disponer de suficientes extintores de incendios portables en cada área y deberán ser probados periódicamente a fin de que puedan funcionar correctamente en casos de emergencias.

- Los sistemas detectores de incendio o humo, deberán estar ubicados en el techo, en caso de que se detecte cualquier incidente, activarán automáticamente la alarma sonora que avisará a los trabajadores.

5. Cada local deberá tener un sistema de aire acondicionado que garantice una buena climatización en las diferentes áreas. Se recomienda que en el Centro de Datos la temperatura deberá estar entre 18 y 25 grados centígrados y la humedad relativa del aire entre 30% y 45%.[25]

6. Teniendo en cuenta que los equipos de aire acondicionado son causa potencial de incendios e inundaciones se les deberá instalar cerca, mecanismos de protección como: detectores y extintores de incendio, cámaras de seguridad y alarmas sonoras para casos de incidente.

2.5.1.1.3 Sistema de Control de Acceso

1. El acceso a cualquier área y tecnología que se encuentre en el Centro de Datos sólo debe efectuarse por las personas autorizadas según el área que les corresponda.

2. Para disminuir los riesgos de actividades ilícitas se deberá restringir el acceso físico a las áreas.

- El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores del centro.

- Cada trabajador deberá tener una credencial con los datos siguientes: nombre (s), apellidos, foto del individuo, cargo que ocupa y el nivel de acceso que denotará las áreas a las que puede acceder.

3. En caso de que un trabajador necesite acceder a un área que se encuentre fuera de su rango de autorización deberá solicitar un permiso.

   - El permiso será otorgado por el máximo responsable del área.

   - El responsable del área u otro trabajador designado por él deberá supervisar al trabajador mientras se encuentre interactuando dentro de su dominio.

   - De igual manera sucederá en caso de no ser la persona un trabajador del centro y necesite acceder a cualquier área.

4. La guardia de seguridad se ubicará en lugares estratégicos fuera del local. Tienen como objetivo fundamental el control de la entrada de todas las personas que accederán al Centro de Datos.

   - A cualquier personal ajeno que llegue al centro se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc.

   - En caso que algún trabajador esté autorizado por la dirección a quedarse en el centro fuera de horario, la guardia de seguridad deberá tener la relación con los datos de dicho trabajador y se deberá reportar la hora de egreso del mismo.

2.5.1.1.4 Medios Técnicos de Detección de Intrusos

1. Deberá existir un sistema detector de intrusos que active automáticamente la alarma sonora cuando el Centro de Datos esté cerrado y cualquier persona intente acceder al local.

   - El sistema deberá utilizar sensores de movimientos o sensores de puertas y ventanas como componentes para la detección de intrusos.

- La alarma sonora no deberá estar por debajo de los 95 decibelios.

- El máximo responsable del Centro de Datos deberá ser el encargado de cerrar el local y de activar la alarma cuando se termine el horario laboral. En caso de cualquier incidente debe estar localizable.

- El máximo responsable deberá desactivar la alarma y abrir el centro para que se inicie la jornada laboral. Se deberá revisar que todo funciona correctamente y que no falta nada antes de comenzar a trabajar.

2. Dentro del sistema de monitoreo deberá existir un circuito cerrado de televisión que permita el control de las personas que ingresan a cada una de las áreas del centro y que permita además la detección de posibles incendios u otros incidentes.

   - Existirá un trabajador que será el encargado de la monitorización durante el horario laboral.

   - Se instalarán cámaras de seguridad que serán ubicadas estratégicamente en las distintas áreas. Principalmente se enfocarán cada uno de los activos dentro del área de servidores para prevenir o detectar algún incidente.

   - Las cámaras deberán estar ocultas para evitar que un posible infractor se de cuenta de que está siendo observado.

   - Los archivos de monitoreo deberán ser almacenados durante dos días, si no se ha detectado ningún incidente podrán ser eliminados.

   - En caso que se detecte algún incidente como robo, fraude, sabotaje, etc., se utilizarán como evidencia los archivos grabados del monitoreo.

   - Se enfocarán los puntos que puedan ocasionar un posible corto-circuito, en caso de detectar alguna anomalía dentro del área de servidores, el trabajador deberá avisar al responsable del área y al personal entrenado en la utilización de extintores para evitar algún incendio o humo

que provoquen daños a la instalación, como primera acción se apagará manualmente todo el sistema eléctrico.

2.5.1.2 Protección Física de los Equipos

2.5.1.2.1 Ubicación

1. Durante la caracterización del sistema o en el **análisis de riesgos** realizado al principio del **Capítulo 2,** en la **Tabla 1,** se identificaron cada uno de los activos informáticos, además de la propuesta sobre el lugar en donde deberán estar ubicados

2.5.1.2.2 Dispositivos de Protección Física a Aplicar

Por el análisis realizado al plan de seguridad del MINED en el **Capítulo 1,** se determinó que se tomaría como guía de trabajo, por las políticas, medidas y normas de seguridad que ofrece. Una auditoría que se llevó a cabo les permitió conocer las deficiencias en el sistema informático que había hasta el momento, lo cual dio paso a que fueran reflejadas en el plan de seguridad, además de poner las medidas y normas para corregirlas. Basado en las deficiencias que detectaron en su sistema informático, se determinó evitarlas en el futuro Centro de Datos, aportando medidas fundamentadas en el plan del MINED que contribuyan a la protección física de los activos informáticos que existirán en el centro. Seguidamente se muestra el resultado del estudio realizado más otras medidas propias de esta investigación:

1. Cada ordenador y servidor deberá disponer de una UPS (Uninterruptable Power Supply) o SAI (Sistema de Alimentación Ininterrumpida) como fuente de respaldo de energía además de un generador central que asumirá la función en caso de fallas eléctricas.

2. El generador central deberá ser capaz de activarse tanto manual como automáticamente en caso de fallas eléctricas. Se deberá controlar siempre la cantidad de combustible que le queda para evitar que su función se acorte mientras se estabiliza la electricidad.

3. Las UPS deberán garantizar el tiempo suficiente las funciones de respaldo en servidores y ordenadores hasta que el generador central asuma esta función.

4. Las UPS se deberán configurar para que realicen la señal de aviso con al menos dos minutos de antelación en caso de que el generador no se haya activado.
   - En caso que el sistema operativo sea Windows:
     -Los administradores configurarán el servicio de UPS. Dentro del Panel de Control seleccionarán el icono Opciones de energía. Seguidamente oprimirán la paleta SAI (UPS) donde aparecerá la opción de habilitarla.

5. Tanto el generador central como las UPS deberán ser probados regularmente. Se recomienda que sea al menos cada seis meses.

   - Se avisará con días de antelación y se tomarán las medidas pertinentes para asegurar que ésta prueba no ocasione pérdidas en los servicios que brinda el Centro de Datos en caso de que falle el generador.

   - Esta operación deberá ser realizada por un especialista autorizado y supervisado por la máxima dirección del sistema y de la entidad a la cual pertenece el centro, asegurándose en todo momento no poner en riesgos los equipos informáticos.

6. El cableado de la red deberá estar protegido de interferencias, para ello se harán canaletas en las paredes que los cubrirán.

   - Dentro de la canaleta del cable de red no deberá estar ninguna instalación de cableado eléctrico.

   - El cableado se encontrará dentro de cañerías metálicas que sirven de barreras contra las interferencias.

2.5.1.2.3 Control de Acceso a las tecnologías informáticas

1. Cada trabajador será responsable de los medios informáticos con los que interactúa diariamente.

2. Si el trabajador necesita acceder a un equipo dentro del área de servidores deberá comunicárselo a su superior o al responsable del área (puede ser una misma persona o personas distintas) el cual

gestionará el acceso a la máquina.

3. En caso de la persona no ser trabajador del Centro de Datos deberá realizar una solicitud y exponer el motivo al jefe de la entidad a la cual pertenece el Centro de Datos (ONRM) además de la aprobación por parte del responsable del área en la cual estará ubicado el equipo informático del que desea hacer uso. Siempre deberá ser supervisado por un trabajador del centro perteneciente al área.

4. En cualquiera de los casos se deberá documentar en un **registro de acceso** que deberá tener cada área y que será supervisado por el administrador del sistema o máximo responsable del Centro de Datos. Este registro contendrá los siguientes campos:
    - Si es trabajador o no del Centro de Datos.
    - Área a la que desea acceder (En el caso del trabajador interno **área 1**; el trabajador externo en cualquiera de las dos áreas).
    - Fecha (Hora de entrada y salida, Día, Mes, Año).
    - Nombre y firma de quién lo autoriza.
    - Los datos personales.
    - Motivos de acceso a las tecnologías.
    - Observación.

5. En caso de que alguna tecnología no se esté usando, deberá guardarse en un lugar seguro bajo llave en el Centro de Datos y la responsabilidad será del administrador del sistema.

6. Independientemente de que el área de servidores estará protegida mediante puertas aseguradas con candados electrónicos u otros métodos de seguridad que restrinjan el acceso a personas no autorizas, cada servidor, Switch u otro dispositivo que allí se encuentre, también deberá estar protegido bajo llave.

7. El trabajador que permita el acceso a las tecnologías informáticas a personas que no trabajen en el Centro de Datos asumirá la total responsabilidad en caso de que ocurriese algún incidente, pudiendo ser sancionado por las siguientes regulaciones internas de la Entidad, con independencia de la responsabilidad penal que proceda según el alcance de la violación detectada:

    - Reglamento Interno.

- Convenio del Colectivo de Trabajo.
- Resoluciones.

2.5.1.3 Soportes de información

2.5.1.3.1 Identificación

1. El máximo responsable del área de servidores será quien realice (aunque puede ser un trabajador autorizado o designado por él) la salva de la información en los soportes correspondientes, además de contar con la autorización para poder acceder a ellos.

2. Según la experiencia del plan de seguridad del MINED y para mayor organización del proceso de salvas de información, es necesaria la existencia de un **registro de control de soporte** que contenga:

   - Datos personales de quien realiza la acción (Nombre, Apellidos, Firma...).
   - No. del Activo Informático (Equipo donde se extrajo la información).
   - No. Consecutivo (Número de la salva).
   - No. del dispositivo de soporte.
   - Contenido fundamental del soporte.
   - Trabajo para el que se destina el soporte.
   - Nivel de acceso del soporte.
   - Fecha y hora de entrada.
   - Fecha y hora de baja.
   - Nivel de clasificación.
   - Periodicidad y ciclo de retención.
   - Observaciones.

3. Los soportes deberán tener visibles en una etiqueta los datos necesarios que ayuden a su identificación para el momento en que se vayan a utilizar.

2.5.1.3.2 Conservación

1. El local donde se guardarán los dispositivos de soporte deberá estar fuera del Centro de Datos y será designado por la administración de la ONRM o por el administrador del sistema.

2. Deberán estar en lugares que cumplan con las condiciones climáticas para que se conserven y no se pierdan los datos contenidos en él. El acceso a ellos deberá ser restringido, por lo que deberán encontrarse bajo llave y cuidado de un responsable.
3. Se deberán realizar copias de más de un ejemplar en caso de que ocurra algún imprevisto como: el deterioro o la destrucción negligente de un soporte con información sensible.

4. Una copia se guardará dentro del centro (bajo de llave) y la otra en el local de almacenamiento.

5. Si el responsable del área de servidores desea acceder a un soporte, deberá informarle al responsable del local de almacenamiento el No. de soporte contenido en el **registro de control de soporte.** El almacenero localizará el dispositivo mediante otro registro, que es el **registro de entrega/recepción de soportes de información** y que contendrá los siguientes campos:

   Entrega:
   - No. del dispositivo de soporte.
   - Contenido fundamental.
   - Nombre y firma de quién lo entrega.
   - Nombre y firma de quién lo recibe.
   - Fecha y hora de entrega.
   - Objetivo de utilización del soporte.

