ESCUELA POLITÉCNICA NACIONAL

CARRERA DE INGENIERÍA EN INFORMÁTICA

ANÁLISIS DE RIESGOS Y DISEÑO DE UN PLAN DE SEGURIDAD DE INFORMACIÓN PARA EL INSTITUTO GEOFÍSICO DE LA ESCUELA POLITÉCNICA NACIONAL

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN INFORMÁTICA MENCIÓN REDES

MANUEL RAÚL ANDRADE RAMOS

DIRECTOR: DR. ENRIQUE MAFLA, PHD

Quito, Marzo de 2006

DECLARACIÓN

Yo, Manuel Raúl Andrade Ramos, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mi derecho de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, su Reglamento y la normatividad institucional vigente.

_____

Manuel Raúl Andrade Ramos

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Manuel Raúl Andrade Ramos, bajo mi supervisión

_____

Dr. Enrique Mafla, PHD

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Mi agradecimiento es para los miembros de mi familia, los cuales me han sabido comprender y siempre han estado a mi lado para ayudarme, en especial mis padres que me apoyaron con su buen ánimo y motivación.

También agradezco a mi director de tesis por que ha sabido guiarme para que este proyecto de titulación sea realizado de manera óptima. También a todos los profesores de la Carrera de Ingeniería en Informática mención Redes, en especial a aquellos profesores que se esmeraron en presentar aspectos nuevos y prácticos de la ciencia y tecnología, y que con su acertada orientación, transmitieron aquellos conocimientos, que son muy útiles para la futura vida profesional.

Manuel Raúl Andrade Ramos

DEDICATORIA

Este proyecto de tesis dedico a mis padres quiénes han sido el apoyo más grande para la realización de trabajo. También dedico a mis profesores de la Escuela Politécnica Nacional, que me han sabido instruir y guiar hacia la consecución de la verdad.

Manuel Raúl Andrade Ramos

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

ANEXOS

RESUMEN

Frente a la necesidad de proteger los sistemas que manejan información delicada y sensitiva del Instituto Geofísico, el autor del presente proyecto, propuso llevar a cabo una evaluación de riesgos y, mediante ésta desarrollar un plan de mitigación de los mismos, utilizando la metodología OCTAVE-S[1], en la cual se resumen la mayoría de las normas y regulaciones internacionales sobre seguridad de información como la ISO 19977[2] y NIST[3], y se puede aplicar a pequeñas instituciones con menos de 100 personas en una red de datos con limitados recursos.

Primeramente se explican los 30 pasos de OCTAVE-S, como las actividades secuenciales a seguir, según se muestra de manera sintética en la hoja de ruta del método, luego de conformar el equipo de análisis, el cual llevar a cabo la evaluación, se comienzan a llevar a cabo entrevistas y reuniones para tomar datos que servirán para llenar las Hojas de Trabajo de OCTAVE-S. De esta forma se identificó el perfil de amenaza de los activos de información considerados críticos[4] y, posteriormente se determinó una aproximación cualitativa de la probabilidad de ocurrencia de eventos de ataque de las amenazas ya identificadas. Basados en el perfil de riesgo de activos críticos anterior, el equipo de evaluación realizó el análisis y selección de las áreas de práctica de seguridad más vulnerables. Para cada área considerada para mitigación se escogieron estrategias de protección, y se desarrollaron actividades de mitigación correspondientes para ubicarlas dentro del plan de seguridad.

Para los activo críticos se seleccionaron áreas de mitigación de acuerdo al tipo de vulnerabilidad característica; así de mayor a menor criticalidad, el Sistema de Información Sísmico y Volcánico, SISV, se considera que deben mejorar el área de Gestión de Seguridad, esto significa que el plan de seguridad compromete a

[1] Cfr. En la Bibliografía ALBERTS, Christopher, et al. , "Lista de documentos guía del método OCTAVE-S", en v03_guidelines v1.doc, ob.cit., página.11, dice: "OCTAVE-S por sus siglas en Inglés, es una metodología operacional y práctica para evaluar los riesgos de seguridad de información, y elaborar los planes de mitigación de estos últimos. OCTAVE-Small se refiere a la aplicación de la evaluación en pequeñas organizaciones. "

[2] Cfr. Bibliografía sobre NORMA ISO 17799

[3] Cfr. Bibliografía sobre DOCUMENTOS NIST.

[4] Activos de información críticos son aquellos bienes de información sin los cuales la institución no puede llevar a cabo su misión. Cfr. Anexo A: Glosario de términos OCTAVE-S.

todos aquellos encargados de gestionar y administrar estos sistemas en actividades concretas de mitigación del riesgo de estos valiosos sistemas. Después se analizó el activo crítico de Información de Usuarios, Informes y Documental, IUIID, para el cual se sugiere el mismo tratamiento que para el SISV, pues es su producto. Al personal de Tecnología de Información en conjunto con el Personal de Monitoreo Volcánico, TI + PMV, como activo de información humano, se lo considera vulnerable en cuanto se necesita mejorar la Gestión de Sistemas y Red, por ello se proponen actividades concretas para mejorar la administración, el control y monitoreo de la red de datos. Para el Centro de Información y Respaldos, CIR, se necesita desarrollar actividades de mitigación principalmente en aquello que se refiere a las áreas de mitigación relacionadas con la Seguridad Física, puesto que son vulnerables a las inclemencias del tiempo, el deterioro y destrucción por cualquier causa. Los Computadores Personales, PCs, que son las herramientas de trabajo principal de los científicos y de todo el personal técnico, deben mejorar en topología e interconectividad, para lo cual se han propuesto actividades de mitigación en el área de Diseño y Arquitectura de la Seguridad.

Con las actividades del Plan de Mitigación que proponen mejoras al área de Diseño y Arquitectura de la Seguridad, se desarrolló el Sistema Tecnológico de Seguridad.

Es notable la articulación de la evaluación del riesgo, con el desarrollo del plan de mitigación, puesto que con aquello encontrado y seleccionado en el análisis del perfil de riesgo, se determinaron actividades concretas para mitigarlo.

Las recomendaciones como culminación del presente Proyecto de Ingeniería sugieren implementar, controlar y monitorear las actividades sugeridas en el Plan de Seguridad planteado por el autor de la presente investigación

En caso de aprobarse el sistema tecnológico de seguridad, se pueden integrar las políticas reactivas de las máquinas y personas, con una mejor prevención. Entendiéndose la prevención no sólo a nivel de parcheo de vulnerabilidades en línea, sino también la prevención en las acciones de las personas como un avance en la gestión que comprometa a todos los miembros de la organización en la difícil tarea de la seguridad de datos.

1. CAPITULO UNO: INTRODUCCIÓN

1.1 CONTEXTO DEL INSTITUTO GEOFÍSICO

1.1.1 GENERALIDADES DEL INSTITUTO GEOFÍSICO

El Instituto Geofísico de la Escuela Politécnica Nacional[5] constituye el principal centro de Investigación existente en el país para el diagnóstico y la vigilancia de los peligros sísmicos y volcánicos, los cuales pueden causar gran impacto en la población, en los proyectos de inversión y en el entorno natural.

El IGEPN está encargado de la vigilancia y detección de los movimientos sísmicos y erupciones ocurridas, mediante la red nacional de sismógrafos de movimientos sísmicos, RENSIG y la red de observatorios volcánicos, ROVIG, respectivamente; además está encargado de la preparación de mapas de peligro y emitir alertas tempranas para que las autoridades y la población tomen a tiempo medidas preventivas.

1.1.2 MISIÓN, VISIÓN Y OBJETIVOS DEL INSTITUTO GEOFÍSICO

1.1.2.1 Misión

Contribuir a la reducción del impacto negativo de los fenómenos sísmicos y volcánicos en el Ecuador, a través de la vigilancia permanente, la investigación científica, el desarrollo y la aplicación tecnológicos promoviendo la creación de una cultura de prevención.

1.1.2.2 Visión

El Instituto Geofísico será una organización líder en la vigilancia, la investigación científica y el desarrollo tecnológico relacionados a los fenómenos sísmicos y volcánicos, que incide en políticas de Estado para el mejoramiento de la seguridad individual y colectiva frente a estos fenómenos y a la sustentabilidad del desarrollo del país, a través de la reducción de sus vulnerabilidades.

---

[5] Las siglas son IGEPN

1.1.2.3 Objetivos generales del Instituto Geofísico

- Reducción del impacto de desastres sísmicos y volcánicos.
- Difusión de los resultados de la vigilancia e investigación de la actividad sísmica y volcánica y comunicación de recomendaciones a entidades locales y público en general
- Proveer servicios de asesoría en vulcanología y sismología en el Ecuador.
- Emitir pronósticos y alertas a las autoridades y población.

1.1.2.4 Objetivos estratégicos del Instituto Geofísico

- Comprender el volcanismo ecuatoriano para reducir el impacto de las erupciones.
- Comprender la sismicidad tectónica y volcánica en el Ecuador para reducir el impacto de los terremotos y las erupciones.
- Realizar la investigación científica fundamental para crear las bases necesarias para una efectiva reducción del riesgo.
- Desarrollar y disponer de las herramientas tecnológicas para generar y mantener el flujo de información necesaria para el monitoreo e interpretación sísmica y volcánica.
- Fortalecer la capacidad de gestión interna y de consecución de fondos externos.

1.1.3 ESTRUCTURA ORGANIZACIONAL DEL INSTITUTO GEOFÍSICO

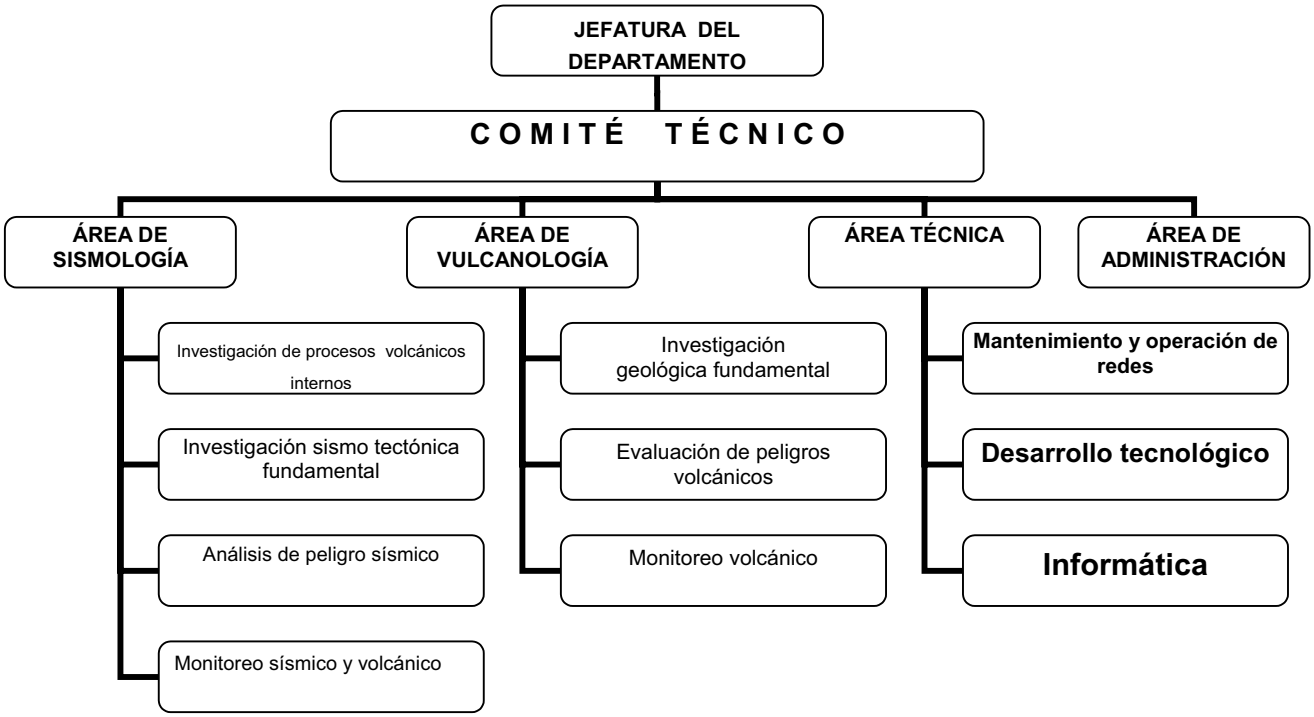


Figura 1.- Organigrama del Instituto Geofísico

Como se puede observar en el organigrama de la Figura 1, El Instituto Geofísico está dividido jerárquicamente de acuerdo con sus niveles de responsabilidad. El Jefe de Departamento, es quien coordina el Comité Técnico. Este Comité está conformado por los jefes de todas las áreas. Y a su vez, cada jefe dirige el personal asignado para cada función según su posición dentro de la propia área y jerarquía.

1.1.3.1 Distribución del personal por áreas

1.1.3.1.1 Departamento de Geofísica

El Instituto Geofísico es orgánicamente dependiente del Departamento de Geofísica de la Escuela Politécnica Nacional. El Departamento de Geofísica está bajo la dirección del Sr. Rector de la Escuela Politécnica Nacional quien es su representante legal. Como se puede ver en el Organigrama de la Figura 1, existen Áreas de Vulcanología, Sismología, Técnica y Administrativa. Las Áreas

que llevan a cabo funciones en directa relación con la misión del Instituto Geofísico son las de Vulcanología y Sismología. Y su personal se puede ver listado en el Cuadro 1:

ÁREA DE VULCANOLOGÍA	
CIENTÍFICOS	ESTUDIANTES, TESISTAS Y PERSONAL DE APOYO
PhD. Pablo Samaniego, Jefe de área PhD. Minard Hall MSc. Patricia Mothes Ing. Patricio Ramón Ing. Gorki Ruiz MSc. Daniel Andrade	David Rivero Diego Barba Roberto Vásconez

ÁREA DE SISMOLOGÍA	
CIENTÍFICOS	ESTUDIANTES, TESISTAS Y PERSONAL DE APOYO
MSc. Alexandra Alvarado, Jefe de área Geol. Alexander García Geol. Indira Molina Ing. Liliana Troncoso Ing. Mario Ruiz Ing. Mónica Segovia MSc. Pablo Palacios Sr. José Egred	Guillermo Viracucha Jorge Bustillos Pablo Cobacango Christian Correa Rolando Guadalupe Dayanara Hinojosa Johana León Diana Ramírez Paúl Silva Gabriela Taipe Mercedes Taipe Sandro Vaca Silvia Vallejo Patricio Verdesoto

ÁREA TÉCNICA	
CIENTÍFICOS	ESTUDIANTES, TESISTAS Y PERSONAL DE APOYO
MSc. Wilson Enríquez, Jefe de Área Instrumentación Tlgo. Vinicio Cáceres Ing. Mayra Vaca Fis. Omar Marcillo Tlgo Eddy Pinajota Tlgo Cristian Cisneros Ing. Cristina Ramos Ing. Richard Jaramillo	Santiago Arellano Andrés Cadena Myriam Paredes Jamie Chalán Jorge Tello Carlos Zambrano Edison Maldonado Darwin Panchi Miguel Ángel Quijia Vinicio Valencia Cristina Charro
SUBÁREA DE TECNOLOGÍA DE INFORMACIÓN (TI)	
Fis. Jorge Aguilar, Jefe de la SubÁrea Ing. Marisol León Desarrollo de Sistemas Tlgo. Edwin Peralta, Administrador de la Red.	

Cuadro 1.- El personal por áreas en el Instituto Geofísico

La denominada Área Técnica tiene las funciones de proveer el soporte de mantenimiento de instrumentación, electrónica a los equipos de monitoreo sísmico y volcánico. Dentro de esta área se considera incluido al personal de

Tecnología de Información, o **TI**, como una subárea de apoyo en todo lo concerniente a sistemas y redes de computación.

Las funciones del personal de Tecnología de Información, fundamentalmente son las de prestar soporte de sistemas y mantenimiento de software y hardware. También proveen de apoyo al desarrollo de sistemas de aplicación, y mantienen al día las configuraciones de los sistemas operativos.

1.1.4 SISTEMA DE INFORMACIÓN DEL INSTITUTO GEOFÍSICO

El Instituto Geofísico tiene implementado un sistema de información sísmica y volcánica con dos redes de vigilancia instrumental, la Red Nacional de Sismógrafos, RENSIG[6] y la Red Nacional de Observatorios Volcánicos, ROVIG[7] . RENSIG tiene instaladas más de 30 estaciones sísmicas de período corto en la parte centro y norte del país y en las Islas Galápagos y por su parte ROVIG consta de varios observatorios volcánicos. Las dos redes tienen una vigilancia permanente durante 24h00 al día y los 365 días del año, por lo cual tiene una respuesta inmediata de los eventos.

Las redes alimentadoras de datos RENSIG Y ROVIG en sí mismas no son objeto del análisis del presente Proyecto, ya que son redes externas a la red de información fuera del alcance del análisis a realizarse.

En cuanto al hardware existente, la red de datos consta de un computador en el cual reside el servidor LINUX, computadores personales, un Switch, Hubs o concentradores como se muestra en la Figura 2 y como se describe en detalle en el Anexo C: Inventario de hardware y software.

---

[6] Mayor detalle sobre estas redes se encuentra en http://www.igepn.edu.ec/instrumentación/sismica/red_rensig.htm.com

[7] http://www.igepn.edu.ec/instrumentación/vulcanología/vulcanología.htm

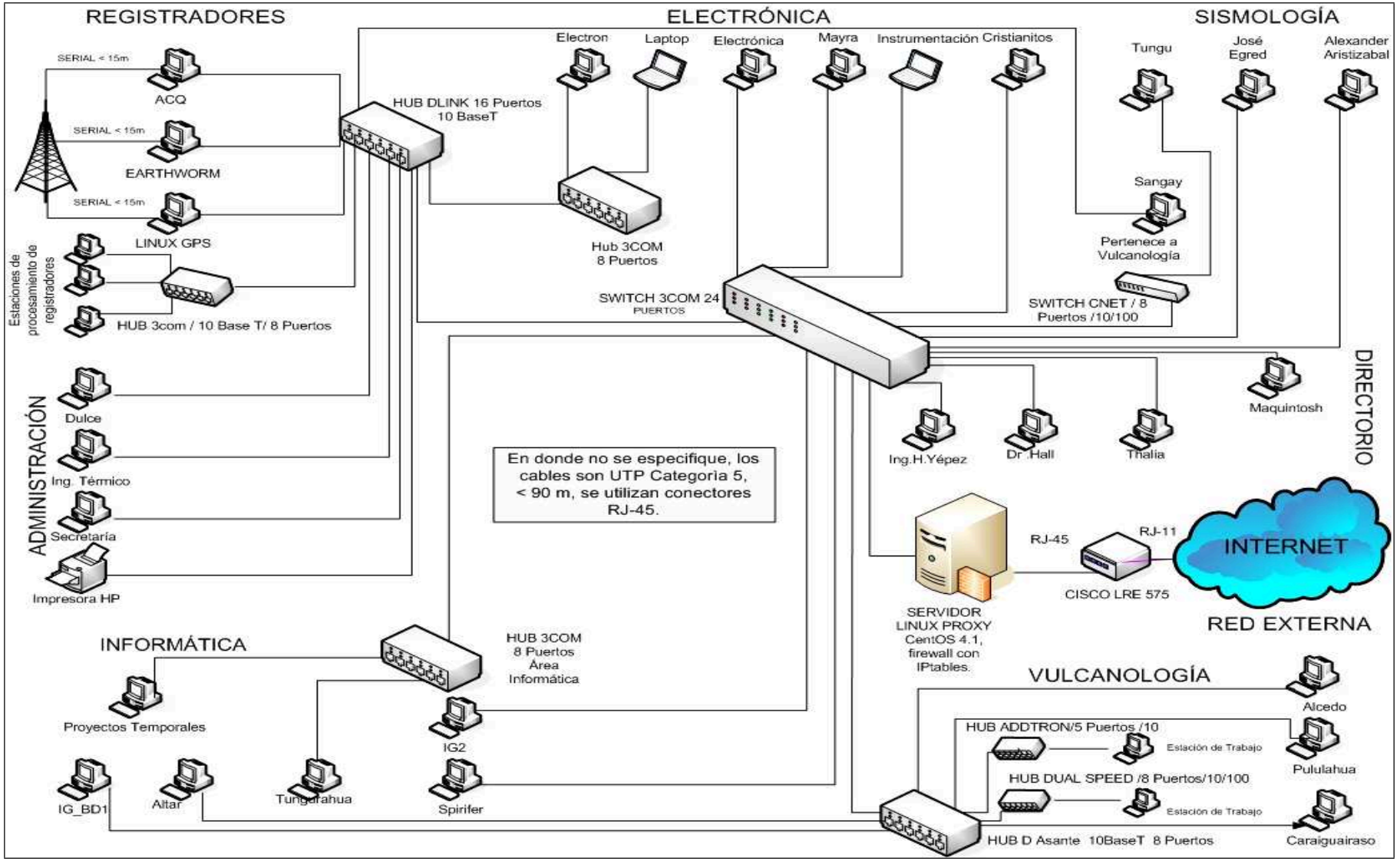


Figura 2 : Topología actual de la red de información del Instituto Geofísico[8]

[8] La Figura 2 fue desarrollada por el autor del presente proyecto, basado en el inventario de hardware proporcionado por el personal de Tecnología de Información del Instituto Geofísico. Cfr. Anexo C: Inventario de hardware y software.

La topología actual de la red es de tipo **estrella**. Como se puede ver en la Figura 2, todas las estaciones confluyen hacia un único Switch 3Com Baseline, y desde éste la información se distribuye por medio de Hubs o concentradores de 8 y 16 puertos. Hay un único punto de entrada/salida a Internet por medio del dispositivo Cisco LRE 575 que está enlazado directamente con el Servidor Linux Proxy con IPTables. Este único Servidor Linux con CentOS 4.1 sirve para administrar toda la red, y gestionar la seguridad de los datos de manera muy incipiente.

En cuanto al software[9], la mayoría de estaciones funciona con Windows Xp, aunque hay una estación que funciona con Linux como sistema operativo. Hay que notar que los computadores en la Sala de Registradores son sólo de lectura, ya que reciben los datos en línea de RENSIG y ROVIG. Los programas Earthworm, ACQ, IRIS y Marslite son utilitarios que permiten la transformación de los datos de monitoreo en imágenes y datos a ser leídos por los científicos, e inclusive las imágenes generadas por Earthworm pueden ser vistas directamente en la página Web y son actualizadas de manera periódica[10].

1.1.4.1 Flujo de datos del Sistema de Información del Instituto Geofísico

Como se muestra en la Figura 3, los registros de monitoreo de RENSIG y ROVIG son recibidos en computadores que funcionan como estaciones de trabajo. Luego estos registros se procesan en el sistema de información sísmica y volcánica SISV[11] y son leídos e interpretados por los científicos, cuyos resultados sirven para elaborar informes documentales y reportes científicos o IUIID. Los documentos oficiales seleccionados y aprobados de IUIID se envían a la página Web del instituto geofísico, en http: //www.igepn.edu.ec, para su difusión por Internet.

Las investigaciones más relevantes se guardan en el Centro de Información y Respaldos, CIR, en las instalaciones de la Sala de Lectura.

---

[9] Ver Anexo C: Inventario de hardware y software

[10] http://69.65.157.50/heli/sgram/index.html

[11] La primera versión del SISV fue desarrollada por CARVAJAL PÉREZ, Luis, CHAMORRO LUCERO, Juan, "Sistema de Información Sísmico y Volcánico para el Instituto Geofísico de la Escuela Politécnica Nacional", Proyecto de Titulación, Código 010029, Director: Ing. Víctor Aguilar, Facultad de Ingeniería de Sistemas, EPN, Quito, 1993.