   Recepción:
   - Nombre y firma de quien devuelve el soporte.
   - Nombre y firma de quien recibe el soporte.
   - Resultado de la comprobación del dispositivo.
   - Resultado de la revisión contra virus.
   - Fecha y hora de recepción.
   - Observaciones.

6. En caso de que sea un trabajador, este deberá llevar la autorización del responsable del área de servidores, de no ser así, queda prohibido terminantemente el acceso a los dispositivos de soporte, siendo el máximo responsable de cualquier incidente que ocurra quien se encuentre administrando o

custodiando el local.

2.5.1.3.3 Destrucción

1. Es necesario que cuando el soporte de información cumpla con su finalidad, se termine el ciclo de retención, contenga sectores malos o deteriorados y luego de que la información contenida sea salvada en otro dispositivo, sea eliminado por medio del borrado físico o la destrucción física del soporte de almacenamiento.

   - Una vez borrado o eliminado el soporte, se actualizará el **registro de control de soporte**, eliminándolo de la lista y especificando en la Observación el por qué, el tipo de acción o método que se utilizó y quién la ejecutó.

2. Existen métodos para que la información contenida en el dispositivo de almacenamiento no sea recuperada por personas mal intencionadas, ejemplos de ellos son los siguientes:

   - Si son soportes no regrabables, como DVD o CD no regrabables: el procedimiento de seguridad es relativamente sencillo, por ejemplo cortándolos en fragmentos, quemándolos, etc.

   - Si se trata de soportes regrabables, como son también DVD, CD o disquetes: el procedimiento a seguir no solo pasa por el borrado de la información que contienen, sino además la destrucción del soporte físico (en el caso de disquetes extrayendo previamente el disco interno de la carcasa) y la de los demás se mencionaron en el punto anterior.

   - Si son soportes como discos duros, tanto internos como externos, o de unidades externas de memoria: el método de destrucción del soporte se complica, tanto en ejecución, como en coste. La destrucción de estos dispositivos es posible mediante uno de los métodos más utilizados que incluye el borrado definitivo por magnetización del dispositivo y su posterior destrucción física.

2.5.1.3.4 Traslado

1. Una vez efectuada la transacción de información hacia el soporte y se proceda al traslado hasta el local de almacenamiento, se deberán realizar las siguiente acciones que ayudarán en el control de los

dispositivos:

- Serán anotados los datos en el **registro de control de soporte** por el responsable del área.

- Una vez en el almacén, se actualizarán los datos en el **registro de entrega/recepción de soportes de información** por parte de la persona que está al frente del local de almacenamiento. Incluye la revisión y comprobación del estado del dispositivo.

2. En dependencia de lo lejos que se encuentre el local de almacenamiento de dispositivos de información del Centro de Datos, se deberán tomar las medidas necesarias para que no se dañe el soporte.

   - Para el traslado del soporte de información, se deberá guardar dentro de un estuche o caja que lo proteja de elementos que puedan afectarlo como: el polvo y el agua.

   - Durante el traslado, se deberá evitar la exposición de los dispositivos de soportes a medios que generen campos magnéticos.

   - Se evitará poner los dispositivos debajo de cualquier objeto pesado que pueda ocasionarle la ruptura.

   - El trabajador que realice el traslado e incumpla, será el máximo responsable de lo que ocurra.

2.5.2 Seguridad Lógica

2.5.2.1 Identificación y autenticación de Usuarios

El centro cuenta con dos categorías de usuarios fundamentalmente. Cada grupo internamente tiene una jerarquía de privilegios que son los que les permiten realizar una u otra tarea. Están los administradores de red y los usuarios externos.

2.5.2.1.1 Identificación y Autentificación de Usuarios

La identificación y autenticación se hará básicamente de dos formas diferentes, una para los

administradores internos y otra para los usuarios externos o remotos.

2.5.2.1.1A Usuarios internos

1. Todas las máquinas internas dedicadas a la administración del centro deberán poseer una contraseña de SETUP que será activada cada vez que es reiniciada la máquina. Además del SETUP, cada puesto de trabajo estará protegido por una clave local y otra del dominio para hacer uso de los servicios.

2. Para hacer uso de los servicios de administración, se deberá, obligatoriamente, ser usuario del dominio interno del centro. Las contraseñas registradas en el dominio interno deberán tener las siguientes características:

   - Tendrán un período de vigencia con cotas mínimas de tres días, durante este período no se puede actualizar la contraseña después de haber efectuado un cambio, y máximas de cuarenta y cinco días donde una vez arribado a este tiempo el sistema pide que se renueve el password o congela la cuenta hasta que es activada nuevamente por el administrador principal.

   - Las contraseñas deben poseer un mínimo de 8 caracteres de longitud, formados por elementos alfanuméricos, de ellos al menos dos deben ser caracteres especiales.

   - Las contraseñas no deben ser palabras del diccionario ni guardar relación con datos personales o laborales.

3. El sistema deberá inhabilitar temporalmente la cuenta después de tres intentos fallidos por parte del usuario.

4. La contraseña no se debe repetir en ninguno de los cambios a las establecidas anteriormente.

5. El sistema deberá tener implementado una aplicación capaz de calcular la complejidad de las contraseñas para ser usado cada vez que se vaya a crear un usuario o éste actualice su contraseña. En caso de que una contraseña no cumpla con el nivel de complejidad requerido se informará al usuario para que repita el intento.

6. La autenticación de los usuarios internos (los administradores), se realizará en el servidor Proxy, donde se tendrán en cuenta las normas para el establecimiento de cuentas implementado en el presente plan de seguridad informática.

7. Cuando el usuario permanece en la máquina de trabajo más de veinte minutos sin realizar modificaciones, automáticamente ésta se bloquea con un refrescador de pantalla siendo necesario el uso de la cuenta de domino para desbloquearla.

2.5.2.1.1B Usuarios externos

Para el caso de los usuarios externos que se conectarán vía remoto, este plan dicta un conjunto de normas y medidas que garantizan la máxima seguridad en cuanto a autenticación, pero no comprende las políticas y normas por las cuales debe regirse este usuario en la entidad a que pertenece.

1. Para entrar a la página principal o portal que hospeda el centro, no es necesario estar registrado, en este caso la conexión será como invitado y sólo se podrá navegar por páginas que brindan información general. Para hacer uso de los servicios de búsquedas, gestión y otros, es obligatorio estar registrado con cierto nivel de privilegio que permita el acceso a los recursos que se desean.

2. Los niveles de privilegios son otorgados por la empresa que hospeda el sitio. Van a existir usuarios con privilegios para hacer consulta y búsqueda de información y usuarios que podrán realizar modificaciones e incorporar nueva información, llamados súper-usuarios.

3. Los súper-usuarios podrán ser registrados por el departamento de Administración de Redes o por otros súper-usuarios donde éste ultimo es el responsable de la acción que realiza.

4. Una vez que se crea un nuevo usuario, éste deberá tener una contraseña inicial, la cual será cambiada obligatoriamente por el propietario de la cuenta al usarla por primera vez, para confirmar y habilitar la cuenta.

5. Para loguear a los usuarios les deberá aparecer en pantalla los siguientes datos:
    - Nombre de usuario.

- Password.
- Opción para cambiar el password.

6. Mientras el usuario está ingresando su contraseña, ésta no debe ser mostrada por pantalla.
7. Una vez logueado el usuario, el sistema deberá mostrar los siguientes datos a modo de información:
    - Nombre de usuario.
    - Fecha y hora de la última conexión.
    - Localización de la última conexión (Ej. la IP de Terminal).
    - Cantidad de intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

Password:

1. Los password deberán tener una longitud mínima de siete caracteres conformados por elementos alfanuméricos, caracteres especiales y letras mayúsculas o minúsculas.

2. El password deberá inicializarse como expirado para obligar el cambio al iniciar nuevamente la sesión.

3. La fecha de expiración del password deberá ser de tres meses. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo.

4. El password no deberá contener el nombre de la empresa, el nombre del usuario, ni palabras reservadas.

5. Una vez que el usuario haya realizado cinco intentos fallidos de forma consecutiva para acceder al sistema se deberá bloquear el perfil.

6. El usuario debe poder modificar su password cuantas veces considere necesario, sin seguir ningún procedimiento formal de aviso.

7. El password ingresado no debe repetirse a los veinte password usados anteriormente.

8. El password deberá tener un período de duración mínimo de 5 días. El sistema no permitirá el cambio de password si este período no se ha cumplido.

9. En caso de que un usuario pierda el password, éste no se le mostrará a ningún administrador, el sistema deberá mandar un nuevo password vía mail una vez que el usuario lo solicite. El password enviado deberá ser cambiado una vez que se entre al sistema con él; el sistema obliga al cambio.

2.5.2.2 Control de Acceso a los Activos y Recursos

Son dos los tipos de usuarios que interactuarán con el Centro de Datos, cada uno con diferentes niveles de accesos, incluso dentro de un grupo existen niveles de privilegios que hacen que el acceso sea diferenciado también. Estos grupos, como se había dicho anteriormente, son los internos (administradores de red) y los externos: usuarios que se conectarán vía remoto para usar los servicios que se prestan. Para un mejor análisis se presentará por separado el control de éstos tipos de usuarios. También algunos activos acceden a otros activos y recursos comportándose como intermediarios entre usuarios e información final que se brinda. De éstos activos, la interrelación y flujo de datos entre ellos, es otro de los temas que abarca el control de acceso a los activos y recursos presentado en este documento.

2.5.2.2.1 Usuarios externos

1. Los usuarios externos tendrán asociado, como dato de importancia, el nivel de privilegio que indica a que recursos puede o no acceder. Una vez autenticados podrán hacer uso de los servicios que el privilegio les permita.

2. Los usuarios externos interactuarán directamente con el servidor Web, donde, como primer paso para hacer uso de los servicios, se autenticarán con su identificador y contraseña.

3. Una vez autenticados podrán hacer uso de los servicios, ya sea realizando búsquedas, modificando información o creando nuevos usuarios según el privilegio lo permita.

4. Todo el flujo de información entre la red externa y la interna será registrado por el Firewall por hardware, es en este dispositivo donde se registrarán las trazas (Log(s)) que dejen las acciones que realice cada usuario externo para luego ser almacenadas y analizadas:

    - Destinatarios de mensajes.
    - Remitentes de mensajes.

- Total de menajes enviados.
- Total de mensajes recibidos.
- Nombre del usuario
- Hora de conexión
- Tráfico total de entrada y de salida.
- Hora de desconexión.

5. Otro activo donde se guardará información referente al acceso de los usuarios es en el servidor de Directorios. Los datos se guardarán en este servidor al inicio y al cierre de la conexión. Estos datos se toman del programa que administra los Log(s) almacenados y son guardados hasta que el usuario accede al sistema otra vez:

   - Fecha, hora y lugar de la conexión (dirección IP o teléfono de conexión).
   - Fecha y hora de desconexión, cantidad de bytes enviados y recibidos.
   - Tráfico total de entrada y de salida.
   - Cantidad de intentos fallidos de conexión.

6. Los usuarios externos también podrán intercambiar archivos en el servidor FTP, pero esto será para casos especiales, estrictamente controlado y autorizado por la dirección del departamento de Administración de Redes.

2.5.2.2.2 Usuarios internos

1. Los usuarios internos se comportarán como externos una vez intenten conectarse desde fuera del centro, en este caso el comportamiento y acceso a los recursos estará regido por las normas y procedimientos que se dictan para ese grupo de usuarios.

2. Para acceder a las PCs de administración lo harán como está establecido en las normas referidas a la autenticación y el acceso se hará directamente en la máquina, nunca vía remoto.