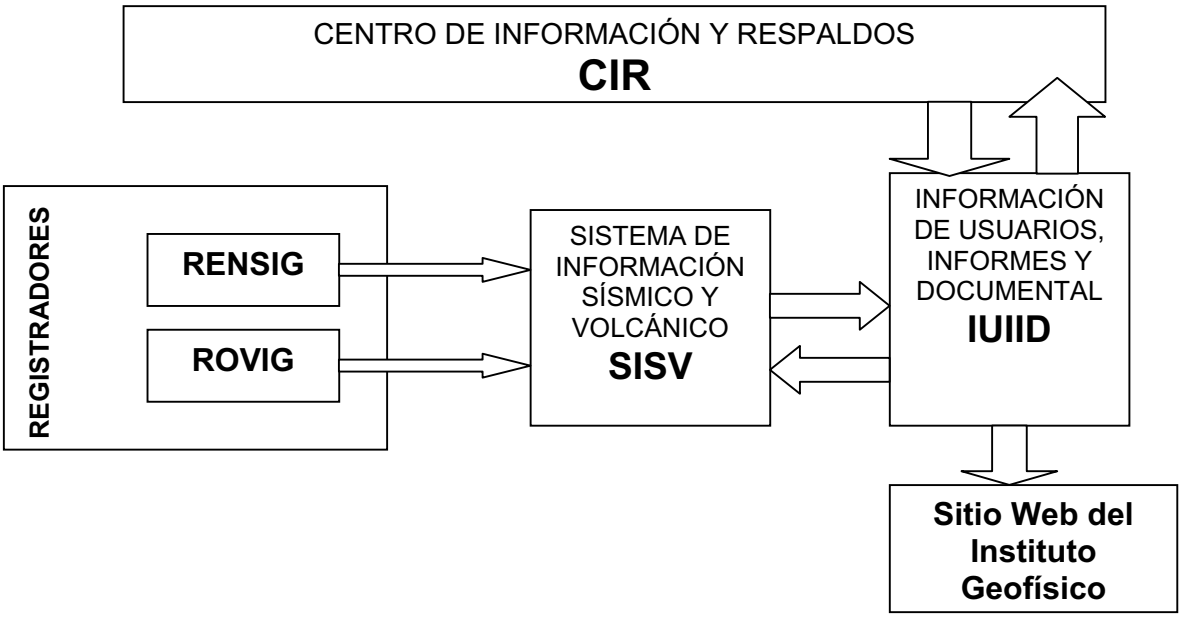


Figura 3.- El Sistema de Información del Instituto Geofísico

1.1.5 MARCO LEGAL DE LA INFORMACIÓN GEOESPACIAL DEL INSTITUTO GEOFÍSICO.

Según se puede ver en el Cuadro 2, dentro el marco de la Constitución de la República, se circunscriben las diferentes leyes y principios del derecho a los cuales está sometida la gestión y administración de la información del Instituto Geofísico. Dentro de este marco general, están los principios jurídicos sobre la seguridad nacional, la moral pública y los derechos de las personas a recibir información pública que sirva para garantizar el desarrollo de su vida y la protección de sus bienes. La garantía del Estado sobre el acceso a este tipo de información pública está respaldada por las Leyes de Transparencia y Acceso a la Información Pública, la Ley de Defensa del Consumidor[12]. Esto significa que toda persona natural tiene derecho a solicitar y recibir los reportes oficiales veraces, actualizados y oportunos[13] del Instituto Geofísico, y éstos deben tener una amplia difusión en la población por el mismo hecho que garantizan la seguridad de su vida y de sus bienes[14].

[12] Art. 4 Ley Orgánica de Defensa del Consumidor No 2000-21 Registro Oficial No. 116 del 10 Julio 2000. Cfr. Constitución Política de la República del Ecuador, Art. 23. lit.7b.
[13] Ley Orgánica de Transparencia y Acceso a la Información Pública, Art. 1.

[14] Art. 81 de la Constitución de la República del Ecuador.

Asimismo, los Artículos 9 y10 de la Ley de Transparencia y Acceso a la Información Pública**,** establecen las responsabilidades de aquellos que están encargados de ella, y establece la obligación de manejar esta información de manera profesional y técnica.

En cuanto al respeto de la **propiedad intelectual** se considera el respeto a los **derechos de autor**, y están incluidas las bases de datos estadísticas y espaciales[15]. Las elaboraciones e interpretaciones científicas de los datos geoespaciales también están dentro de esta categoría; lo cual significa que toda persona que participe en el acceso a información geoespacial específica, debe respetar los derechos de propiedad intelectual de los autores de reportes en donde haya habido elaboración intelectual. La mención de los autores es obligatoria en caso de que se utilicen sus ideas para cualquier elaboración científica, y en caso de que se haga alguna publicación con fines comerciales, se les debe pagar los derechos correspondientes.[16].

Por otra parte, se han hecho reformas al Código Penal[17], para definir el Delito Informático cuando se violenten los principios de seguridad de la información[18], estableciéndose penas y multas para el manejo doloso de información digital pública. Aunque este delito generalmente no se da en este tipo de información, la norma previene contra la utilización alarmista, la modificación no autorizada y la apropiación indebida.

Según la Ley de Comercio Electrónico[19], el proveedor de ISP y de WebHosting del Instituto Geofísico, deslinda su responsabilidad sobre la precisión, y calidad del contenido de la información que le envían para publicarse en la página Web. No obstante el proveedor de ISP se responsabiliza de mantener la integridad del mensaje original, y no añadir, ni cambiar nada a la información oficial enviada por el personal del Instituto Geofísico.

---

[15] En la Ley de Propiedad Intelectual, Art. 8. Literal b, se dice que entre las obras protegidas están: "Las bases de datos, …que sean creaciones intelectuales" y el lit h) "Ilustraciones, gráficos, mapas y diseños relativos a la geografía, la topografía, y en general a la ciencia"

[16] Cfr. Ley de Propiedad Intelectual, Artículos 19 al 25. Caso contrario constituye un plagio intelectual.

[17] Código Penal, Art. 262

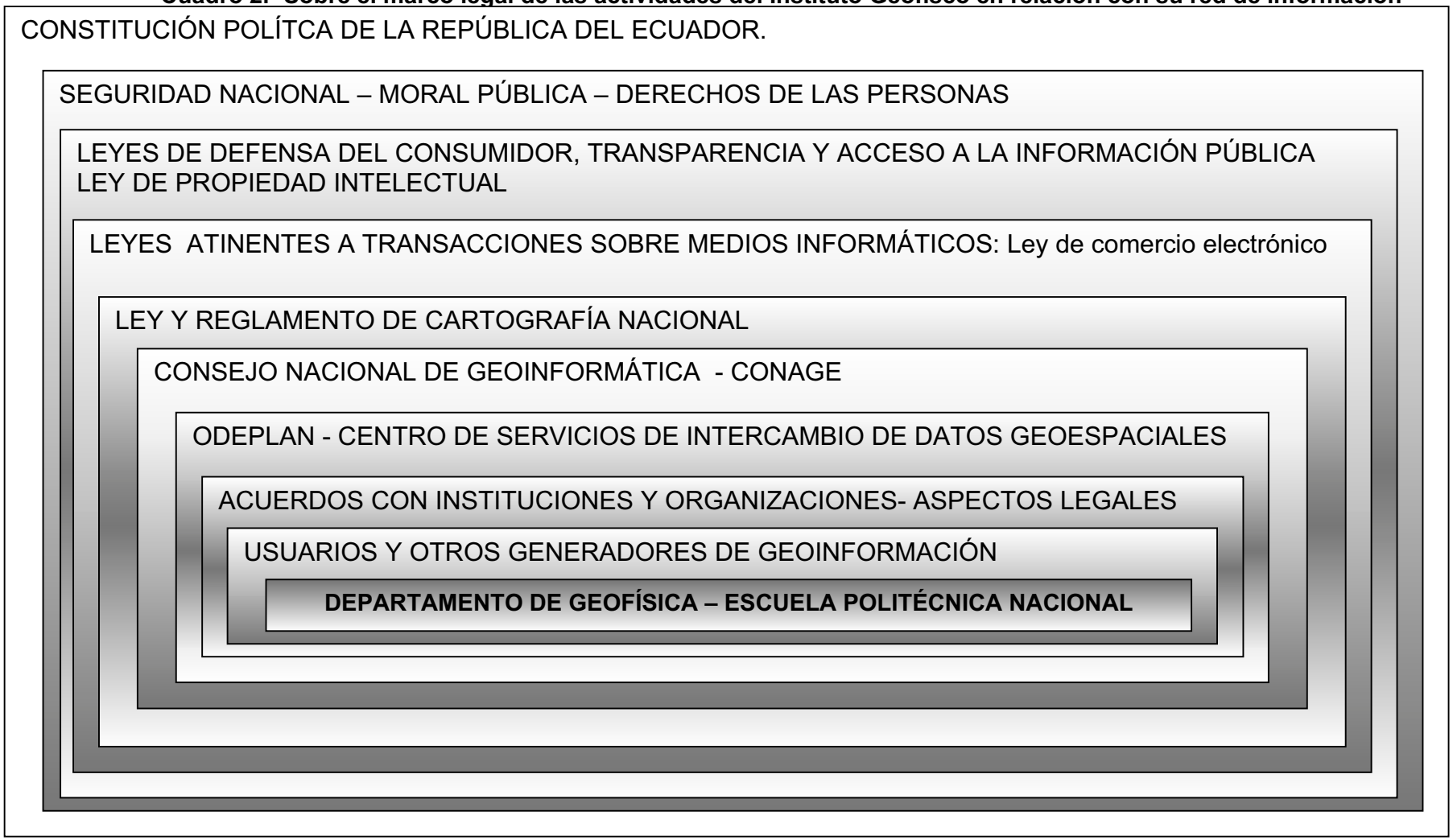
[18] Atinente a la " Ley de Comercio Electrónico ", Art. 58.- A continuación del artículo 202, del Código Penal, se tipifica el delito informático.

[19] Reglamento a la Ley de Comercio Electrónico, art. 8

En lo atinente a la aplicación de la Ley y del Reglamento de Cartografía Nacional[20], que norma el intercambio de datos geoespaciales, la información que maneja el Instituto Geofísico está regulada por el Consejo Nacional de Geoinformática que será explicado en el siguiente literal.

[20] Art. 22 de la Ley de Cartografía Nacional Registro Oficial No. 643, julio 17, 1978 y el CAPITULO VI del Reglamento de la Ley de la Cartografía Nacional Registro Oficial No.828, Diciembre 9, 1991.

Cuadro 2.- Sobre el marco legal de las actividades del Instituto Geofísco en relación con su red de información [21]



[21] Fuente: Elaborado por el autor del presente proyecto.

1.1.6 LA INFORMACIÓN DEL INSTITUTO GEOFÍSICO DENTRO DE LA INFRAESTRUCTURA DE DATOS GEOESPACIALES

Según se puede apreciar en el Cuadro 3, la información geoespacial se divide en pública y no pública. El Consejo Nacional de Geoinformática[22] ha determinado que la información geoespacial se la maneje en tres componentes

1) La Información Fundamental Nacional en las bases de datos geoespaciales.
2) El ODEPLAN, o Centro de Servicios de Intercambio de Datos. Además están incluídos los acuerdos entre las diferentes instituciones.
3) Los usuarios y otros generadores de geoinformación. El Instituto Geofísico está inscrito en este componente.

La Información Geoespacial Fundamental Nacional consta de dos niveles [23]:

El primer nivel que lo maneja el Instituto Geográfico Militar, al interpretar y procesar las fotografías aéreas, referencias fotogeométricas, modelos de terreno y elevación, bases topográficas, y nombres geográficos.