Acceso a internet:

1. Los usuarios internos podrán hacer uso de la Internet solo con fines de trabajo.

2. No estará permitido el acceso a los sitios que ofertan cuentas de correo gratuitos tanto dentro como fuera del país.

3. No estará permitido el acceso a sitios con información que perjudique la imagen de la Revolución Cubana.

4. No estará permitido el acceso a sitios con información que vaya en contra de las normas elementales de conducta social y moral.

5. Todo el acceso a Internet quedará registrado en el servidor Proxy.

Acceso a los recursos:

1. Los administradores de red podrán acceder a todos los recursos instalados en el centro, con cierta diferencia entre los servidores de comunicación y servidores de Bases de Datos.

2. Los administradores de red podrán acceder a los servidores de comunicación (servidor Proxy, servidor FTP, servidor DNS, servidor de Directorios de Usuarios, servidor de Aplicaciones y servidor de correo), con el fin de configurar los servicios que estos activos prestan y poder actualizar las aplicaciones que aquí corren, así como mantener un control total de la seguridad.

3. Para realizar actualizaciones en los servidores de comunicación, se deberá contar con la autorización de la máxima dirección del departamento de Administración de Redes y en todos los casos deberá quedar constancia de los cambios realizados.

4. Para acceder a los servidores de Bases de Datos será obligatorio contar con la autorización de la máxima dirección del departamento de Administración de Redes, quien deberá dejar constancia de la operación que se realice.

5. En los servidores de Bases de Datos no se deberá hacer cambios por parte de los administradores, que afecten o modifiquen la actual prestación de servicios, como podría ser la eliminación, adición o actualización de alguna tabla física del sistema de bases de datos; esta operación la podrá realizar la empresa involucrada con los datos que se modifican en coordinación con la dirección del centro, dejando constancia en todos los casos de la operación realizada.

6. Los administradores de red podrán acceder al Router, al Firewall por hardware y a los Switch para configurar las políticas de seguridad acorde con las normas establecidas para la configuración de estos activos.

2.5.2.2.2A Flujo de información entre activos informáticos

No solo los usuarios externos e internos acceden a los recursos y servicios, también lo hacen los propios activos. Analizando sin mucha profundidad, se puede ver como un usuario externo realiza una consulta de búsqueda donde los datos que recibirá saldrán del servidor de Bases de Datos, sin embargo, en ningún momento accede directamente a éste, ya que el proceso lo hacen otros servidores que actúan de mediadores. Aquí se refleja como un activo accede a otro realizando alguna petición. El ejemplo que se muestra no es un proceso para hacer más difícil la comunicación, el objetivo está enfocado a la seguridad e independencia de los recursos. Seguidamente se muestran un conjunto de normas y procedimientos que rigen el comportamiento entre los activos, estableciendo las conexiones que reciben cada uno.

1. Los usuarios externos siempre que traten de consultar información almacenada en el centro lo harán a través del servidor Web.

2. En el servidor Web el usuario se autentica y se le habilita el privilegio que se le haya otorgado al crearse su perfil.

3. El servidor Web podrá aceptar peticiones de cualquier procedencia a menos que alguna dirección haya sido bloqueada. Desde de la red interna acepta también conexiones de las máquinas de administración, cualquier otro intento de conexión desde la red interna será rechazado.

4. Para efectuar el proceso de autenticación, el servidor Web deberá conectarse con el servidor de Directorio de Usuarios para comprobar los datos del perfil que intenta identificarse.

5. El servidor de Directorio de Usuarios solo recibirá peticiones del servidor Web y de las máquinas de administración, cualquier otro intento de conexión será rechazado.

6. Toda conexión que provenga de la red exterior podrá acceder solamente a los servidores: SMTP

(correo), FTP o Web.

7. Una vez que el usuario selecciona los parámetros de entrada para realizar una consulta y la manda a ejecutar, automáticamente son enviados al servidor de Aplicaciones donde se conforma la consulta. Éste proceso es transparente para el usuario ya que lo próximo que se observa en pantalla son los resultados.
8. La conexión entre servidores se realizan mediante los protocolos TCP e IP.

9. El servidor de aplicaciones sólo aceptará conexiones procedentes del servidor Web y de las máquinas de administración, cualquier otro intento de conexión será rechazado.

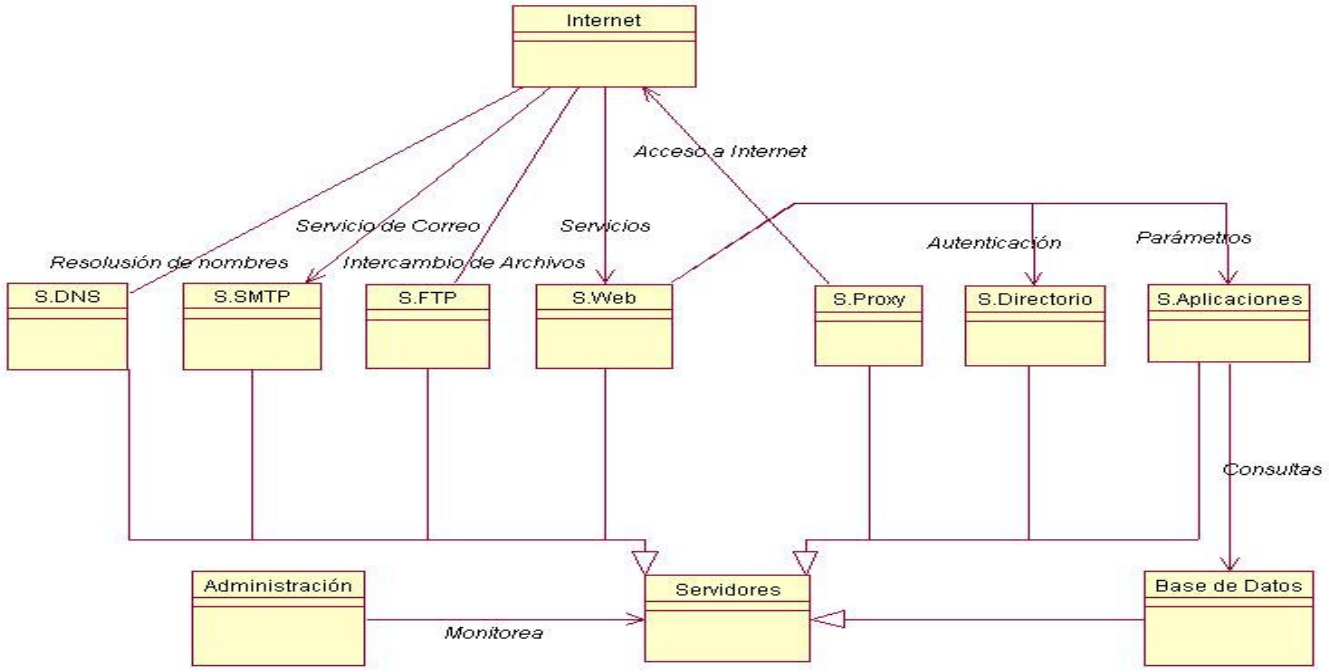
10. Una vez conformada la consulta, es enviada a los servidores de Bases de Datos para ser ejecutada finalmente.

11. Los servidores de Bases de Datos sólo aceptarán conexiones provenientes del servidor de Aplicaciones y de las máquinas de administración, cualquier otro intento de conexión será rechazado.

12. Al ejecutarse la consulta en los servidores de Bases de Datos, es enviado el resultado al servidor de Aplicaciones, el cual configura la respuesta para ser enviada al servidor Web y finalmente ser mostrada al usuario siguiendo el proceso inverso a la ejecución.

    A continuación se muestra gráficamente como quedaría el flujo de la información en el Centro de Datos, donde se refleja el acceso de los usuarios a los activos y de los activos a otros activos.

Diagrama del Flujo de Información entre activos:



2.5.2.3 Integridad de los Ficheros y Datos

Hasta el momento, en cuanto a seguridad lógica, se ha tratado sobre los activos tangibles del centro, específicamente los equipos de cómputo que componen la red. También se ha hablado de los diferentes grupos de usuarios y la interacción de ellos con el sistema. Cuando se trata de lograr en un centro cualquiera, que los recursos y servicios permanezcan íntegros, disponibles y confiables, es de vital importancia la máxima seguridad sobre la célula base de la información formada por los ficheros y datos. A continuación se muestra un conjunto de normas y procedimientos relacionados con el tema, que abarcan desde la configuración segura de la red hasta el uso de Firewall, entre otros aspectos.

1. Las direcciones asignadas en la red interna del centro no serán visible desde la red exterior.

2. Todos los servidores de comunicación e Internet (Proxy, SMTP (correo), FTP, DNS y Web), más el servidor de Directorio de Usuarios y el servidor de Aplicaciones, estarán ubicados bajo la configuración de un zona desmilitarizada (DMZ). Éste tipo de configuración se hace con el objetivo de que si en algún momento la seguridad del Firewall principal por hardware, se ve comprometida por ataques de

terceros, esta porción de la red no sea visible a los atacantes desde el Firewall y así garantizar mayor seguridad.

3. Desde la DMZ los únicos servidores que aceptan peticiones del exterior son:

   - Servidor SMTP (correo): presta servicio de mensajería a usuarios externos e internos.

   - Servidor Web: mediante este servidor los usuarios externos hacen uso de los servicios de consulta y modificación de la información almacenada en el centro.

   - Servidor DNS: este servidor intercambia información con otros servidores DNS en el proceso de resolución de nombres.

   - Servidor FTP: usuarios con autorizaciones especiales podrán intercambiar archivos de gran tamaño mediante este servidor.

El diagrama de red ya fue explicado en el proceso de caracterización del centro en el **Capítulo 1**. También se analizó como cada activo accede y permite el acceso a otros activos en el presente capítulo. Seguidamente se muestran normas y procedimientos relacionados con la red que tratan el tema de las restricciones con más profundidad.

2.5.2.3.1 Firewall por hardware

1. El Firewall estará conectado seguido del Router WAN y será un firewall por hardware dado las ventajas que este dispositivo ofrece con respecto a un firewall por software.

2. Con el fin de disminuir la posibilidad de Spoofing, el Firewall deberá denegar el acceso a cualquier intento de conexión desde la red externa que posea una dirección fuente que esté asignada a un host de la red interna.

3. El Firewall tendrá habilitado solo dos zonas de seguridad para establecer las conexiones internas del centro. Estas zonas tendrán configuraciones diferentes y específicas para el uso que se les va a dar.

   - Primera zona: en esta zona estará configurada la DMZ y tendrá conectado a él un Switch

capa tres con los servidores de comunicación (Proxy, SMTP (correo), FTP, DNS y Web) más el servidor de Directorio de Usuarios y el servidor de Aplicaciones.

- Segunda zona: en esta zona estará conectado un Switch Core capa tres con el resto de la red conectada a él.

4. El Firewall debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios.

5. Por la primera zona, donde estará configurada la DMZ, solo circularán peticiones hacia los servidores que prestan los servicios establecidos en el Centro de Datos.

6. La primera zona deberá permitir el acceso desde la red interna de las direcciones IP de las máquinas de administración, cualquier otro intento de conexión desde la red interna será rechazado.

7. La segunda zona no permitirá ninguna conexión que provenga desde la red externa.

8. La segunda zona solo permitirá conexión desde el servidor de Aplicaciones cuando éste acceda a los servidores de Base de Datos para ejecutar consultas.

9. Para lograr las políticas descritas en el Firewall, se configurarán rangos de direcciones IP con accesos a las diferentes zonas en las IP-Tables, así como los puertos descritos en la sesión de **Ataques de red**.

10. Cuando una dirección host externa envíe múltiples intentos de conexión (segmentos SYN) al centro y no confirme la conexión, será bloqueada con el fin de evitar un intento de ataque Flooding.