El segundo nivel de geoinformación es el nivel de datos y aplicaciones que los administra el CLIRSEN[24], que es la institución que provee la información satelital y de recursos naturales para estudios de hidrología, suelos, geología, vegetación, cobertura, catastros, etc

De los niveles anteriores se alimenta el ODEPLAN, o el Centro de Servicios e Intercambio de Datos Geoespaciales, que es la institución que gestiona los datos fundamentales en dos aspectos:

- **Administrativo.-** Se definen los integrantes de la infraestructura, su organización, su base legal, derechos de autor, costos de información, registro de productores de información geográfica – cartográfica.
- **Técnico.-** Se encarga de definir y normar estándares de producción de información geográfica y protocolos de intercambio de datos. Los organismos de planificación del Estado deben determinar la cantidad,

---

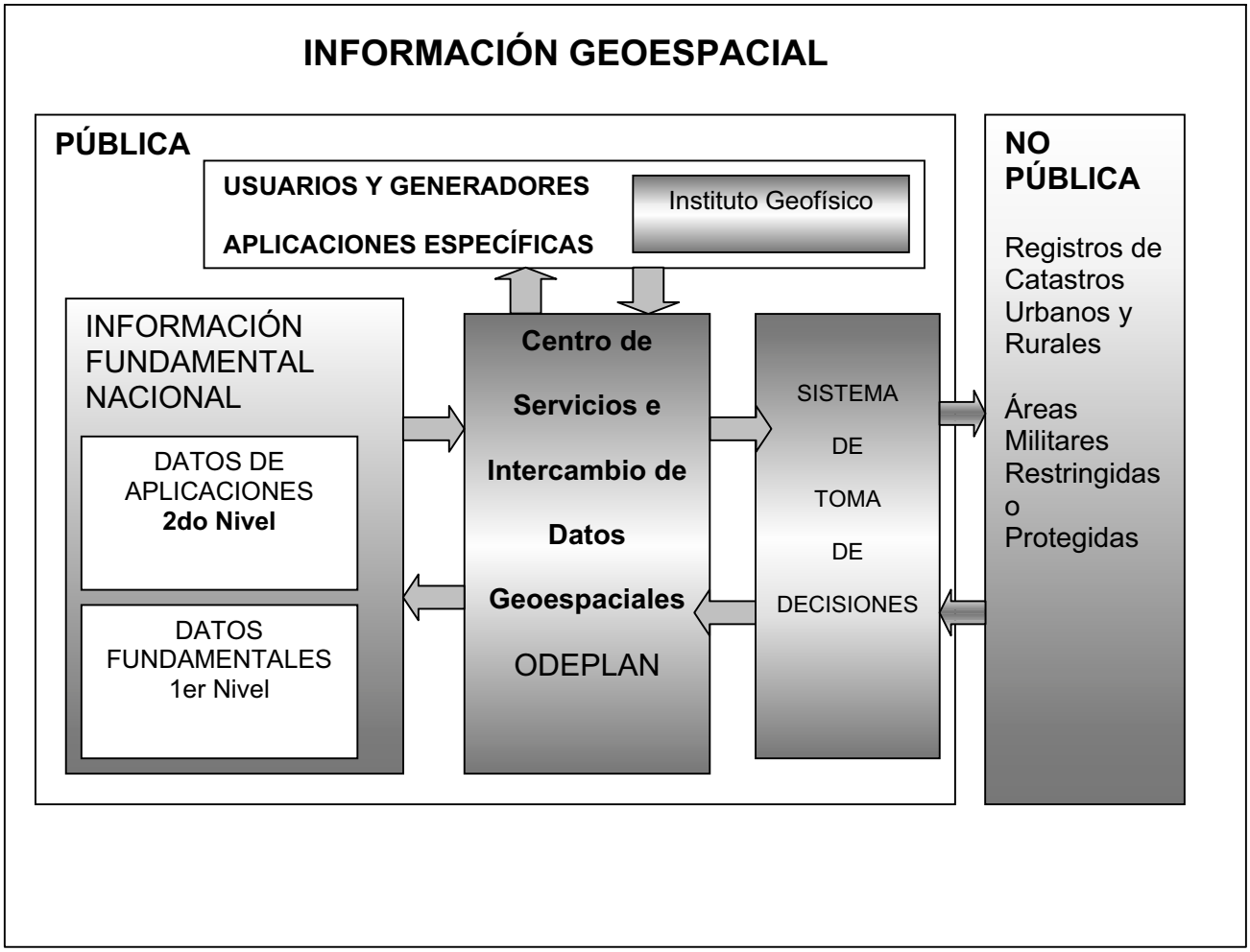
[22] SALAZAR MARTÍNEZ, Rodolfo, Implementación de la infraestructura nacional de datos geoespaciales de Ecuador, Junio 26, 2003 en **www.igm.gov.ec/articulos/geoinformatica2.htm**

[23] Se ha hecho una adaptación y resumen de SALAZAR MARTÍNEZ, Rodolfo, Implementación de la infraestructura nacional de datos geoespaciales de Ecuador, Junio 26, 2003 en **www.igm.gov.ec/articulos/geoinformatica1.htm**

[24] CLIRSEN es el Centro de Levantamiento Integrado de Recursos Naturales por Sensores Remotos.

calidad y localización de la información requerida para la ejecución de los planes de desarrollo nacional.

El Instituto Geofísico maneja la información pública en lo que son las aplicaciones específicas, usuarios y generadores de geoinformación. Como se ve en Cuadro 3, el Instituto Geofísico intercambia información con el ODEPLAN.



Cuadro 3.- El Instituto Geofísico en relación con los niveles de intercambio de información geoespacial [25]

[25] El Cuadro 3 se ha adaptado del cuadro de niveles de intercambio de datos geoespaciales de SALAZAR, MARTÍNEZ, Rodolfo,op.cit., en http://www.igm.gov.ec/articulos/geoinformatica3.htm

1.2 PLANTEAMIENTO DEL PROBLEMA

El Instituto Geofísico posee sistemas de monitoreo que alimentan su red interna con grandes volúmenes de información sísmica, lahárica, pluviométrica, volcánica, gráfica, de instrumentación y documental, que se almacenan en línea y de forma continua en algunos casos, cuyo manejo requiere de respaldo frecuente y constante depuración; sin embargo esta información delicada y sensitiva actualmente no está adecuadamente protegida y es muy vulnerable de ataques contra su seguridad.

Debido a lo cual, el Comité Técnico del Instituto Geofísico bajo la dirección de su Jefe de Departamento, considera la necesidad una revisión integral de la seguridad de información dentro de sus instalaciones. Frente a este requerimiento, el autor del presente proyecto de titulación bajo la asesoría de su profesor director, propuso a los encargados de la gestión de la seguridad de datos en el Instituto Geofísico, aplicar la metodología OCTAVE-S[26] para realizar el análisis de riesgos a los que está expuesta la delicada y sensitiva información que manejan y el consiguiente desarrollo del plan de mitigación asociado.

1.3 OBJETIVO GENERAL

El objetivo del presente proyecto de titulación es el desarrollar un plan de seguridad y mitigación de riesgos para la red de información interna del Instituto Geofísico y de esta manera, mejorar y desarrollar actividades para proteger sus activos de información y muy en particular, sus activos críticos[27].

[26] Igual que la Nota 1.

[27] Activos es una palabra tomada de la Contabilidad Financiera, como aquel bien que sirve para el desarrollo de la actividad u operación del negocio. Si el activo es crítico, su ausencia compromete el alcanzar la misión de la organización. Cfr. Ver concepto de Activos Críticos en el Anexo A: Glosario de términos OCTAVE-S.

1.3.1 OBJETIVOS ESPECÍFICOS

a) Evaluar los riesgos a los cuales está expuesta la información del Instituto Geofísico.
b) Basándose en los resultados del anterior análisis de riesgos , definir una política de gestión que contemple las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados, y así reducir al mínimo su potencialidad o posibles perjuicios.
c) Recomendar las acciones y herramientas necesarias para poner en marcha un sistema de seguridad de información para el Instituto Geofísico.
d) Identificar por niveles de importancia relativa los bienes de información, y proponer acciones para protegerlos.
e) Entrenar al personal de Tecnología de Información, sobre las políticas o las áreas de "buena práctica" de seguridad que son el "deber-ser" de la seguridad.
f) Mejorar la presentación de proyectos de diseño de seguridad de información a las autoridades y funcionarios, y de esta forma facilitar las relaciones y contratación de empresas externas.
g) Mejorar la presentación de proyectos de diseño de seguridad de información a las autoridades y funcionarios, para mejorar la toma de decisiones y la agilitar la gestión presupuestaria en esta materia.

1.4 METODOLOGÍA

Se ha escogido OCTAVE-S, por las siguientes razones [28] que justifican la conveniencia de aplicarlo en el Instituto Geofísico:

- Resume la mayoría de las normas y regulaciones sobre seguridad de información internacionales como la ISO 19977[29] y NIST[30] en una sola síntesis operacional y práctica.

---

[28] Estas características se hallan en: ALBERTS, et.al., "Visión general de OCTAVE", ob.cit., pp. 38-68 en http://www.cert.org/archive/pdf/octave_Alt_Exec_Session.pdf

- Es autodirigido, es decir, recurre al personal de la misma organización, quienes al conocer internamente los problemas de la misma, pueden enfocar el análisis en los puntos más críticos, y de esta manera no desperdiciar recursos ni tiempo en estudios innecesarios y muy costosos.

- Se adapta a pequeñas instituciones con menos de 100 personas cuya red de datos posee limitados recursos.

- Es una metodología de evaluación integral, ya que considera el mayor número posible de factores[31] que intervienen en la seguridad; donde los riesgos de gestión se integran con los riesgos tecnológicos; es decir, el método toma en cuenta los elementos tecnológicos de la seguridad, en relación con la organización, y sus puntos más débiles o vulnerables se los evalúa en relación con los demás factores que afectan la seguridad de la información.

- OCTAVE-S está enfocado hacia asuntos estratégicos de la organización; esto significa, que sus activos críticos de información, puntales de la misión y objetivos de la misma, se hallen resguardados.

Como se ha escogido OCTAVE-S para llevar a cabo el diseño del plan de seguridad de datos en el Instituto Geofísico, a continuación se describe una síntesis de su proceso y la Hoja de Ruta que se debe seguir en la aplicación.

1.4.1 EL PROCESO DE OCTAVE-S

El proceso de OCTAVE-S fundamentalmente tiene dos partes:

---

[29] Cfr. Notas a pie de página 2 y 3.

[30] Cfr. Bibliografía sobre DOCUMENTOS NIST

[31] Más adelante se tratará la relación entre las políticas, normas y procedimientos en OCTAVE-S aplicado al Instituto Geofísico en el Literal 3.1

a) Identificar el perfil de riesgo, es decir, las amenazas y vulnerabilidades que atañen a los activos críticos[32], tanto desde el punto de vista organizacional como tecnológico.

b) Análisis del riesgo encontrado en el literal anterior, para el desarrollo de estrategias y el plan de mitigación.

Como se puede ver de manera sinóptica en la Figura 4, el proceso comienza con una Fase de Preparación para constituir el equipo de análisis y realizar las entrevistas iniciales. Una vez constituido el equipo de análisis, éste lleva a cabo una serie progresiva de talleres de trabajo para identificar el perfil de riesgo de los activos críticos, desde el punto de vista Organizacional para la Fase 1 y Tecnológico para la Fase 2. Posteriormente el equipo de análisis desarrolla las estrategias y planes de mitigación en la Fase 3 basado en el análisis del riesgo encontrado en el proceso anterior.

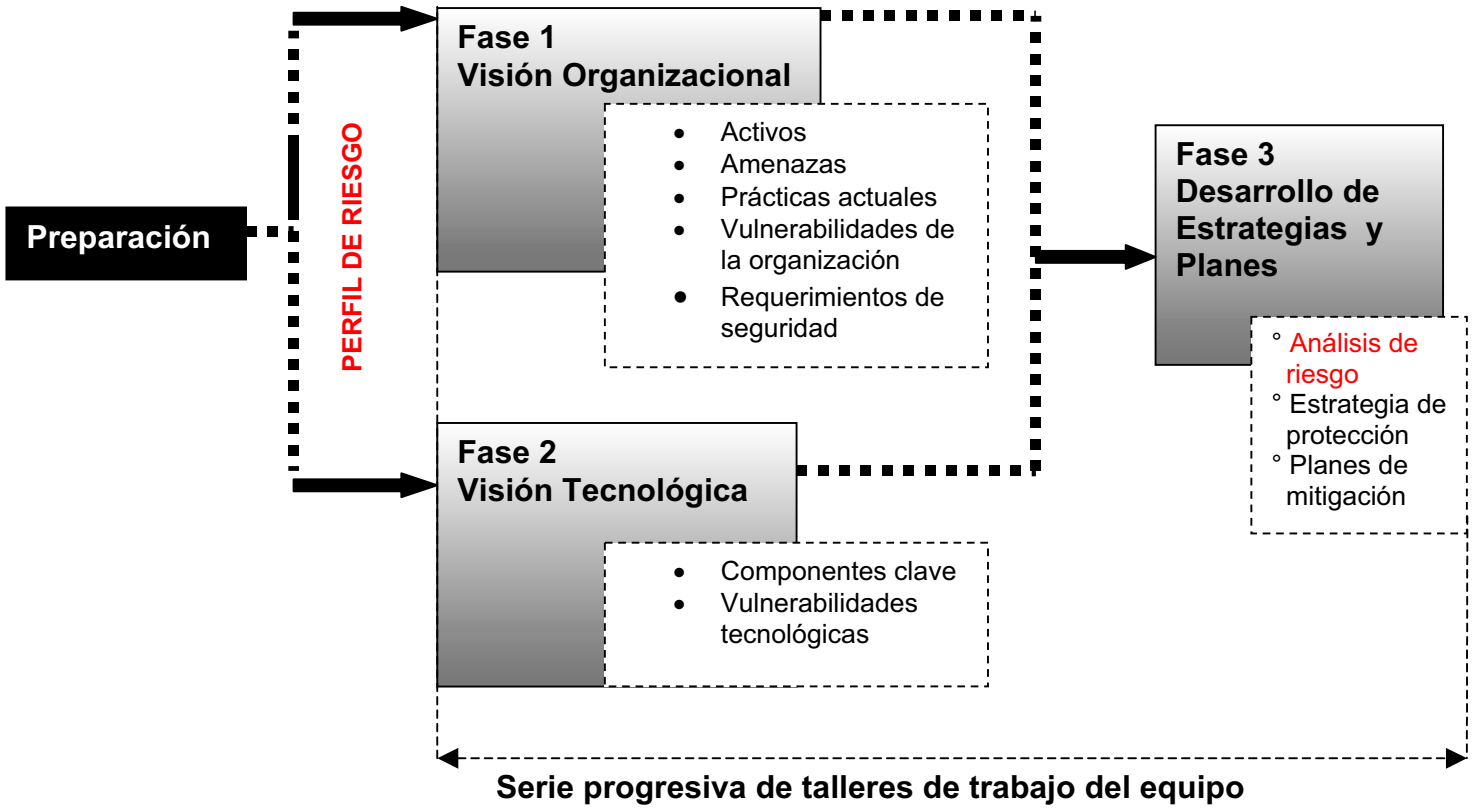


Figura 4.- El proceso de OCTAVE-S[33]