11. El encargado del mantenimiento de la red debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados obtenidos.

2.5.2.3.2 Protección Contra Programas Dañinos

1. Cada equipo de cómputo contará con un producto antivirus previamente certificado por la dirección del departamento de Administración de Redes. Este producto podrá ser de producción nacional o

importado, en ambos casos debidamente autorizados y con posibilidades de actualización frecuente.

2. Deberán programarse escaneos periódicos con vista a encontrar archivos infectados por virus en todos los equipos del centro; esta tarea estará a cargo del personal designado por el administrador de redes y se efectuará en horarios donde el tráfico de la red sea el menor posible, fuera del horario pico de intercambio de información.

3. La dirección del departamento de Administración de Red será responsable de someter a un proceso de cuarentena todo software, sistemas y programas de aplicaciones adquiridos a través de Internet o a través de terceros. Este proceso se realizará en la subred, donde se encuentran las máquinas de administración, en una PC que no esté comprometida con la información que protege el centro y que todo su sistema esté descontaminado y bajo control.

4. El servidor de correo será escaneado diariamente para encontrar archivos infectados. Por defecto todo archivo con extensión ".exe" será eliminado automáticamente al igual que aquellos archivos infectados y virus encontrados, en todos los casos se le enviará un mensaje al dueño de la cuenta informando el hecho.

5. En caso de encontrar un virus desconocido, los responsables de la seguridad informática actuarán consecuentemente según el daño que pudiera ocasionar. Como resultado final, para todos los casos, el virus será eliminado, ya sea descontaminando el archivo o actualizándolo en el repositorio por un respaldo descontaminado. Existen diferentes vías de entrada de un virus al sistema que requieren de procedimientos distintos para lograr la descontaminación:

   - El virus es entrado al sistema unido a un fichero o software adquirido por terceros en un acto de compra o actualización por parte de la ONRM que almacena sus datos en el centro. En este caso el producto será sometido al proceso de cuarentena establecido en las normas del centro. Una vez demostrado que el virus no puede ser eliminado se le informa a las entidades implicadas sobre el hecho, así como a las autoridades (MININT). La PC involucrada en el proceso se mantiene aislada hasta encontrar una solución. Si no aparece una solución factible la PC es formateada y restaurada para que siga prestando su función.

   - El virus entra vía correo. En este caso todos los mensajes son escaneados antes de entrar al

servidor, por lo que si se encuentra algún paquete contaminado y no se puede descontaminar es eliminado automáticamente, informándole al dueño de la cuenta la acción realizada.

- El virus penetra a través del intercambio en el servidor FTP. Una vez que el antivirus encuentra ficheros infectados en el servidor FTP y no los puede desinfectar, automáticamente los elimina y es responsabilidad de los administradores de red avisarle al usuario implicado para que logre desinfectar los archivos y vuelva guardarlos en el servidor. Quedará un informe de la situación como constancia del hecho.

2.5.2.3.3 Ataques de red

Las normas sobre el acceso y flujo de la información a través del Firewall por hardware ya fueron tratadas en el tópico **Firewall por hardware**, seguidamente se mostrará un conjunto de procedimientos relacionados con la configuración del Firewall por hardware enfocados al proceso de detección de intrusos y posibles ataques a la red interna.

1. El Firewall tendrá habilitadas dos zonas; zona desmilitarizada (DMZ) y zona de administración y servidores.
2. En el Firewall se habilitarán puertos para prestar los servicios de comunicación e Internet:
   - Puerto 25 para correo SMTP.
   - Puerto 21 para intercambio en el servidor FTP.
   - Puerto 80 para el acceso a Internet mediante el Proxy.
3. El Router WAN también será configurado para garantizar la seguridad aprovechando sus posibilidades. En este dispositivo serán bloqueadas aquellas direcciones IP que resulten no confiables o que, por algún motivo, se decida que no deben acceder al centro.

Otros parámetros a tener en cuenta:

Para darle cumplimiento a estos puntos solo se habilitarán los puertos necesarios en el Firewall.

1. El servidor DNS pide consultas a otros servidores DNS y es consultado también por éstos en el proceso de resolución de nombres.

2. El servidor Proxy tiene salida solo al exterior, desde la red externa no se puede acceder a él.

3. El servidor Web es consultado por los usuarios pero él jamás se conectará al exterior.

4. El servidor FTP es accedido desde el exterior para copiar datos y en caso extraordinario subir archivos.

5. Los puertos que no estarán en uso serán bloqueados.

Procedimientos para detectar ataques de intrusos:

1. En el Firewall por hardware será registrado, mediante Log(s), todo el tráfico entre las redes interna y externa en ambos sentidos. Estos Log(s) serán enviados a los servidores de Base de Datos donde serán almacenados para su gestión. Mediante un programa para gestionar los Log(s) almacenados, se monitoreará en tiempo real todas las acciones que ocurren en la red interna, éste programa permite también mostrar datos estadísticos como podrían ser: saber que usuarios han realizado mayor cantidad de consultas, que consultas son ejecutadas con más frecuencia, entre otras.

2. Los Log(s) se mantendrán almacenados en los servidores de Bases de Datos por un tiempo prudencial establecido por los administradores de red, donde, pasado ese tiempo, se eliminarán aquellos que no hagan falta en futuras auditorías.

2.5.2.3.4 Seguridad de Bases de Datos

Para lograr la seguridad de las Bases de Datos es necesario establecer un conjunto de normas y procedimientos que garanticen la explotación adecuada de los recursos que se almacenan. Muchas de éstas normas ya se han tratado en diferentes epígrafes anteriores por la alta relación que existe entre los temas que tratan sobre aspectos específicos y de ciertas maneras comunes entre ellos.

1. Los servidores de Bases de Datos solo permitirán conexiones procedentes del servidor de Aplicaciones y de las máquinas de administración, cualquier otro intento de conexión será rechazado.

2. Toda consulta que llega a los servidores de Bases de Datos habrá pasado por un proceso de autorización donde se le habrá dado los permisos necesarios al usuario para ejecutarla:

   - El usuario se autentica en el servidor Web.
   - Una vez autenticado se le asigna una credencial o nivel de privilegios para acceder a los servicios.
   - Según el nivel de privilegio podrá ejecutar una u otra consulta.
   - El servidor de aplicaciones antes de mandar a ejecutar la consulta verifica que el usuario tiene suficiente privilegio para ello.
   - Cuando la consulta llega al servidor de Base de Datos es porque está lista para ser ejecutada sin riesgos.

3. En el mecanismo detector de intrusos implementado en el centro se deben registrar los diferentes datos de cada usuarios con respecto al uso de las bases de datos:

   - Duración de los usuarios conectados al sistema.
   - Número de consultas realizada a las bases de datos.
   - Número de intentos fallidos de consultas a las bases de datos.
   - Ocurrencia de deadlock con las bases de datos.
   - Generación de nuevos objetos de base de datos.
   - Modificación de los datos.

4. Deberá realizarse chequeos periódicos a los sistemas de control y de bases de datos para verificar los siguientes parámetros.

   - Se hacen y son efectivos los backup(s) y los mecanismos de seguridad.

- No exista un usuario en el servidor de Directorio que no tenga un privilegio asignado y una contraseña robusta que cumpla con las normas establecidas en el centro.

- Se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo.

- Solo el administrador del departamento de Administración de Redes tiene acceso de lectura y escritura en los archivos de programas instalados en el centro.

- Las bases de datos y todas las aplicaciones y sistemas del centro tienen suficientes recursos libres para trabajar eficientemente.

5. Cada cambio que se haga en las bases de datos quedará guardado en un backup temporalmente por un tiempo estimado por la dirección del centro con el objetivo de revertir la información a su última configuración válida en caso de surgir algún problema.

6. Los registros de las bases de datos no se borrarán físicamente, sino que se marcarán como eliminados.

7. Los datos en las bases de datos estarán clasificados en diferentes grupos dependiendo de la importancia que tengan. Las clasificaciones serán: crítica, confidencial y públicas. El acceso a los diferentes grupos de datos se define cuando el usuario se autentica en el servidor Web y le es otorgado un nivel de privilegio.

2.5.3 Auditoría

En el proceso de auditoría al Centro de Datos se comprobará que todas las normas y procedimientos establecidos se cumplen cabalmente como está establecido. Inicialmente la actividad se llevará a cabo cada tres meses una vez puesto en funcionamiento este plan de seguridad. Luego de comprobar que el sistema funciona correctamente, las frecuencias de auditorías cambiarán a seis meses o a un año. Los responsables de que el proceso se lleve a cabo eficientemente serán, el jefe del departamento de Administración de Redes y un responsable designado por la Oficina Nacional de Recursos Minerales.

Durante el proceso de auditoría se deberá comprobar:

1. Que todos los usuarios registrados cuentan con una contraseña robusta acorde a las normas implantadas y que tienen un nivel de privilegio para acceder a la información.

2. Que el sistema de autenticación de usuarios funciona correctamente y que no haya la posibilidad de que exista un usuario externo que haga uso de los servicios sin estar registrado previamente en el sistema.

3. Que el acceso a la Internet por parte de los usuarios internos se efectúe acorde a las normas establecidas.

4. Que el acceso de los usuarios a los recursos y de activos a activos se realice acorde a las normas establecidas, para comprobar esto se harán intentos de acceso a lugares y servicios restringidos para verificar que el sistema responde adecuadamente.

5. Que el Firewall por hardware esté correctamente configurado permitiendo solamente los accesos establecidos.
6. Que todos los equipos de cómputo cuentan con un producto antivirus instalado, configurado y actualizado correctamente.

7. Que todos los informes generados al hacer las diferentes acciones que lo exigen estén correctamente documentados y actualizados.

8. Que el mecanismo detector de intrusos funciona correctamente y es capaz de gestionar los Log(s) capturados en el Firewall brindando así estadísticas e informaciones importantes tanto en tiempo real como de los datos almacenados.

9. Que los requerimientos técnicos como: la climatización, el cableado de la red, la instalación eléctrica (incluye los UPS y el generador central), etc., estén funcionando correctamente en cada área.

10. Que las áreas cuenten con los sistemas de protección física requeridos como: extintores manuales, sistemas detectores de incendios y humo, sistemas detectores de intrusos, alarmas sonoras, guardia

de seguridad, etc.

11. Que la guardia de seguridad está cumpliendo con el horario y el objetivo establecido y que se compruebe que el personal del Centro de Datos se encuentre debidamente acreditado y use correctamente las credenciales, siempre en un lugar que sea visible.

12. Que los diferentes registros como: el de acceso, control de soporte y entrega/recepción de soportes magnéticos estén actualizados y que se pueda comprobar que cada soporte de información perteneciente a la entidad esté registrado e identificado según el registro, es decir, que se pueda establecer una comparación.

13. Que los dispositivos de soporte fueron debidamente eliminados o borrados y que los datos pertinentes estén reflejados en la Observación del registro de control de soportes.

2.5.4 De Seguridad de Operaciones

2.5.4.1 Salvaguardas

Para mayor organización se analizará por separado el área de servidores de Bases de Datos y el área de los servidores de comunicación (DMZ).

Servidores de Bases de Datos:

1. Para realizar las salvaguardas a los servidores de Bases de Datos la técnica a aplicar será: "salvaguardas cruzadas"; este proceso consiste en realizar salvas frecuentes de forma tal que los datos a salvar de un servidor se guarden en otro servidor dentro de la misma área de servidores de Bases de Datos. El horario para poner acción a este procedimiento será escogido por los administradores de redes de tal forma que ocurra en un lapso de tiempo donde el tráfico de la red sea el menor posible.

2. Los archivos (Log(s)) pertenecientes al Firewall serán almacenados temporalmente en un servidor de Bases de Datos y aquellos que se consideren importantes serán guardados en CD o DVD bajo llaves.

3. Los datos correspondientes a la configuración del Firewall serán almacenados junto a los Log(s) en los

servidores de Bases de Datos y posteriormente guardados en CD o DVD bajo llaves.

4. Los datos de configuración del Firewall estarán también impresos en informes de papel guardados bajo llaves en el Centro de Datos.

5. La información de configuración de todos y cada uno de los Switch y el Router se almacenarán en el área de servidores de Bases de Datos y además se grabarán en CD o DVD y estarán impresos también en un informe de papel guardado bajo llaves.

Área de los servidores de comunicación (DMZ):

1. Las salvaguardas de los servidores del área de la (DMZ) se harán en el servidor Proxy. Este servidor es utilizado solamente para garantizar y controlar el acceso a internet de los usuarios internos, por lo que su uso será muy pobre y podrá fácilmente almacenar las salvaguardas de ésta área sin afectar su función original.

2. El servidor Proxy para almacenar las salvaguardas tendrá una partición en el disco duro independiente a la partición donde corre el programa Proxy. A ésta partición solo podrá acceder la máxima dirección del departamento de Administración de Redes.

3. Las salvas de configuración de los servidores de la DMZ la hará personalmente el máximo representante del departamento de Administración de Redes manualmente, es decir, desde su PC ubicada en el área de administración. Estos datos no cambiarán con frecuencia por lo que será fácil llevar a cabo la tarea sin problemas.

4. Todas las salvas almacenadas, tanto en CD, DVD, servidores de Bases de Datos, como las almacenadas en el Proxy, que se consideren de alta importancia se pasarán para un disco duro externo. Este será conectado directamente vía USB a los servidores y el proceso será controlado desde las PCs de administración. Esta actividad tiene como objetivo trasladar las salvaguardas hacia la Oficina Nacional de Recursos Minerales y así poder hacer uso de ellos en caso de contingencias. El traslado será regido según las normas establecidas en el presente Plan de Seguridad.

2.5.4.2 Instalaciones de Software

1. Es importante mantener el control de los software(s) instalados en cada uno de los equipos de cómputos y servidores. Por lo que será necesario seguir los siguientes procedimientos:

   - Deberá existir un registro para el **control de software** en la Administración del Sistema. El registro contendrá los siguientes datos:
     - No. de Activo Informático (Equipo donde se encuentra instalado el software; puede ser el número del inventario o el número de serie).
     - ID del Software.
     - Nombre del Software.
     - Versión instalada.
     - Versión anterior (En caso de que se haya modificado).
     - Fecha de instalación.
     - Nombre y Firma de quien lo instaló.
     - Nombre y Firma de quien autorizó la instalación.
     - Observación.

   - Cada vez que se instale o se modifique algún software existente deberá existir un responsable dentro de la Administración del Sistema quien verificará que el registro fue actualizado debidamente.

2. Una ves que el Centro de Datos se encuentre funcionando y los administradores de redes encuentren deficiencias en las aplicaciones, los servicios o en el funcionamiento del sistema deberán tener en cuenta los siguientes procedimientos basados en el **[Anexo #1]**:

   - Deberá investigar sobre la existencia de un software que detecte cada vez que ocurra el incidente o simplemente que sea capaz de dar solución al problema.

   - Deberá comprobar la compatibilidad con el sistema operativo, si es software libre o propietario e informar a la Administración del Sistema sobre las demás características del producto y solicitar una autorización para su instalación en el sistema.

   - Antes se le realizarán pruebas de seguridad por parte de un especialista que deberá estar

supervisado por uno de los responsables del área de administración. El especialista puede ser un trabajador del centro.

- En dependencia de la función del producto el especialista introducirá datos ficticios o simplemente realizará un simulacro en una máquina aislada para no comprometer el sistema y comprobar si realmente cumple con las expectativas, además de que el producto se encuentre libre de programas malignos.

- Por último, al comprobarse la veracidad del producto se procederá a instalarlo en el sistema informático y a la actualización del **registro de control de software**.

2.5.4.3 Mantenimiento y reparación de las Tecnologías de Información

Para lograr que el Centro de Datos trabaje correctamente en cuanto a funcionamiento y servicios que brinda, es necesario mantener protegidos adecuadamente los equipos electrónicos que permiten cumplir el objetivo de la entidad. Para ello es preciso:

1. Dar mantenimiento a todos los equipos una vez cada 5 o 6 meses.

   - La administración del sistema deberá ponerse de acuerdo para designar a las personas capaces de realizar esta acción.

   - De no existir en el centro el personal calificado para realizar el mantenimiento, se le solicitará a COPEXTEL[1] el servicio requerido. Siempre bajo la supervisión de un trabajador perteneciente a la Administración del Sistema.

2. Para la reparación de los equipos se procederá de la misma manera que con el mantenimiento, en caso de no existir personal calificado en el centro, se solicitarán los servicios de otra empresa.

3. El Centro de Datos deberá tener un **registro para controlar el estado de todos los equipos** cada vez que se le realice la reparación de alguno de ellos y se deberá actualizar en cada

[1]COPEXTEL: Empresa cubana comercializadora de equipos electrónicos y tecnologías.

momento que efectúe esta acción.

4. El registro deberá contener los siguientes puntos:

    - Fecha de reparación.
    - Nombre(s) y Apellidos (De el/los especialista(s)).
    - Firma del responsable (En caso de que sean más de un especialista).
    - Nombre y Firma del trabajador de supervisión.
    - No. de. Activo Informático (Equipo donde se encuentra instalado el software; puede ser el número del inventario o el número de serie).
    - Observación (Se describirán los errores encontrados y los cambios realizados).

2.5.5 De Recuperación Ante Contingencias

El Plan de Contingencias se activa una vez que el sistema no puede ser controlado aplicando el conjunto de normas y procedimiento descritos hasta el momento. Normalmente la seguridad, tanto física como lógica, es controlada eficazmente. Si por algún motivo surge un incidente que, aunque haya sido concebida su materialización, no se pueda dar una respuesta factible con el mecanismo implementado hasta el momento, en cuanto a seguridad se refiere, entonces es cuando entra en acción el Plan de Contingencias.

El Plan de Contingencias no se puede analizar separado del análisis de riesgos y del conjunto de políticas, normas y procedimientos que se siguen en el centro para garantizar la seguridad de los recursos y servicios. Como primera acción se tendrá en cuenta el conjunto de amenazas a las que está sometido el sistema en cuestión, clasificándolas en, bajas, medias y altas, según la probabilidad de que se materialicen. En todo el plan de seguridad informática se establecen los pasos a seguir para mitigar las amenazas de las que se están hablando, sin embargo, el Plan de Contingencias continúa, de cierta forma, tratando de lograr los mismos objetivos. Lo que hace diferente a un plan de contingencias del resto del plan de seguridad informática es la situación específica en que se encuentra el sistema en el momento en que se aplica.

El plan de contingencias internamente comprende cuatro planes:

a) **Plan de respaldo.** Contempla las medidas preventivas antes de que se materialice una amenaza.

Su finalidad es evitar dicha materialización.

b) **Plan de emergencia.** Contempla las medidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es contrarrestar los efectos adversos de la misma.

c) **Plan de recuperación.** Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

d) **Plan en caso de huracanes.** Incorpora las acciones, responsables y actividades en caso de una amenaza de huracán.

El primer punto "Plan de respaldo", ya ha sido desarrollado por momento en el presente documento, por lo que éste tópico estará centrado en las restantes parte que comprende el Plan de Contingencias.

Grupo de trabajo ante Contingencias:
El grupo de trabajo ante contingencias estará compuesto por todos los trabajadores del Centro de Datos, al frente de la brigada estará el máximo representante del departamento de Administración de Redes.

1. Éste grupo de trabajo deberá tener pleno dominio del conjunto de procedimientos a realizar en caso de presentarse una contingencia.

2. Deberán conocer las técnicas que se aplican para sofocar incendios.

3. Deberán conocer el número de teléfono de la Policía Nacional Revolucionaria y del cuerpo de bomberos, así como el de la Oficina Nacional de Recursos Minerales e informar cualquier situación que ocurra en el menor tiempo posible.

4. Cada trabajador tendrá asignado un conjunto de actividades que cumplir definidas previamente a la contingencia.

5. Las actividades son asignadas por el máximo representante del Centro de Datos o por otro trabajador designado.

6. Una vez se presente una contingencia de cualquier índole, el grupo de acción comenzará a funcionar hasta que el sistema vuelva a restablecerse nuevamente bajo parámetros aceptables.

Seguidamente se muestra un conjunto de amenazas que podrían materializarse en algún momento causando daños a diferentes niveles en la prestación de servicios y en los datos en sí. Éstas amenazas no significan que haya un cien por ciento de probabilidad de que algún día se materialicen; si bien es cierto que el centro no está libre de ellas, también se puede decir que es difícil que ocurran.

- Falla eléctrica por largo tiempo.
- Incendio.
- Falla en el servidor Web.
- Falla en el servidor DNS.
- Falla en el servidor de Aplicaciones.
- Falla en el servidor de Directorio.
- Huracanes.

Todas las acciones a tomar en una etapa considerada antes de la contingencia, en lo que sería un día normal, ya se han tratado en el resto del plan de seguridad.

2.5.5.1 Falla eléctrica por largo tiempo:

Una falla eléctrica se considera por largo tiempo cuando, una vez interrumpido el fluido eléctrico, el tiempo que transcurre es tal que el generador automático de corriente eléctrica se aproxima al agotamiento de sus reservas.

- El centro contará con un generador eléctrico de gran capacidad por lo que, cuando ocurra un fallo eléctrico pasará un largo tiempo antes que la reserva se agote.

- El centro, a pesar de contar con activos consumidores, es pequeño con respecto a la capacidad

del generador eléctrico, lo que propicia que el tiempo en agotarse la reserva de combustible sea mayor.

- Se deberá controlar el combustible del generador después de ocurrida una falla eléctrica.
- Se deberá tener combustible de reserva en caso de que la falla eléctrica se extienda demasiado y en caso de que se esté agotando solicitar o comprar la necesaria para que el generador mantenga su función.

Acciones Durante la Contingencia:

1. Cada equipo de cómputo del Centro cuenta una UPS que brinda servicios por un tiempo aproximado de veinte minutos una vez interrumpido el fluido eléctrico.

2. Cuando las reservas de combustible puedan abastecer al centro solo por dos horas y el fluido eléctrico de la red nacional no se restablece se llamará a los teléfonos de la compañía eléctrica para informarse sobre el posible restablecimiento. También se dará parte a la Oficina Nacional de Recursos Minerales.

3. En el centro casi todos los equipos son de alta importancia por lo que deben mantenerse prendidos a tiempo completo.

4. Si en el momento existe algún servidor que no esté prestando servicio se procederá a desconectarse de la red eléctrica.

5. Si el servidor Proxy solo está prestando servicios como servidor Proxy, será desconectado de la red eléctrica, esto implica que los usuarios internos no tendrán acceso a Internet.

6. Se le enviará un mensaje vía correo a todos los usuarios del Centro de Datos avisando que puede haber una interrupción en la prestación de servicios explicándoles el motivo.

7. La máquina de administración, que su uso sea prescindible, será desconectada de la red eléctrica.

8. Si la empresa encargada del suministro de combustible para el Centro de Datos repone la reserva

de combustible, se podrá prestar servicios por más tiempo.

9. Cuando se compruebe que el servicio eléctrico de la red nacional no será restablecido antes de que la reserva se acabe y ésta ya se esté agotando, se procederá a desconectar paulatinamente todos los equipos del centro comenzando por los aires acondicionados. El apagado de los equipos de cómputo será por software después de terminar correctamente todos los procesos que están corriendo, nunca se deberá permitir que la energía se acabe antes de haber apagado correctamente el equipo.