[32] Igual que Nota 27.
[33] ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, "Visión general de OCTAVE", Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 2003, página 50, http://www.cert.org/archive/pdf/octave_Alt_Exec_Session.pdf

1.4.2 HOJA DE RUTA

La serie progresiva de talleres de trabajo que el equipo de análisis debe llevar a cabo, sigue la **Hoja de Ruta**[34]**,** en la cual prácticamente se siguen los Pasos 1 al 30 de manera sistemática. En cada Paso se definen actividades a ser llenadas en las Hojas de Trabajo correspondientes. Las Hojas de Trabajo de OCTAVE-S son altamente estructuradas y de fácil utilización. Los pasos se siguen de manera secuencial, y esto no obsta que se vuelva sobre datos de pasos anteriores o que estos ayuden a los posteriores, o viceversa.

[34] Cfr. La Hoja de Ruta ha sido elaborada por el autor del presente proyecto de titulación basado en el detalle de las actividades en el Anexo D: Descripción de las actividades de OCTAVE-S.

FASE PREPARATORIA: Conformación del equipo de análisis, entrevistas previas.

Fase Uno	Proceso	Actividad	Paso
Construir Perfiles de Amenaza de Activos de Información.	**S1**: Identificar la Información Organizacional	**S1.1:** Establecer los Criterios de Evaluación del Impacto	1
		S1.2: Identificar Activos de Información de la Organización.	2
		S1.3: Evaluar Prácticas de Seguridad Organizacional	3, 4
	S2: Crear Perfiles de Amenaza	**S2.1:** Seleccionar los Activos Críticos	5, 6, 7, 8, 9
		S2.2: Identificar los Requerimientos de Seguridad para Activos Críticos	10, 11
		S2.3: Identificar las Amenazas a los Activos Críticos	12, 13, 14, 15, 16

Fase Dos	Proceso	Actividad	Paso
Identificar Vulnerabilidades en la Infraestructura	**S3:** Examinar Infraestructura Computacional en relación con los Activos Críticos.	**S3.1:** Examinar Rutas de Acceso	17, 18
		S3.2: Analizar Procesos relacionados con la Tecnología.	19, 20, 21

Fase Tres	Proceso	Actividad	Paso
Desarrollar Estrategias y Planes de Seguridad.	**S4**: Identificar y Analizar Riesgos.	**S4.1:** Evaluar Impacto de las Amenazas	22
		S4.2: Establecer Criterio de Evaluación de la Probabilidad	23
		S4.3: Evaluar Probabilidad de Amenaza	24
	S5: Desarrollar Estrategias de Protección y Planes de Mitigación.	**S5.1:** Describir Estrategia de Protección Actual	25
		S5.2: Seleccionar Enfoques de Mitigación	26, 27
		S5.3: Desarrollar Planes de Mitigación del Riesgo	28
		S5.4: Identificar Cambios en la Estrategia de Protección	29
		S5.5: Identificar los Pasos Siguientes	30

DESPUÉS DE LA EVALUACIÓN: Aprobación, implementación, puesta en marcha

Cuadro 4.- Hoja de ruta de las Fases, procesos y pasos de OCTAVE-S

1.4.2.1 Fase Preparatoria

En la fase preparatoria de OCTAVE-S, se conforma el **equipo de análisis,** el cual está compuesto de 3 a 5 personas, y entre ellas debe haber miembros pertenecientes a la organización objeto de evaluación, para que ésta sea autodirigida, lo cual no obsta que haya colaboración de personal externo. De preferencia el equipo debe ser un grupo multidisciplinario, lo cual enriquece su visión y perspectiva.

1.4.2.2 Fase Uno

Como se observa en la Hoja de Ruta en el Cuadro 4 y la Figura 4, la Fase Uno está enmarcada en una visión organizacional o de gestión. Dentro de esta fase, el equipo de análisis primero según el **Paso 1,** determina los Criterios de Evaluación de Impacto**,** que serán usados más tarde para hacer una aproximación del grado de gravedad de una amenaza (alto, medio o bajo) en caso de que ésta se produzca sobre las áreas de confianza de los usuarios, financiera, seguridad de las personas, productividad y multas o penalizaciones legales. Posteriormente, como el ataque a la seguridad se lo realiza sobre los bienes de información que sirven de medios para llevar a cabo la misión de la organización y mantener la continuidad de las operaciones, según indica el **Paso 2,** se deben identificar los activos de información considerados de más relevancia. Seguidamente y según el **Paso 3,** se evalúa el cómo las 15 Áreas de Práctica de Seguridad de Datos OCTAVE-S están siendo actualmente observadas dentro de la organización[35], y de esta forma tener un primer contacto con aquellas prácticas con mayores falencias o que estén más descuidadas**.** Así, en el **Paso 3a** se marca el grado en el cual la organización sigue el principio de seguridad, y en el **Paso 3b** se identifica lo que la organización está o no haciendo bien respecto a esa área de práctica de seguridad. Como indica el **Paso 4,** se marca luego el estado de semáforo **V**erde, **R**ojo o **A**marillo con las letras **V**, **R** o **A**, respectivamente según

[35] En el literal 3.1 se tratará el papel de las Áreas de Práctica de Seguridad dentro de la planeación de mitigación de riesgos. Cfr. Anexo A: Glosario de términos OCTAVE-S. En cada Área de Práctica están concentradas y sintetizadas bajo un mismo nombre, las prácticas más afines y similares entre ellas. Así por ejemplo, el Área de Seguridad Física incluye el Control de Acceso de las personas, la correcta gestión del inventario de los equipos, la protección anti-desastres, etc.

se considere la atención que hay que poner en cada área en un primer vistazo, El semáforo en Rojo es un indicativo que la seguridad en esa área se la lleva de manera muy deficiente. El estado de semáforo Amarillo indica un problema no tan grave, y el semáforo en Verde nos indica que todo va aceptablemente bien. Si alguna práctica de seguridad no es aplicable para la organización, se marca la casilla correspondiente. Luego, como indica el **Paso 5,** se seleccionan de entre los activos de información, basados en su importancia relativa para la organización, aquellos tres a cinco activos considerados como críticos, los cuales serán analizados en profundidad**.** Después, según el **Paso 6,** se identifica cuál es el nombre del sistema crítico, y como indica el **Paso 7,** la razón para que sea considerado como tal; se identifica en el **Paso 8**, quién usa y quién es responsable de este sistema, y también cuáles activos están relacionados con él, como se determina en el **Paso 9.** Posteriormente, según el **Paso 10,** el equipo ubica los requerimientos de seguridad para cada activo crítico, sea éste la disponibilidad, la confidencialidad o la integridad, y se determina cuál de estos últimos es el más importante, siguiendo el **Paso 11.** Para comenzar a determinar el perfil de riesgo, como indica el **Paso 12,** se comienza con escribir en una casilla el nombre del activo crítico a analizar, y se lo ubica en una matriz que interseca a un árbol de amenazas. Las ramas estos árboles delinean las características de su actor de amenaza. Puede el actor tener acceso físico, interno o externo, y cuyo motivo puede ser deliberado o accidental. Para cada amenaza se sigue la **lógica de la relación causa-efecto**, al identificar un **actor como causa de ella y una consecuencia de su ataque**, que puede ser revelación, modificación, pérdida o interrupción del flujo de información. El contexto de amenaza se identifica según el **Paso 13,** primero con el determinar cuáles actores son de mayor consideración para el sistema que se trate en la respectiva rama, y siguiendo el **Paso 14,** se determina posteriormente la fuerza del motivo de ataque, y qué confianza se tiene en esta estimación, y, finalmente, como indica el **Paso 15,** se identifica el historial de ocurrencias de ataques en el pasado y una estimación de cuán precisos son estos datos**.** Después, y siguiendo el **Paso 16,** en las áreas de interés se dan ejemplos concretos de cómo el actor ha atacado dentro de su rama de amenaza**.**

1.4.2.3 Fase Dos

Tanto la Fase Uno como la Fase Dos están concatenadas e integradas. Como se puede apreciar en el Cuadro 4 y Figura 4, en la Fase Dos, el equipo de análisis enfocándose dentro de una visión tecnológica, conduce una revisión a nivel general de la infraestructura computacional de la organización, y la relaciona con los encargados de su mantenimiento. Así se evalúa cómo ha sido considerada la seguridad de la infraestructura computacional por la organización. Según el **Paso 17,** el equipo de análisis primero identifica los sistemas más cercanamente relacionados con el activo crítico considerado principal, que es llamado el sistema de interés**.** Luego, y siguiendo el **Paso 18a,** se identifican los componentes clave de la red que son parte o están relacionados con el sistema de interés.

Posteriormente y según el **Paso 18b,** se determinan los puntos de acceso intermedio, es decir cuáles componentes en la red son usados para transmitir información desde el sistema de interés hacia los diferentes usuarios**.**

Después, como indica el **Paso 18c,** se consideran desde cuáles clases de componentes de red pueden acceder las personas al sistema de interés**.**

Además según el **Paso 18d,** se determina la localización del almacenamiento de información y se identifican en cuáles clases de componentes está almacenada la información para propósitos de respaldo. Luego en el **Paso 18d,** se identifican cuáles otros sistemas, aplicaciones u otra clase de componentes pueden ser utilizados para acceder al sistema de interés. Según el **Paso 19a,** se marca el camino para cada clase seleccionada en los pasos 18a - 18e para identificar cuáles clases de componentes de red están relacionados con uno o más activos críticos**.** Después en el **Paso 19b,** se relacionan los activos críticos con cada clase**.** Además como indica el **Paso 20,** se determina la responsabilidad de mantener y asegurar cada clase de componente**.** Finalmente en esta Fase Dos, y siguiendo el **Paso 21,** se identifica el grado de protección cuando se configura y mantiene cada clase de componente, y si se conoce este hecho por medios formales o no.

1.4.2.4 Fase Tres

Para entrar en la Fase Tres, se supone que las Fases Uno y Dos ya han sido completadas. Según se puede ver en la Hoja de Ruta del Cuadro 4, en la Fase Tres se comienza según indica el **Paso 22,** con el registro de los Criterios de Evaluación del Impacto ya obtenidos en **el Paso 1** para identificar el potencial daño a la seguridad en las áreas ya indicadas en los diferentes árboles de amenaza, en los correspondientes cuadros en las Hojas de Trabajo de Perfil de Riesgo de cada activo crítico

Seguidamente en el **Paso 23,** el equipo determina la probabilidad de un evento de amenaza como alta, media o baja de acuerdo con el número de ocurrencias registradas en el historial, respecto a un periodo de tiempo**.** Después según el **Paso 24,** se llenan con esta probabilidad las casillas correspondientes en las matrices de perfil de riesgo para cada activo crítico. La más alta probabilidad de ocurrencia de una amenaza servirá para considerar un área de práctica de seguridad para un activo crítico como candidata para mitigación**.**

En el **Paso 25** se analizan las estrategias actuales de protección en aquellas áreas de práctica consideradas más críticas, y de acuerdo con la realidad de las actividades de mitigación propuestas en grados de mayor a menor seguimiento.