Acciones después de la contingencia:

1. Una vez restablecido el servicio eléctrico de la red nacional se procederá a poner en funcionamiento todos los equipos y servicios que presta el centro.

2. Si un equipo de cómputo presenta algún problema, se le dará solución por parte de los trabajadores del centro de ser posible, o se avisará a los servicios técnicos

3. Se enviará un correo a todos los usuarios informando que los servicios han sido restablecidos.
4. Al final quedará un informe con todos los detalles acontecidos durante la contingencia.

2.5.5.2 Falla en servidores del área desmilitarizada (DMZ):

El Centro de Datos entrará en período de contingencias una vez que alguno de los servidores que se mencionan a continuación deje de prestar servicios. La situación que se presenta en éstos casos no es crítica porque los mecanismos establecidos permiten que la afectación cause el menor impacto posible. El conjunto de medidas que se tomarán serán válidas tanto para cuando estos servidores dejen de funcionar por algún problema desconocido como para cuando son sometidos a mantenimiento.

- ✓ Servidor Web.
- ✓ Servidor de Aplicaciones.
- ✓ Servidor de Directorios.
- ✓ Servidor DNS.

2.5.5.2.1 Falla en el servidor Web:

En caso de que ocurra alguna afectación en el servidor Web que impida su funcionamiento, el servidor FTP comenzará a prestar este nuevo servicio. ¿Por qué?

- Porque el servidor FTP presenta características similares al servidor Web en cuanto a usuarios que pueden conectarse a él. Su función en tiempos de normalidad no es tan activa por el restringido número de usuarios que hará uso de éste servidor, lo que permite asumir con facilidad más carga de funciones.

2.5.5.2.2 Falla en el servidor de Aplicaciones:

Si falla el servidor de Aplicaciones ésta función la seguirá realizando en el servidor en de Directorios de Usuarios. ¿Por qué?

- Porque el servidor de usuarios no es accedido directamente por ningún usuario exterior y en éste sentido es similar al servidor de Aplicaciones. Dada la similitud que presentan, se aprovecha a favor las configuraciones de seguridad.

2.5.5.2.3 Falla en el servidor de Directorios:

Si falla el servidor de Directorios de Usuarios esta función se continuará en el servidor Proxy. ¿Por qué?

- Porque el servidor Proxy permanece prácticamente inactivo todo el tiempo, además ningún usuario exterior se conecta a él directamente.

2.5.5.2.4 Falla en el servidor DNS:

Si falla el servidor DNS esta función se seguirá realizando en el servidor SMTP de correo. ¿Por qué?

- Porque el servidor de SMTP de correo será accedido desde la red exterior por los usuarios del centro y el servidor de DNS también intercambiará información con el exterior en el proceso de resolución de nombres.

Al efectuar alguna de las medidas descritas anteriormente, el servidor que asuma la nueva tarea recargará sus funciones, lo que puede provocar una disminución en el tiempo de respuesta en los

servicios que presta, llegando a provocar, en ocasiones, disminución en el tiempo de respuesta del sistema en general cuando el tráfico de información sea elevado. Cada Servidor deberá estar preparado con anterioridad para asumir la nueva tarea y así agilizar el proceso en caso de que ocurra una contingencia.

Una vez concluida la contingencia todos los servidores afectados volverán a prestar los servicios para los cuales fueron destinados originalmente.

2.5.5.3 Incendio:

La probabilidad de que ocurra un incendio es muy pequeña dada las condiciones físicas con que cuenta el Centro de Datos, pero, como probabilidad al fin, puede que en algún momento se materialice y hay que estar preparados para enfrentar la situación.

Acciones Durante la Contingencia:

1. Una vez detectado un indicio de fuego o humo en el Centro, se procederá a activar manualmente las alarmas en caso de que no se hayan activado automáticamente.

2. En dependencia de la magnitud de la situación se procederá a sofocar el incendio con extintores. El uso de los extintores será una opción cuando la Contingencia en sí lo permita; si el fuego es fuerte se llamará a los bomberos, a la policía y a la Oficina de Recursos Minerales.

3. Teniendo en cuenta que la única causa que pueda provocar un incendio o hacerlo mayor en caso de que ocurra por otra vía, es el cableado y sistema eléctrico en general, se desconectará todo el sistema eléctrico del Centro de Datos.

4. Una vez que el cuerpo de bomberos llegue comenzará a realizar su trabajo.

Acciones después de la contingencia:

1. Se procederá a analizar los daños ocasionados por el desastre para conocer la magnitud de la afectación.
    - ✓ Sistemas que han sido afectados.

- ✓ Equipos que han quedado no operativos.
- ✓ Cuales se pueden recuperar.
- ✓ En cuanto tiempo.

2. Se elaborará un informe donde se recogen los datos necesarios para mantener informados a la dirección de la empresa responsable del Centro de Datos.

3. Paulatinamente se irán restableciendo los servicios que prestaba el Centro de Datos antes de la Contingencia.

4. Para restablecer la información original se hará uso de las salvas de respaldo almacenadas anteriormente en la Oficina Nacional de Recursos Minerales.

5. Una vez que el Centro esté listo para reanudar sus servicios se enviará una notificación a todos los usuarios informándoles la razón del tiempo que se mantuvo la afectación y el restablecimiento de los servicios.

2.5.5.4 Huracanes:

El Centro tendrá una constitución física lo suficientemente fuerte como para soportar vientos huracanados y ciclones de gran escala, lo que no impide que se tomen las medidas pertinentes en caso de que ocurra un desastre.

Acciones antes de la contingencia:

1. Los trabajadores de guardia se mantendrán informados y al pendiente en todo momento sobre la situación atmosférica a través de los medios radiales y televisivos.

2. Las antenas que estén instaladas en el techo del Centro de Datos serán bajadas y guardadas en el interior.

3. Se comprobará que todos los sistemas de comunicación funcionan correctamente.

Acciones durante de la contingencia:

1. Los trabajadores del Centro seguirán informándose sobre el desarrollo del fenómeno meteorológico.

2. Como hay grandes posibilidades de que el fluido eléctrico de la red nacional se vea afectado, los trabajadores deberán estar pendientes de esa situación.

3. Una vez que el fluido eléctrico de la red nacional falle se activará el grupo electrógeno.

4. Si el huracán es de gran intensidad se procederá a desconectar de la red eléctrica todos los equipos de cómputo y el grupo electrógeno será apagado para evitar un incendio o mayores daños.

5. Las puertas permanecerán cerradas todo el tiempo impidiendo la entrada de aire exterior.

Acciones después de la contingencia:

1. La situación crítica acabará cuando se informe por parte del instituto de meteorología que ha pasado a fase informativa la provincia en la cual está instalado el Centro de Datos. A partir de este momento el Centro pasará a la etapa de recuperación.

2. Las antenas de comunicación serán colocadas nuevamente en sus lugares de origen.

3. Si el fluido de corriente eléctrica de la red nacional no se ha restablecido no se pondrá en funcionamiento el grupo electrógeno para así evitar caer en otra etapa de contingencias por falla de corriente eléctrica.

4. Una vez se restablezca el fluido eléctrico de la red nacional se comenzará a poner en funcionamiento los equipos de cómputo del Centro según las normas establecidas para una etapa de contingencias por falla eléctrica.

5. Se hará un informe resumen donde se refleje toda la situación acontecida durante la etapa de contingencias, reflejando también posibles acciones a tomar para similares etapas de contingencias donde se acuerden nuevas normas a aplicar que mejoren la conservación y restauración de los servicios en un menor tiempo según las experiencias adquiridas.

6. Se enviará un aviso correo a todos los usuarios del Centro de Datos explicando la situación acontecida y el restablecimiento de los servicios.

2.6 Análisis de los beneficios que se obtienen con el resultado de la solución

La tecnología avanza para bien y con ella el desarrollo de la humanidad. En los tiempos presentes, estar correctamente actualizado en el campo de la informática no es una moda, es una necesidad que preocupa y ocupa a todas aquellas personas que luchan por mantener su información protegida bajo cualquier circunstancia. Nuestro país no se queda detrás en tal sentido y como muestra de ello surge esta investigación. El plan de seguridad informática que aquí se presenta, está directamente enfocado a la Oficina Nacional de Recursos Minerales pero, aún así, los beneficios que aporta van más allá de esa frontera visible. Como objeto tangible se aprecia un documento elaborado con la mayor exquisitez, de forma tal que expone desde la estructura interna, lógica y física de un centro de datos, hasta todo el conjunto de políticas, normas y procedimientos que regulan el comportamiento del sistema en sí. Lo que plantea la investigación, es aplicable también a cualquier otro centro de datos que internamente tenga implementado la misma estructura lógica (la red interna) que se diseña en la investigación. Construir un sistema con las características expuestas en el presente trabajo, implica invertir gran cantidad de dinero en un inicio, pero, una vez puesto en funcionamiento, las ganancias a nivel de país son considerables. Si se entra a analizar al detalle, fácilmente se encuentra que no es menos cierto, que cada empresa trata de proteger sus bienes informáticos de la manera que estime conveniente en dependencia de los conocimientos y las posibilidades económicas con que cuente. Esto implica que habrá instituciones muy bien protegidas y otras no tanto, hasta aquí nada nuevo, pero, ¿Donde está el aporte de un centro de datos con respecto a lo que se plantea? Pues bien, una vez se cuente con un centro lo suficientemente protegido y confiable donde todos puedan almacenar, sin ningún tipo de dificultad, el patrimonio informático que poseen, ninguna empresa individual tendrá que preocuparse por adquirir los costosos equipos de cómputo para realizar estas funciones, además de contar con la máxima seguridad en consecuencia con la información que se almacena. Visto todo de un punto más cercano a la realidad que vive la Revolución Cubana, donde se lucha por ser cada vez más socialista y para que la igualdad reine en la vida de los ciudadanos, es una magnífica opción materializar los resultados de la presente investigación en aras de lograr la equivalencia de

posibilidades entre las diferentes empresas en cuanto a seguridad informática.

El plan de seguridad informática mostrado en este documento fue elaborado bajo la "Metodología para la Elaboración del Plan de Seguridad Informática" dictado por la Dirección de Protección del Ministerio del Interior. El diagrama de red final, que representa la estructura lógica interna de un centro de datos, fue resultado de varias entrevistas a especialistas competentes que se desempeñan en aspectos de redes informáticas en la Universidad de las Ciencias Informáticas. Para garantizar también un correcto desempeño al tratar la seguridad informática, se realizaron entrevistas al jefe de seguridad informática en el mencionado centro de altos estudios. Además, la investigación está respaldada por todo un conjunto de bibliografías que reflejan como se tratan estos temas a nivel internacional en la actualidad. Precisamente este respaldo científico es lo que le da confianza a aquellas entidades que decidan implementar un centro de datos aplicando el presente plan de seguridad informática.

Otros aspectos válidos a analizar, surgidos como resultado de la investigación, lo constituyen el empleo de distintos componentes de red que aseguran el control y flujo de la información al máximo. Dentro de estos componentes, uno de gran importancia y poco usado en nuestro país por el alto costo que implica adquirirlo, es el Firewall por hardware. Para una empresa común es desfavorable incorporar un equipo como éste solo por lograr un poco más de seguridad. La perspectiva cambia cuando la misma empresa si llega a utilizar el mencionado equipo pero de forma indirecta, es decir, hospeda sus recursos informáticos en un centro de datos que si contiene las condiciones ideales de seguridad en todos los sentidos. Transitivamente, la empresa ha asegurado su información sin tener que invertir en recursos económicos elevados para tal sentido. Otros componentes son los diferentes Switch(s) que se emplean, capaces de filtrar paquetes de información que circulan en grandes cantidades y a altas velocidades; ¿Que institución sin grandes recursos puede darse el lujo de usar dicho dispositivo? Mencionar también el uso de la zona desmilitarizada (DMZ) para mayor seguridad, el conjunto de servidores de comunicación de altas prestaciones, etc. Éstos son resultados intangibles reflejados directamente en la investigación realizada, materializada en un plan de seguridad informática para un centro de datos.

2.7 Conclusiones Parciales

En este capítulo se le ha dado solución al problema científico planteado mediante la realización de

como deberá estar compuesto el futuro sistema informático y la propuesta y descripción de sus componentes. Dando paso a que posteriormente se le realizará el análisis de riesgos donde se identificaron y evaluaron cada uno de los activos, así como las amenazas que puedan afectarlos. Obteniendo un resultado final, determinando cual sería el riesgo total del sistema y de cada una de sus áreas.

Además se establecieron las políticas de seguridad a seguir y que regirán lo que está bien o no, para evitar incidentes que puedan afectar al sistema o a algunos de sus elementos. Las políticas están respaldadas por las medidas de seguridad tanto físicas como lógicas ante los ataques y contingencias que puedan permitir las vulnerabilidades que existan en el sistema. También se desarrolló un plan de contingencias que se aplicará en caso de que las medidas y procedimientos preventivos no hayan sido suficientes para evitar algún incidente o contingencia. Además se realizó un análisis de los beneficios del trabajo efectuado.

CONCLUSIONES

La presente investigación abordó sobre la necesidad existente de proteger la información que coexistirá en el Centro de Datos que fundará la Oficina Nacional de Recursos Minerales. Para lo que se planteó como objetivo principal la elaboración de un plan de seguridad informática que gestionaría la integridad, confiabilidad, disponibilidad de la información y de los medios informáticos que la contendrán y que además harán posible ofrecer los distintos servicios que brindará el centro.

Dentro del plan de seguridad se realizaron diversas actividades como: la realización del Análisis de Riesgos al sistema informático propuesto, recordando que para efectuar el análisis debe existir un sistema y que en ausencia de este, se propuso en la **Caracterización del Sistema** un **Diagrama de Red** de cómo deberá estar conformado el Centro de Datos. De igual forma se concretaron y clasificaron cuales serían las políticas de seguridad a aplicar y se desarrollaron las medidas y procedimientos de seguridad tanto físicos como lógicos para la protección completa del sistema, abarcando todas las posibles vulnerabilidades que podrían ponerlo en riesgos y que en caso de que ocurriese un incidente estaría respaldado por un plan de contingencias para la combatividad del suceso y recuperación en el menor tiempo posible.

Por último se realizó un análisis de los beneficios que aporta la investigación para la ONRM, nuestro país y al futuro Centro de Datos. Beneficios que son tanto tangibles como intangibles y que se obtienen una vez que se cumplieron los objetivos del trabajo.

Para complementar todo lo que se ha expuesto en esta investigación y obtener los resultados o beneficios ya mencionados en el **Capítulo 2** es necesario seguir las recomendaciones que se muestran en el acápite siguiente.

RECOMENDACIONES

- Tener en cuenta todas las medidas y los procedimientos descritos en el presente documento a la hora de elegir la ubicación del local y de los activos.

- Reflejar en un documento las responsabilidades de cada uno de los participantes en el proceso informático.

- Documentar el listado nominal de usuarios con Acceso a Redes con Alcance Global.

- Realizar la primera auditoría al sistema a los tres meses de implantado el sistema y perfeccionar el Plan de Seguridad según las deficiencias detectadas.

REFERANCIAS BIBLIOGRÁFICAS

[**1**] "Centro de Procesos de Datos (Data Center)," 2008. [http://es.wikipedia.org/wiki/Centro_de_proceso_de_datos].

[2] C. d. E. d. l. R. d. Cuba, "DECRETO-LEY No. 199/ SOBRE LA SEGURIDAD Y PROTECCION DE LA INFORMACION OFICIAL," 1999, Pág. 2.

[3] I. C. S. C., "¿Qué es la seguridad informática?," 2005. [http://www.citel.oas.org/newsletter/2005/septiembre/seguridad_e.asp].

[4] M. E. e. D. d. S. G. y. D. e. D. d. S. d. l. I. Ignacio B. López, "Confidencialidad, integridad y disponibilidad de la información", 2004.

[5] C. I. y. C. d. MINED, "Plan de Seguridad informática." [http://seguridadinformatica.rimed.cu/].

[6] A. V. HUERTA, "Seguridad en Unix y Redes," in Seguridad física de los sistemas, 2002.

[7] "Seguridad Lógica," [http://www.segu-info.com.ar/logica/seguridadlogica.htm].

[8] "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información," MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Madrid, 2006.

[9] "Conceptos Básicos de Seguridad Informática." [http://www.daforos.com/index.php/topic,85.0.html].

[10] J. R.-P. Holbrook, "Site Security Handbook," 1991.

[11] L. J. J. Bardi, "LA SEGURIDAD CONTINENTAL Y LAS NUEVAS AMENAZAS". [http://www.geo-strategy.com/geoestrategia/america/articulos/ame031112.htm]

[12] P. I. P. MARIA DOLORES CERINI, "PLAN DE SEGURIDAD INFORMÁTICA," 2002.

[13] CIENTEC, "EL PUENTE MÁS FAMOSO DE LAS REDES." [http://www.cientec.com/analisis/puente.asp].

[14] "Firewall / Cortafuegos." [http://www.segu-info.com.ar/firewall/firewall.htm].

[15] "Manual del Profesor," presentado en Tecnologías de Redes de Computadoras.

[16] "Módulo Proxy," Sistemas Internet Empresariales. [http://www.albasoft.com/docu/prd/ser_red_proxy.html].

[17] A. E. C. Quezada, "PROXY. Buen Punto," INFORMATIZATE. [http://www.informatizate.net/articulos/proxy_buen_punto_20030822.html].

[18] "Servidor DNS," Tecnológico de Monterrey.

[19] J. Vegas, "Desarrollo de Aplicaciones Web," 2002.

[20] "Servidor FTP." [http://servidorftp.es/].

[21] "Introducción a los servidores de aplicaciones," 2004.

[22] J. M. L. Franco, "Servidores de aplicaciones," 2001.

[23] "DICCIONARIO INFORMÁTICO,"

[24] "Política oficial de Seguridad Informática del CICESE," Tercer Módulo de la Academia Latinoamericana de Seguridad Informática., 2001.

[25] I. R. A. Ávila, "Administración de las instalaciones," 2007.

BIBLIOGRAFÍA CONSULTADA

1. Sandra Rocio Murillo Cano. ASIS: Diseño y Aplicación de un Sistema de Seguridad Informatica para la UDLA. Cholula, Puebla, México : s.n., 2001.

2. Ministerio de Administraciones Públicas. Metodología de Análisis y Gestión de Riesgos de los Sistemas Informáticos. Madrid : s.n., 2006. Vol. 1.1.

3. CÓDIGO DE ÉTICA PARA USUARIOS DEL MINED.

4. Jorge A. Zárate Pérez / Mario Farias Elinos. Implementación de una DMZ. 2006.

5. Lázaro Orlando Aneiro Rodríguez. Elementos de Arquitectura y Seguridad Informática. Ciudad de la Habana : PUEBLO Y EDUCACI, 2001.

6. E. J. Mira, R. Montañana y F. J. Monserrat. Implantación de un sistema de detección de intrusos en un entorno universitario. 2003.

7. BMC Software y Enterprise Management Associates. Gestión eficaz de los cambios en todo el centro de datos. 2006.

8. Ortin Jimeno Jose Maria. Guía para la elaboración del marco normativo de un sistema de gestión de la seguridad de la información (SGSI). 2008.

9. Sistema de Gestión de Seguridad. Norma NTC-ISO/IEC 27001. 2005.

10. La politica de seguridad. Tercer Módulo de la Academia Latinoamericana de Seguridad Informática.

11. Coordinación Administrativa de Tecnologías de Información. Plan de Contingencias. Yucatán. 2007.

12. Universidad de la Habana Nodo Central. Plan de Seguridad Informática y de Contingencia. 2004.

13. Dirección Telemática. Política oficial de Seguridad Informática del CICESE. Ensenada : s.n., 2001.

14. Borghello, Cristian Fabian. Seguridad Informática: Sus Implicancias e Implementación. 2001.

15. Huerta, Antonio Villalón. SEGURIDAD EN UNIX Y REDES. 2002.

16. DeepZone Digital Security . Métodos de deteción de Virus informáticos. 1999.

17. Stephanson, Thomas. Amanecer en la Red(Warriors of the Net). 2002.

18. DECRETO-LEY No. 199/ Sobre la Seguridad y Protección de la Información Oficial.

19. Seguridad de la Información. [http://www.segu-info.com.ar].

20. Segunda edición de la Norma ISO/IEC 17799 (ISO 27002). 2005.

21. J. Vegas, "Desarrollo de Aplicaciones Web," 2002.

22. P. I. P. MARIA DOLORES CERINI, "PLAN DE SEGURIDAD INFORMÁTICA," 2002.

23. C. I. y. C. d. MINED, "Plan de Seguridad informática."

24. Ignacio B. López, "Confidencialidad, integridad y disponibilidad de la información", 2004.

25. MININT, “Metodología para la Elaboración del Plan de Seguridad Informática”. 2000.

ANEXOS

Anexo # 1: Entrevista realizada al Ing. Pablo Yunier Medina Martínez, Especialista General en la Dirección de Redes y Seguridad Informática de la UCI.

1.1 ¿Cuáles son los pasos o los componentes para desarrollar un Plan de Seguridad Informática?

Respuesta:
Primeramente se debe elaborar una descripción de los bienes informáticos existentes en el sistema, además de que por cada vulnerabilidad que se detecte deberá haber N políticas y M medidas que la respalden para impedir actividades ilícitas o contingencias de cualquier procedencia que lo pongan en riesgo; y en el caso de que alguna tenga éxito saber qué acciones realizar. Por lo que debe existir un equipo de especialista que responda ante cualquier incidencia guiados por las medidas que se tomaron en el plan de contingencias. También es necesario que se realicen auditorías y que se modifique el plan de seguridad informática según las deficiencias o errores detectados y las soluciones que se le dieron o las medidas con los que se pueden evitar.

1.2 ¿Existen documentos por los cuales se puedan regir los especialistas a la hora de elaborar un Plan de Seguridad?

Respuesta:
Para desarrollar un plan de seguridad es necesario tener en cuenta varios estándares de la seguridad de la información dentro de los que puedo mencionar los estándares ISO – 27001 e ISO – 27002 que sirven como guías de cómo se deben desarrollar los elementos que componen y facilitan la elaboración de un plan de seguridad. También existe una Metodología utilizada aquí en Cuba que es un documento complementario de la Metodología para el Diseño de un Sistema de Seguridad Informática desarrollado por la Dirección de Protección del Ministerio del Interior y que es la **Metodología para la Elaboración del Plan de Seguridad Informática**.