En el **Paso 26** se transfieren los estados de semáforo de las áreas de práctica de seguridad en las Hojas de Perfil de Riesgo, y con la intersección de la matriz, amenazas, probabilidad , se marcan con un círculo aquellas áreas de práctica que se las considere para mitigación. No importa si se marcan dos o más actividades para una misma rama de amenaza, pues se trata de un primer indicador a ser utilizado en seguida. Es por ello que según el **Paso 27** se definen[36] criterios para determinar si una determinada práctica es candidata para mitigación; en el caso que para una misma rama de amenaza la probabilidad de ocurrencia sea alta, el impacto sea también alto, y tenga un mayor número de círculos marcados, se considerará esa rama para mitigación, caso contrario se marcará la casilla diferir la mitigación o aceptar como está siendo llevada

[36] Lo novedoso de esta metodología es el ubicar en la matriz de perfil de riesgo, horizontalmente las ramas de árbol de amenaza para cada activo crítico, y verticalmente las áreas de práctica de seguridad. Si se cruzan con una alta probabilidad de ocurrencia, se marcan para mitigación. De esta forma se tiene una **visión de conjunto, o sinopsis, del perfil de riesgo.**

actualmente. En el **Paso 28 se proponen las actividades de mitigación para las áreas de práctica de seguridad** seleccionadas, se explica la razón para haberlas seleccionado, quién es asignado como responsable para llevarlas a cabo, y qué soporte adicional se necesita para implementarlas. Luego en el **Paso 29,** se identifican y transfieren aquellos cambios en la estrategia de protección que se anotan como actividades en el plan de mitigación. En realidad el plan de mitigación se enfoca hacia aquellas estrategias de protección que necesitan ser creadas o mejoradas, que se transforman en actividades de mitigación para aquellas áreas de práctica de seguridad que se hallen más vulnerables. Finalmente, según el **Paso 30,** se elabora una Hoja de Trabajo de los Pasos Siguientes, y ésta incluye recomendaciones de qué acciones son inmediatas y cuándo se sugiere realizar la siguiente evaluación.

En cualquiera de las fases, el equipo puede elaborar sus recomendaciones de mejora y marcar los puntos importantes de práctica de seguridad en relación con las actividades pertinentes de evaluación ya realizadas.

1.5 ALCANCE DE LA EVALUACIÓN

- El ámbito de esta evaluación se limita a la red de datos **interna** del IGEPN, por lo tanto la evaluación OCTAVE-S no se realizará sobre las redes de estaciones de monitoreo RENSIG y ROVIG.

- Además se debe precisar que la evaluación que se hará en el presente proyecto con el método OCTAVE-S **no** constituye una auditoría informática; en realidad esta evaluación se limita solamente a los procesos de identificación y análisis de riesgos de información, y mediante este análisis, se pretende desarrollar un **plan de seguridad informática.** En el Cuadro 4 se pueden ver de manera resumida, las diferencias entre OCTAVE-S y la auditoría informática.

OCTAVE-S	AUDITORÍA INFORMÁTICA[37]
Evaluación organizacional o de gestión.	Evaluación sistemática.
Evaluación y planeación de la seguridad	Evaluación de la totalidad del sistema de información.
Enfoque en las prácticas de seguridad	Enfoque más en la tecnología que en la organización en sí.
Establece comunicación entre tecnología y gestión en la organización..	La tecnología se utiliza para evaluar los sistemas de información de la organización.
Va hacia asuntos estratégicos de seguridad de datos.	Se enfoca más hacia asuntos tácticos de posicionamiento en el mercado.
Es autodirigida por miembros de la misma organización.	Es liderada por expertos de fuera de la organización.
Es operacional, ya que analiza no la operación en sí, sino los procesos que tienen que ver con esa operación.	Analiza la operación en sí y sus procesos, por medio de pruebas sustantivas: métricas y benchmarking.
Es pro-activa frente a las vulnerabilidades.	Es generalmente más reactiva que proactiva a las vulnerabilidades.
Analiza perfiles de riesgo basados en análisis de vulnerabilidades de los activos críticos seleccionados.	Evalúa el sistema de información en su totalidad desde sus entradas, procedimientos, controles, archivos, seguridad y salidas de información. No solo activos críticos, sino todos los activos y sus sistemas relacionados.
La evaluación sirve para elaborar estrategias de protección y planes de mitigación del riesgo de seguridad.	Una auditoría informática sirve para la toma de decisiones gerenciales.

Cuadro 5.- Análisis de las diferencias entre OCTAVE-S y auditoría informática

Puede colegirse del Cuadro 5, que la metodología OCTAVE-S, puede servir de apoyo o ser instrumento para una auditoría informática.

Además se debe puntualizar que la aprobación, puesta en marcha del plan de mitigación, la revisión de la evaluación, las pruebas e implementación de las actividades del plan de seguridad están fuera del alcance del presente proyecto de titulación, puesto que es el propio Instituto Geofísico quien se encarga de llevarlas a cabo[38].

[37] CEVALLOS, Diego, "Guía de Estudios: Auditoría de Sistemas de Información, Maestría CA", Universidad Tecnológica Equinoccial, Quito, Marzo 2003, páginas 12 y siguientes.

[38] La evaluación se encuentra dentro del marco de la gestión de riesgos, según se puede ver en el Anexo A: Glosario de términos OCTAVE-S. La evaluación de riesgos consta de los procesos de identificación, análisis y planeación de mitigación los mismos. La gestión de riesgos incluye además de la evaluación, los procesos de implementar, monitorear, controlar los planes de mitigación desarrollados.

2. CAPITULO DOS: EVALUACIÓN DEL RIESGO

En este capítulo, luego de conformar el equipo de análisis en la Fase Preparatoria, se siguen los Pasos 1 al 21 de la evaluación, hasta completar las Fases Uno y Dos. Para cada Fase se siguen las actividades [39]correspondientes a cada una, y se llenan sus correspondientes Hojas de Trabajo[40].

2.1 FASE PREPARATORIA: CONFORMACIÓN DEL EQUIPO DE EVALUACIÓN

El Jefe del Departamento, MSc. Hugo Yepez, ha mostrado mucho interés en el desarrollo del presente proyecto; pues podría constituirse en un valioso apoyo al Plan Informático del Instituto Geofísico, de ser éste aprobado por el Comité Técnico. La participación del Jefe de Departamento y los Jefes de Área ha sido sustancial, puesto que bajo su supervisión y asesoría técnica, se ha puesto en marcha la evaluación. El equipo está conformado por los miembros descritos en el Cuadro 6.

Miembros	Función en la Evaluación
Ing. Marisol León	Ingeniera informática encargada del desarrollo de sistemas, es quien provee la mayor parte de la información al equipo de evaluación
Tlgo. Edwin Peralta	Administrador de la Red del IGEPN
Sr. Manuel Andrade	Tesista de la Carrera de Ingeniería Informática, quien utiliza los resultado del método OCTAVE-S para el desarrollo del presente proyecto de ingeniería.
Fis. Jorge Aguilar	Máster en Geofísica, supervisa de manera activa la evaluación.

Cuadro 6.- Los miembros del Equipo de Evaluación

[39] Anexo D: Descripción de las actividades de OCTAVE-S.
[40] Anexo E: Hojas de Trabajo

2.2 RIESGOS DE GESTIÓN

Básicamente este tipo de riesgo se refiere a la evaluación desde el punto de vista organizacional, que comprende la Fase Uno de la Figura 4.
A continuación se describen los resultados de la serie de talleres de trabajo:

2.2.1 FASE UNO: CONSTRUIR PERFILES DE AMENAZA DE ACTIVOS

Esta fase está desarrollada según las actividades de los pasos 1 al 16. Los resultados de estas Hojas de Trabajo[41] se describen a continuación:

2.2.1.1 Proceso S1: Identificar Información Organizacional

2.2.1.1.1 Actividad S1.1 Establecer Criterios de Evaluación de Impacto

Paso 1

Se definieron los rangos de potencial impacto, (alto, medio o bajo), en el Instituto Geofísico de las amenazas a la seguridad de datos en las áreas de confianza de los usuarios, financiera, seguridad de las personas, productividad y de multas o penalizaciones legales:

- **Confianza de los usuarios**

  El Instituto Geofísico goza de prestigio ampliamente reconocido por la seriedad de sus informes. Los gobiernos seccionales, los municipios de todo el Ecuador tienen gran confianza en la información que éste emite.

  Según el Instituto Geofísico un porcentaje mayor al 30% de caída de credibilidad frente a la opinión pública significaría un serio problema que podría ser irreversible. Esta área es considerada de posible y potencial alto impacto sobre el Instituto Geofísico.

[41] Anexo E: Hojas de Trabajo.

- **Financiera**

  El presupuesto del Instituto Geofísico está incluido en presupuesto general de la Escuela Politécnica Nacional, con las asignaciones fijas anuales del Estado Ecuatoriano. Este presupuesto incluye un 2% de margen para cambios inesperados en costos operativos y un margen de 5% para cambios en ingresos totales[42] , tomando en cuenta que el manejo directo de esos fondos está fuera del alcance de la propia gestión. Además se debe notar que muchos ingresos económicos provienen de donaciones o convenios con instituciones nacionales e internacionales, las cuáles han desembolsado estos recursos gracias a que confían en el prestigio y seriedad del Instituto Geofísico, y por lo tanto tendría mayor relación con el potencial impacto del área de confianza de los usuarios. Es por ello que esta área se la considera de bajo potencial impacto.

- **Seguridad de las personas**

  En realidad la información del IGEPN es de vital importancia para la seguridad de las personas; sin embargo **El ámbito de análisis del presente Proyecto de Titulación se refiere a la seguridad de la información dentro de la red del Instituto Geofísico, y no atañe directamente a la seguridad de las personas en sí.** Es por ello que en general no se lo considera de alto impacto, en general es de bajo impacto.

- **Productividad**

  Se estima que casi todo el personal trabaja en el peor de los casos, hasta unas 24 horas adicionales posteriores al periodo crítico[43] para recuperar el tiempo perdido por invasiones de virus o los gastos en tiempo para reinstalar sistemas operativos, vacunar con antivirus, poner parches al software, instalar programas antitroyanos, configurar el servidor de correo en Linux, etc. El potencial impacto de una amenaza en esta área se considera de alto valor.

---

[42] SIGEF, Departamento financiero EPN, presupuesto anual 2003-2004

[43] Según los datos proporcionados por el Administrador de Red, se estima una pérdida de 24 horas trabajo por mes debido a la inseguridad. Las instalaciones de programas antivirus y antispamming suelen hacerse en las horas en las cuales el personal no está laborando, para evitar que la pérdida de tiempo de trabajo en horas se multiplique por cada estación inactiva.

- **Multas y penalizaciones legales**

  Las licencias de software están cubiertas en su totalidad y nunca ha habido demandas de las empresas proveedoras. No se han tenido demandas de otras empresas o instituciones, tampoco de los proveedores de programas de software, ni del ISP. El potencial impacto de esta área es relativamente bajo.

2.2.1.1.2 Actividad S1.2 Identificar Activos de Información del Instituto Geofísico

Paso 2

Se toma como punto de partida para identificar los activos de información, el conocimiento y experiencia que tiene sobre la red de datos el personal de Tecnología de Información. Hay que notar que la mayoría de miembros de Tecnología de Información forman parte del equipo de evaluación. Además se considera el volumen[44] que manejan los sistemas y su grado de importancia relativa para identificar a un determinado bien como activo de información.

Activos de Información

A continuación se describen sus características más importantes:

- **El Sistema de Información Sísmica y Volcánica, SISV** constituye el principal activo del IGEPN, tanto por el volumen que maneja, como por la importancia que tiene esta información para la misión del Instituto Geofísico[45].

[44] Anexo B: Cuadros de volumen de información

[45] Anexo B: Cuadros de volumen de información, los cuales son parte del Proyecto de Desarrollo Informático del Instituto Geofísico, desarrollado por el personal de Tecnología de Información en Marzo de 2005.

- **La Información de Usuarios, Informes y Documental IUIID** que procesan la información SISV y obtienen informes, documentales y reportes científicos.