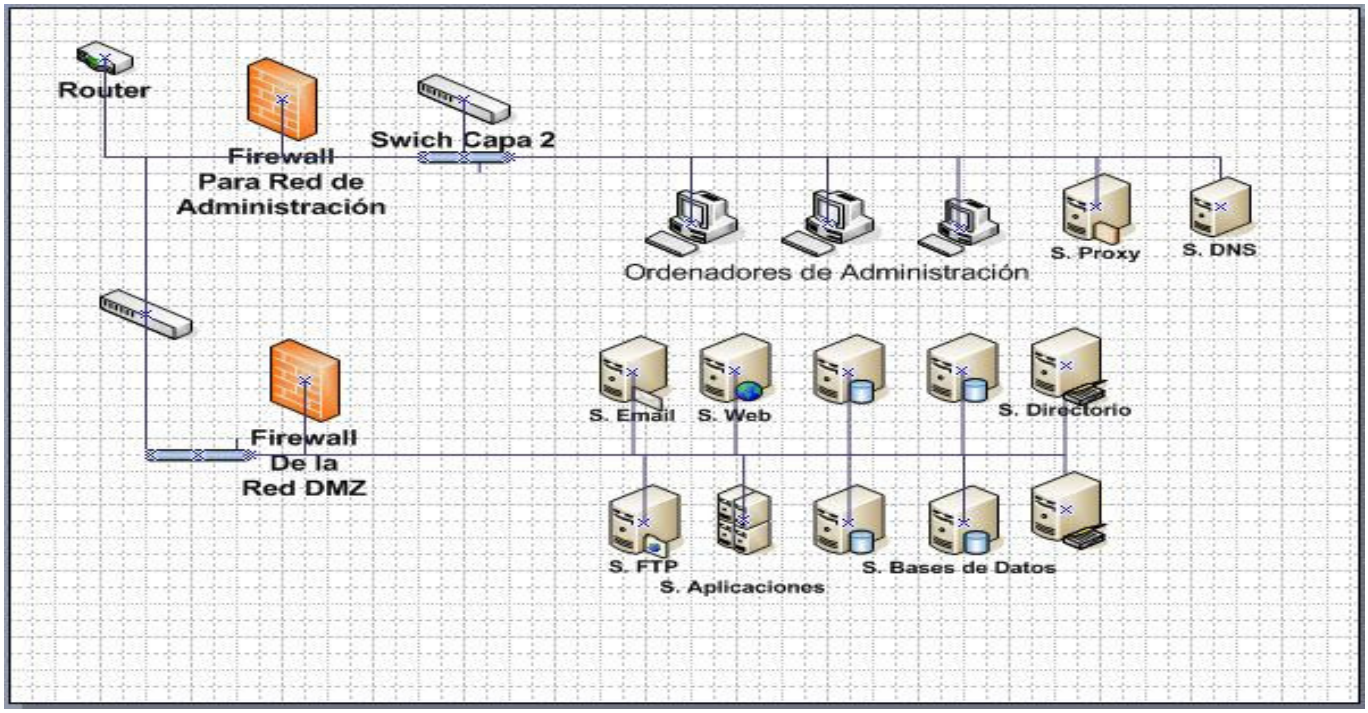
1.3 ¿Cómo saben cuáles son las aplicaciones que se deben instalar para controlar que el sistema funcione correctamente?

Respuesta:

No existe un documento que diga las aplicaciones que debe llevar un centro de datos, por ejemplo para poder controlar la red, el ancho de banda, los servicios que brinda, etc., sino que los fallos que tiene el mismo, los cuales pueden ser las caídas de uno o más servicios por la cantidad de usuarios que se conectan, se investiga para saber si existen aplicaciones que le den solución al problema, además de cual es la más factible; o simplemente se le asigna la tarea a un equipo especializado en implementar una solución para este fallo. Por lo que el sistema debe ser escalable y permitir la incorporación de nuevas aplicaciones.

Anexo # 2: Entrevista realizada al Ing. Dixan Mastrapa Torre. Administrador de Redes en el Nodo Central.

Para la entrevista realizada al compañero Dixan Mastrapa Torre se tenía como principal objetivo realizar y definir una estructura de red con todos sus componentes y que fuera capaz de responder eficientemente a las necesidades propias de un Centro de Datos. Para comenzar el debate le fue presentado al especialista un diagrama de red surgido del estudio intensivo de documentos en la Internet y bibliografía perteneciente al plan de estudio para la asignatura de Tele Informática en la Universidad de las Ciencias Informáticas. Después de exponer con detalles lo que se perseguía con el diagrama de red que se muestra a continuación, se le realizó un conjunto de preguntas al profesor.



2.1 ¿Con el diagrama de red mostrado se podrán alcanzar los objetivos que se persiguen?

Respuesta:
Ese diagrama presenta dificultades que influyen en la seguridad informática de los activos de las diferentes áreas del diagrama. El mayor problema radica en la ubicación lógica que se le da a los servidores de comunicación, de bases de datos y a las máquinas de administración.

2.2 ¿Explíquenos como debería estar estructurada una red de forma tal que garantice la máxima seguridad de los activos que contemple y a su vez pueda dar respuesta a las demandas de un Centro de Datos?

Respuesta:
Para que una red informática que, como la de un Centro de Datos, será accedida desde una red exterior pueda ser segura, tendrá que contar con una configuración de Firewall que solo permita el flujo de información autorizada para ambos sentidos. Todos los servidores que serán accedidos directamente desde la Internet deberán estar ubicados en una zona desmilitarizada (DMZ) y los servidores de bases de datos al igual que el resto de la red en otra zona diferente a la DMZ. Para conectarse a Internet se usará un Router WAN por sus características técnicas:

- Un Router WAN es un dispositivo que se usa para conectar dos redes donde al menos una de ella es del tipo área amplia (WAN). Dentro de sus ventajas se puede decir que presenta características avanzadas de Firewall y filtraje de contenido de la información que circula por él, presenta también múltiples opciones de balanceo de carga para un mayor ancho de banda total. En fin para en trafico que va a existir en un centro de datos es muy importante este tipo de Router.

Se deberá usar un Firewall por hardware para proteger la red de todo tipo de ataques dado las características técnicas que este dispositivo presenta:

- Un cortafuegos por hardware, es un dispositivo específico instalado en una red para levantar una defensa y proteger a la red del exterior. Su configuración es independiente de los sistemas operativos que corren en la red y por ser un dispositivo independiente, al reinstalar una máquina de

la red no lo afecta. En su interior es capaz de almacenar todo el tráfico de información que circula a través de él. Es capaz también de analizar paquetes de información y actúa mucho más rápido que un firewall por software. Como inconveniente solo se puede decir que es un producto muy caro para ser instalado en un lugar donde realmente no sea necesario tanta seguridad y eficiencia, generalmente en empresas pequeñas.

Para conectar los activos de la red de la zona donde no se encuentra la DMZ se usará un Switch Core capa tres por sus características técnicas:

- Un Switch modular LAN Capa 3 de alto rendimiento para aplicaciones Core en el campo soporta convergencia de voz, video y datos con calidad de Servicio (QoS), administración de ancho de banda, y Giga bit y Fast Ethernet de alta densidad. Este Switch protege la integridad de los datos en la red a través de funciones avanzadas de seguridad, respondiendo a los requerimientos empresariales más críticos del presente.

Core Layer, capa de núcleo, es literalmente la capa de núcleo de la red, esta es la parte más alta y se responsabiliza en puro transporte de mucho tráfico (de una manera muy rápida), es decir esta capa solo le interesa conmutar, por lo general los Router(s) de dicha capa, están conectados en fibra óptica u otro medio rápido, a veces Router(s) o sino unos switches.

Todo el flujo de la red quedará registrado mediante Log(s) en el Firewall por hardware. Dentro del diagrama explica también como conectar toda una red LAN del tamaño que se desee pero este aspecto no entraba dentro de los objetivos de la investigación.

Luego de la entrevista, el **Diagrama de Red** quedó conformado como se refleja en la Caracterización del Sistema en el **Capítulo 2,** al igual que los componentes que lo integrarán**.**

GLOSARIO

A

Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

Ataque activo: Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

Ataque pasivo: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo puede dar información importante sobre el sistema, así como permitir la aproximación a los datos que contiene.

Antivirus: Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominado malware).

B

Backups: Significado en español: Copia de seguridad. Es la copia total o parcial de información importante del disco duro, CD(s), bases de datos u otro medio de almacenamiento que se realiza en otro dispositivo de almacenamiento con el objetivo de restablecer los datos originales en caso de que se pierdan o destruyan.

Bytes: es la unidad fundamental de datos en los ordenadores personales, un conjunto de ocho bits **contiguos.**

Base de Datos: Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

C

Cuarentena: Proceso donde los productos de Software son sometidos a mecanismos de revisión y descontaminación en caso de estar contaminados. La duración de este proceso es determinada por los responsables de la actividad.

Contingencia: Posibilidad de que algo suceda. Lo que puede o no suceder.

D

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces se utiliza: información como sinónimo de datos.

Deadlock: Significado en español: Abrazo fatal. Ocurre cuando un conjunto de procesos está en estado de espera por recursos y nunca cambia de estado porque los recursos por los que espera están siendo utilizados por otros procesos en estado de espera.

Dominio: Es un nombre base que agrupa a un conjunto de equipos o dispositivos y que permite proporcionar nombres de equipos más fácilmente recordables en lugar de una dirección IP numérica.

F

Flooding: Tipo de ataque donde se activan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red para que nadie pueda utilizarla.

H

Hardware: es la parte física de un computador o de cualquier dispositivo electrónico.

Host: máquina conectada a una red con un nombre que la identifica, el hostname. La máquina puede ser una computadora, un dispositivo de red.

Hub: un dispositivo que se utiliza como punto de conexión entre los componentes de una red de área

local.

I

ID: identificador que se le da a un usuario del centro. Éste identificador es único en el sistema.

Incidente: Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

Invitado: La categoría de invitado le será asignada por defecto a todo usuario.

IP: Las direcciones IP (IP es un acrónimo para Internet Protocol) son un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

IPS: Sistema de Prevención de Intrusos.

IP-tables: Permite configurar un Firewall de forma que se tenga controlado que entra y que sale; es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.

L

Log(s): Registro oficial de eventos durante un período de tiempo en particular**.**

M

Modem (Modulador, Demodulador): Periférico que permite transmitir datos entre dos ordenadores a través de una línea telefónica.

MINBAS: Ministerio de la Industria Básica.

O

ONRM: Oficina Nacional de Recursos Minerales.

P

Password: Significado en español: clave o contraseña. Es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa. En sistemas multiusos, cada usuario debe incorporar su contraseña antes de que el ordenador responda a los comandos.
PC(s): ordenador(es) personal(es).

Privacidad: Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

Puertos: Un puerto es un número de 16 bits, empleado por un protocolo host a host para identificar a que protocolo del nivel superior o programa de aplicación se deben entregar los mensajes recibidos.

R

RFC (**Request For Comments**): Significado en español: Petición de comentarios. Es una serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet y experimentos similares. No todos los RFC(s) describen estándares de Internet pero todos los estándares Internet están escritos en forma de RFC(s). La serie de documentos RFC es inusual en cuanto los protocolos que describen son elaborados por la comunidad Internet que desarrolla e investiga, en contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como CCITT y ANSI.

S

Segmentos ASK: Acuse de recibo. En una comunicación entre computadoras, es un mensaje que se envía para confirmar que un mensaje o conjunto de ellos han llegado.

Segmentos SYN: Petición de conexión. Este segmento le dice al servidor que el cliente desea establecer una conexión cuando un programa pide conexión enviándole un segmento SYN.

SETUP: Es un programa de configuración grabado dentro del Chip del BIOS. Se lo conoce también como el CMOS-SETUP. A diferencia de las instrucciones de control propias del BIOS que son

inmodificables por el operador, el SETUP permite cambiar modos de transmisión y el reconocimiento o no de dispositivos en el PC.

Spoofing: En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.
Súper-usuarios: Categoría que se le da a un usuario que hace que tenga privilegios superiores a los usuarios comunes. Ejemplo: directores de empresas.

T

TCP: protocolo de transmisión de datos por la red; garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

Terabyte: Un Terabyte es una unidad de medida de almacenamiento informático cuyo símbolo es (**TB**) y es igual 1024 GB, aproximadamente un trillón de bytes.

U

UCI: Universidad de las Ciencias Informáticas.

W

WAN: Red de Área Amplia (Wide Area Network), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km.

Z

Zona Desmilitarizada o DMZ: es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.