- **Centro de Información y Respaldos, CIR.** Es el activo de backups, mapas, bandas de monitoreo, videos de respaldo de las investigaciones más relevantes útiles para las presentes y futuras investigaciones en el área geofísica.

- Para el presente análisis también se identifican a las personas consideradas más relevantes para la seguridad de los sistemas, como verdaderos activos de información: Los científicos que controlan e interpretan los datos del monitoreo; como también los técnicos electrónicos que resuelven los problemas de hardware para los usuarios; el Administrador de Red son considerados valiosos para la seguridad de la información que manejan; sobre todo **el personal de Tecnología de Información en conjunto con el Personal de Monitoreo, TI + PMV,** constituye el activo más importante de recursos humanos relacionados con la seguridad de la información.

- **El sitio Web del Instituto Geofísico**, que reside en el Servidor de la empresa proveedora del ISP, AccessRAM MEGADATOS y es actualizada por el Webmaster[46], siempre que se disponga de información nueva. Generalmente cada semana se la actualiza con los informes elaborados por el científico de turno y por el encargado de monitoreo sísmico, y diariamente, si hay informes de los volcanes que así lo ameriten por ser eventos de consideración. Los informes que se publican en la página Web son parte esencial del servicio a la comunidad. Todo lo que se envía a la página Web debe ser aprobado previamente por los jefes de las áreas de Sismología y Vulcanología.

[46] Webmaster es la persona que hace cambios o actualiza la página Web, estas acciones se realizan vía el servicio de File Transfer Protocol, FTP.

- **El servidor de correo interno del Instituto Geofísico**, residente en la misma estación del Servidor Linux. El correo interno tiene un enlace en la página Web http:/www.igepn.edu.ec al correo interno en http://69.65.128.42/cgi-bin/openwebmail/openwebmail.pl. El manejo de las contraseñas de correo interno lo gestiona el Administrador de Red. Todo el personal dispone de una cuenta de correo, con la cual puede accesar vía mail o cliente de correo por Internet.

- **Los Computadores Personales, PCs**, funcionan como estaciones de trabajo, son consideradas como otro activo de importancia. Las estaciones de trabajo, que incluyen PCs y laptops, están enlazadas en una **red tipo estrella**, y proveen de un medio de transmisión para toda la información electrónica sensitiva e importante. La Información de usuarios guardada en las PCs, los archivos personales y de correo, el servidor Linux también se consideran como parte de este activo crítico.

- También la información administrativa se la considera un activo de información pero no directamente dentro de lo que es la misión de IGEPN, y por ello **no** es considerada un activo de esencial relevancia.

2.2.1.1.3 Actividad S1.3 Evaluar Prácticas de Seguridad Organizacional

Paso 3

En el **Paso 3a** se analiza el grado en el cual los principios definidos para cada una de las áreas de práctica de seguridad se siguen en el Instituto Geofísico. En el **Paso 3b** se registra aquello que se está haciendo bien o en lo que se está fallando respecto a la teoría propuesta en el principio del área de seguridad. Puede decirse que el Paso 3b es equivalente a identificar fortalezas por un lado, y por otro las debilidades en cada área de práctica de seguridad.

Paso 4

A la mayoría de áreas de práctica de seguridad les fue asignado el estado de semáforo[47] **Rojo**. Esto indica que hay prácticas muy deficientes e inclusive nulas en cuanto se refiere a seguridad de la información. No se asignó un estado de semáforo **Verde** a ninguna de las áreas, y se consideró como un estado de semáforo de **No Aplicable** para el área de práctica de Encriptación de la Información, por no ser ésta un área de práctica relevante para el tipo de información geofísica y para el nivel de acceso que ésta tiene[48].
Se detallan a continuación los resultados de esta primera aproximación al estado actual del cómo está la seguridad en el Instituto Geofísico de acuerdo con las 15 Áreas de Práctica de Seguridad OCTAVE-S:

Práctica de Seguridad 1

La gestión de **Avisos de Seguridad y Entrenamiento** está reflejada en la organización cuando se nota como positivo que existe resistencia a la ingeniería social, y además el personal se responsabiliza en buena medida de la información a su cargo. Pero se nota una falta de entrenamiento sobre seguridad informática en los niveles que se exige actualmente tanto para TI como para todo el personal. Hay poca comprensión de los roles y las responsabilidades individuales sobre la información. No se provee de entrenamiento mediante avisos de correo, ni se dan alertas y precauciones oportunas a través de mensajes por cualquier medio. . No se toma muy en serio el asistir a cursos de entrenamiento en seguridad de datos.

[47] Anexo A: Glosario de términos OCTAVE-S. El estado de semáforo es análogo a un estado de alerta roja, amarilla o verde de seguimiento a la práctica de seguridad actual, es decir al cómo se la está llevando en la realidad.
[48] El Instituto Geofísico maneja información pública como generador y usuario de geoinformación, y a este nivel de tratamiento, la información no se encripta. Cfr. Literal 1.1.5. Marco legal de información geoespacial en el Instituto Geofísico.

Práctica de Seguridad 2

La Estrategia de Seguridad. Si bien es cierto, el Plan Informático del Instituto Geofísico, incluye la seguridad de datos dentro de las estrategias[49] para la supervivencia de los sistemas y sus operaciones; sin embargo, en la práctica todavía no se ha hecho efectiva y carece de sensibilidad frente a la importancia de su grave misión. Es por ello que no se toma en cuenta el valor que tiene la información que se maneja, ni mucho menos su propia seguridad. La estrategia actual no es preventiva, es más bien reactiva y muchas veces tardía.

Práctica de Seguridad 3

La Gestión de la Seguridad de la información no se muestra como un todo integrador e integral. No existe una política organizacional sobre la seguridad de información. No están bien definidos los roles y responsabilidades sobre seguridad de información. La gestión de riesgos de seguridad de datos no incluye los pasos para mitigarlos. Los Jefes de Área reciben informes muy exiguos del Administrador de la Red y éstos sugieren soluciones "parche", que no son verdaderas soluciones. Debido a ello, no se toman acciones integrales y estratégicas sobre seguridad de datos. El presupuesto asignado actualmente para la seguridad de los datos es mínimo.

Como positivo, el comenzar a desarrollar esta evaluación OCTAVE-S es un paso en la dirección correcta para mejorar esta área de seguridad. Si bien es cierto, la empresa AccessRAM MEGADATOS tiene certificación de calidad ISO 9001:2000, pero ésta no oferta la seguridad de los datos en el contrato de servicios. En esta circunstancia, la calidad de servicio de ISP no implica la seguridad de los datos, ya que se los han tratado como dos temas separados, diferentes y no integrados. También como aspecto positivo se debe recalcar que existe ética profesional en los miembros del Instituto Geofísico, y esa es la mejor garantía para la adecuada gestión de la seguridad de los datos.

[49]FLORES y FONSECA, op.cit., páginas. 84-85.

Práctica de Seguridad 4

Las Políticas de Seguridad y Regulaciones. A nivel de seguridad de los datos en la red había muy poco escrito. No existen políticas y procedimientos específicos definidos y documentados sobre seguridad de datos.

Desafortunadamente, las políticas del Instituto Geofísico relacionadas con seguridad han quedado solamente como una recomendación del Plan Informático[50]. De las pocas políticas que existen, no siempre son leídas y seguidas por el personal, la comunicación en ese sentido es muy pobre. Debido a esto, el refuerzo que se tiene sobre ellas es muy débil.

Cuando se reportan incidentes o violaciones contra la seguridad de la información, no hay procedimientos establecidos para tratar estos asuntos.

Práctica de Seguridad 5

Gestión de la Seguridad Colaborativa

AccessRAM MEGADATOS provee el servicio de WebHosting a la página Web, y además es la proveedora del servicio de Internet ISP. El único punto de salida hacia Internet es a través del dispositivo CISCO LRE 575, propiedad de AccessRAM MEGADATOS, a partir de ese punto, es responsabilidad de esta empresa la buena calidad de los procesos y servicios que provee a través de sus instalaciones. La información que va y viene por Internet, a través de ese único punto de salida, y ha sufrido varias veces por contaminación de virus, worms y troyanos. Es un tanto difícil obtener respuesta a algunas de las preguntas sobre tecnología de seguridad a AccessRAM MEGADATOS[51], ya que consideran que es parte del "secreto del negocio". Aunque AccessRAM MEGADATOS posee la calificación ISO 9001:2000 sobre calidad de los procesos, otorgada por la empresa SGS, válida desde julio 2004 hasta enero del 2007,[52] ésta no toma en cuenta la seguridad de la información como parte de la calidad del servicio QoS, y ese es el punto débil del ISP respecto a la gestión de la seguridad colaborativa.

---

[50] Íbid Nota anterior.

[51] Sea por vía telefónica o por e_mail, la empresa proveedora del ISP no revela información desde de su punto de conexión de red hacia dentro de sus instalaciones.

[52] http://www.accessinter.net

No existe una conexión alternativa a Internet, en caso de falla o interrupción del servicio de AccessRAM MEGADATOS. Nunca se ha tomado en cuenta la seguridad de los datos desde un punto de vista integral dentro de los contratos con las empresas proveedoras de hardware y software.

Práctica de Seguridad 6

Planeación de contingencias

No se ha desarrollado, ni peor documentado un plan de contingencias o recuperación de desastres para asegurar los equipos y programas de la red del Instituto Geofísico en caso de desastres naturales, terremoto, incendio, inundación, etc. No existe un plan de contingencias para mantener la continuidad de las operaciones y de servicios. No se consideran los peligros información clave o equipos electrónicos que colapsen por fuego, inundación o desastres naturales. Se descuidan en ese sentido los datos y los backups. No hay una verdadera gestión de respaldos. Los respaldos de información de usuarios no están bien organizados, IUIID. Todas copias de respaldos en CD-ROM se guardan en el mismo lugar, lo que pone en riesgo a la información en caso de que se pierdan los duplicados por algún desastre natural o contingencia. Es preferible colocar un duplicado en un sitio distinto al del original, para que en caso se pierde la una copia, queda la otra de reserva. Si bien es cierto, existen respaldos bien organizados de información sísmica, SISV, sin embargo las bandas de monitoreo sísmico en papel, se hallan sin protección, y son las más vulnerables de sufrir deterioro en caso de contingencia o desastre natural.

Nunca se ha hecho antes un análisis de activos críticos. Nunca se ha hecho un análisis de criticalidad[53] del sistema, ni de las operaciones, ni de aplicaciones. No se sabe en realidad la importancia que tienen unos activos de información respecto a los otros.

Si bien es cierto, existe un plan general de evacuación y recuperación en caso de desastres naturales y emergencias, sin embargo en él no se han integrado la seguridad de los datos, ni tampoco de los equipos.

[53] Criticalidad es la importancia relativa que tiene un bien respecto a los otros, respecto a la misión y objetivos de la organización. Este concepto se deduce del manual de la norma ISO 17799, http://www.security-manual.com además en http://www.iso17799software.com/contacts.htm

Práctica de Seguridad 7

Control de Acceso Físico

Respecto a las prácticas de Seguridad Física se les asignó originalmente un estado de semáforo Amarillo para el Control de Acceso Físico. Sin embargo, al observar las débiles prácticas reales de seguridad física se asignó un estado de semáforo **Rojo**. Existe un portero eléctrico a la entrada de las instalaciones del Instituto Geofísico en el 6to Piso del Edificio de la Facultad de Ingeniería Civil, con el cual se controlan las visitas de personal externo, periodistas o invitados. Hay un letrero en la puerta de ingreso que prohíbe el ingreso a personal no autorizado, y exige el registro o identificación. Hay personal del Instituto Geofísico las 24 horas, lo cual es una ventaja para la seguridad del acceso físico. La seguridad de acceso a la Sala de Registradores no es óptima, puesto que la puerta de ingreso está siempre abierta. Los computadores personales están localizados en sitios muy estrechos. Hay una necesidad de "compartir" las PCs de forma imprudente y no controlada. Además se comparten archivos de investigadores y tesistas con mucha libertad, lo cual no garantiza debidamente la seguridad de esta información.

Práctica de Seguridad 8

Auditoría y Monitoreo de Acceso Físico

El monitoreo de la seguridad física la realiza el Departamento de Servicios Generales de la Escuela Politécnica. Lo que se debe notar es la falta de coordinación con el Área Administrativa del Instituto Geofísico para monitorear la seguridad física en conjunto con los guardias de seguridad del campus. Se debe poner atención también en la gestión de inventarios de hardware y software para controlar los cambios en los equipos. Aunque existen registros de mantenimiento en papel, sin embargo el inventario de hardware está desactualizado, incompleto y no se lo lleva en forma automática con un programa específico.

Práctica de Seguridad 9

Gestión de Sistemas y Red.

No hay planes de seguridad documentados y probados para salvaguarda de sistemas y red. Esta es la primera vez que se trata de realizar una planificación de la seguridad de la información. Las herramientas que actualmente se utilizan para la gestión de la seguridad de los datos no son las adecuadas, ni están actualizadas.

El personal de TI maneja adecuadamente la actualización y manejo de cambios de software y hardware en general, pero las actualizaciones sobre seguridad casi no se las conoce. Los parches para mitigar vulnerabilidades casi no se los conoce ni utiliza[54]. La configuración de herramientas de seguridad Linux es complicada y se han debido contratar expertos de fuera para instalar herramientas de monitoreo, antivirus y antispam de correo. Hay una saturación y concentración de trabajo en el Administrador de la Red.

Es positivo que la mayoría del personal utiliza los equipos computacionales para realizar trabajos únicamente del Instituto Geofísico. Esto es un factor a favor de la seguridad, ya que los programas de aplicación geofísica tienen menor incidencia de ataques que los programas de aplicación general.

Así es notable que haya una mayor seguridad para SISV que para IUIID. Se mantienen bien los programas de aplicación pero no así los respaldos de informes. En la sala de Lectura se guardan los respaldos o backups de información para investigación. El archivo de respaldos no tiene una política de desecho de información innecesaria. Tampoco se ha hecho un estudio de caducidad y durabilidad de los medios de almacenamiento.[55]

Los sistemas no están bien protegidos con una buena política de claves de acceso, contraseñas de usuarios, registros de acceso, etc.

Hay que anotar que no se limpian muy bien los derechos de acceso heredados.

---

[54] http://www.cert.org http://www.sans.org

[55] HOWARD FUHS, "The Fragility of Digitally Stored Information", 2004, Documento PDF, en http:// www.continuityshop.com menciona la forma de conservar discos y medios magnéticos para una mayor durabilidad. Se recomienda sacar respaldos cada cinco años por lo menos. No se da durabilidad mayor a 100 años a los CD-ROMs, por lo cual se puede deducir que los medios digitales duran menos que el medio convencional en papel.

No se tienen avisos oportunos de seguridad de la información. Los avisos de seguridad de información por correo electrónico deben mejorar, y estos deben ser periódicos.

Entre los aspectos positivos se puntualiza que los servicios innecesarios detectados ocasionalmente son bloqueados o eliminados, de esta forma no se permite ver video, ni descargar música por Internet.

Práctica de Seguridad 10

Monitoreo y Auditoría de Seguridad de Tecnología de Información

No se utilizan rutinariamente herramientas para llevar a cabo procedimientos de monitoreo y auditoría del sistema y red. No existe gestión planificada para estos procedimientos. El monitoreo de la seguridad de datos es muy incipiente. Existen reportes ocasionales sobre problemas de seguridad. No hay políticas establecidas ni documentadas de monitoreo ni auditoría de la seguridad de la información. Nunca se ha realizado una auditoría informática en la red de datos del Instituto Geofísico. El Comité Técnico recomienda hacer una auditoría informática como punto de partida para promover el desarrollo de mejoras en el futuro.

Como aspecto positivo, existe un firewall con IPTables instalado en el servidor Linux. Recientemente se realizó una reconfiguración del servidor para combatir el Spamming de correo, con personal contratado ex profeso. Para el correcto desempeño de los servicios ClamAV y SpamAssesin en el servidor Linux CentOS, se deben realizar actualizaciones diarias de antivirus y direcciones antiSpam, lo cual requiere amplio conocimiento de la configuración y de actualización de los parches de vulnerabilidades. En este momento no existe el personal entrenado para el efecto en el Instituto Geofísico.

Práctica de Seguridad 11

La Autenticación y Autorización

No hay políticas documentadas y procedimientos para establecer y terminar el derecho de acceso a información. Tampoco hay métodos ni mecanismos para asegurar que no se haya accesado a información sensitiva con propósitos

maliciosos. En general, no hay políticas y procedimientos para permisos de acceso y control en las PCs del Instituto Geofísico.

Si bien algunas PCs están protegidas con contraseñas de acceso, no existe una buena política de contraseñas, el usuario hereda muchos privilegios. Se comparten contraseñas de muchos usuarios, e inclusive hay contraseñas individuales que dificultan el trabajo si es que son olvidados o sus dueños abandonan el país. No hay un registro de cuentas de acceso en la bitácora de servicios del servidor. El Firewall con IPTables en el servidor Linux Proxy destina servicios y direcciones, pero no hace gestión de ingreso de usuarios.

Práctica de Seguridad 12

Gestión de Vulnerabilidades

El Administrador de Red, selecciona las herramientas de evaluación de vulnerabilidad, listas de chequeo, y scripts en el servidor Linux. Se investigan y detectan los parches para eliminar las vulnerabilidades pero la implementación de éstas en el servidor Linux es muy complicada. El Administrador de Red no está adecuadamente entrenado para gestionar, interpretar, reportar e implementar los parches de las vulnerabilidades.

En caso de necesidad, para parchar el servidor Linux se debe contratar personal externo. No se manejan las actualizaciones de CERT y SANS[56] de manera periódica sobre parches. Se investiga mucho en Internet sobre herramientas de evaluación de vulnerabilidades, pero el presupuesto limitado, la falta de una gestión eficiente y económica y la falta de entrenamiento en implementación de herramientas Linux, no ha permitido llegar a una apropiada gestión.

Práctica de Seguridad 13

Encriptación

No se consideró de relevancia evaluar esta práctica, ya que la información que se maneja es pública, y por lo tanto no se la encripta. El regular los nuevos formatos

---

[56] http://www.sans.org/top20 ; http://www.cert.org/nav/html

de la información geoespacial le corresponde al ODEPLAN[57], lo que está fuera del alcance del Instituto Geofísico.

Práctica de Seguridad 14

Arquitectura y Diseño de Seguridad

No están documentados procedimientos formales sobre la Arquitectura y Diseño específicos de seguridad de la información. Se ha documentado el diseño general de la red, pero no se ha incluido el diseño del sistema de seguridad de información. Se construye desde Agosto del 2005 la nueva infraestructura física en las mismas instalaciones del Instituto Geofísico. Se tiene planificado instalar sobre esa infraestructura cableado estructurado con estándares TIA/ANSI. La metodología OCTAVE-S en el plan de mitigación propone diseñar el sistema tecnológico de seguridad[58], y elaborar un documento de apoyo de utilidad para quienes desarrollen el nuevo diseño y arquitectura de la seguridad en las instalaciones remodeladas.

Práctica de Seguridad 15

Gestión de Incidentes legales

Esta es un área en la cual Instituto Geofísico tiene un conjunto básico de procedimientos documentados. El Jefe del Área Técnica se encarga de los asuntos legales de adquisición de hardware y licencias de software. No obstante, para el caso de incidentes que comprometan a la seguridad de los datos, no existen procedimientos internos de recuperación y guarda de respaldos. No se han contratado seguros para las pérdidas de hardware, anti-incendio, seguro por robo, pérdida etc. Aún así, los aspectos legales no se los consideró de tan alto riesgo, por lo que se le asignó un estatus Amarillo para el semáforo de esta área.
A continuación, dentro de esta práctica para gestión de incidentes legales, se describen según[59] el Cuadro 7, los principales requerimientos legales para el

[57] Cfr. En el Lit. 1.1.6 se menciona que el ODEPLAN en su componente técnico se encarga de definir y normar estándares de producción de información geográfica y protocolos de intercambio de datos.
[58] Esta propuesta está desarrollada en el literal 3.3 del presente proyecto.
[59] Elaborado por el autor del presente proyecto.

tratamiento de los principales activos de información del Instituto Geofísico, y de haberse detectado falencias en esta práctica, se las anota en relación con los preceptos legales correspondientes:

Activo de Información	Requerimientos legales
SISV	Pago oportuno de licencias de software para evitar posible piratería.
IUIID	Exigencia de profesionalismo y ética en la presentación de informes. Debe haber mención de autores, no copia de ideas.
TI + PMV	Exigencia de profesionalismo, no plagio de programas. Pago oportuno de licencias de software. Para el personal deben contratarse seguros médicos y contra accidentes.
Sitio Web del Instituto Geofísico	El proveedor de ISP no se responsabiliza del contenido de la página Web. La empresa del ISP garantiza la integridad y calidad de la presentación del mensaje original.
Servidor de correo interno	Se debe proteger la identidad de los usuarios, evitar la suplantación y el préstamo de cuentas de usuario y contraseñas.
PCs	Contratar un seguro para los equipos. Mantener el inventario actualizado para poder hacer reclamos y denuncias.
CIR	Se deben mencionar los autores en las copias de documentos científicos. Puede haber pérdida de información de respaldo por negligencia de los responsables.

Cuadro 7.- Asuntos legales de los principales activos de información del Instituto Geofísico

- **El Sistema de Información Sísmica y Volcánica, SISV**. – El pago oportuno de licencias de software de los programas de aplicación que se utilizan para la interpretación sísmica y volcánica, y de esta forma evitar la posible piratería. Según el inventario de software, no han existido hasta este momento problemas legales por caducidad de licencias de software. Tampoco se han presentado problemas de piratería o copias ilegales de programas o peor de sistemas.

- En el caso de contaminación por virus en los programas de aplicación del SISV, no se puede tipificar el delito informático, ya que el sujeto del ataque no se puede identificar con precisión y la debida celeridad. Los virus son enviados por terceros, que en el caso del Internet, es virtualmente imposible identificar al atacante. Mientras no exista el procedimiento legal para encontrar al sujeto actor del ataque, no se puede iniciar ninguna acción legal.
- Si alguna persona realiza algún acto doloso en el SISV, se sujeta a las sanciones que están tipificadas como delito informático, en las reformas tratadas al Código Penal en relación con la Ley de Comercio Electrónico, ya mencionadas en el marco legal de la información geoespacial[60]. Estos hechos nunca han sucedido en el Instituto Geofísico, pues la selección del personal es muy exigente en cuanto a lo ético y profesional. Así que la probabilidad de conformación de un delito informático en el SISV es muy baja o casi nula.
- **Información de Usuarios, de Investigación, Informes y Documental, IUIID.** – La responsabilidad de presentación veraz, completa de los informes de IUIID, está sujeta al derecho de las personas a recibir información de calidad. Como se trató en el marco legal de la información geoespacial[61], en la ley Orgánica de Defensa del Consumidor, Artículos 2 y 4, y en la garantía del Estado sobre la información pública en la Ley Orgánica de Transparencia y Acceso a la Información Pública en su Art. 1. Además, la exigencia del manejo de esta información de manera profesional con normas técnicas para facilitar su acceso está garantizada en el Art. 10 de la misma Ley de Transparencia y Acceso a la Información Pública. El profesionalismo y la ética del personal del Instituto Geofísico son valores que se conservan como bienes muy preciados, y por ello es lógico suponer, que no se han presentado problemas legales por fallas por negligencia profesional o técnica. Siempre se han respetado y mencionado los autores de trabajos científicos o técnicos, no se ha incurrido en plagio

[60] Literal 1.1.5
[61] Íbid a la Nota anterior.

profesional. Además los informes que se han presentado siempre han coincidido con la realidad y han sido oportunos.

- **La Subárea de Tecnología de Información en conjunto con el Personal de Monitoreo y Vigilancia, TI+PMV.** También el profesionalismo del **TI+PMV** es muy alto, y es por ello que no se han presentado problemas legales por fallas por negligencia profesional o técnica. En el desarrollo e implementación de aplicaciones e interfaces de software para los sistemas no se han presentado problemas legales por plagio de programas, o la no-mención de derechos de autor. Las licencias de programas de aplicación son gestionadas por el Jefe de Área Técnica y hasta este momento se hallan vigentes, y sin problemas de caducidad.
- Los seguros médicos de **TI + PMV,** en cuanto a su seguridad física de las personas, los gestiona el Área Administrativa, en caso de accidentes, enfermedades o calamidades domésticas, según el trámite correspondiente para cubrir estos eventos.
- **Página Web del IGEPN y enlace al correo interno.** El proveedor de ISP y de WebHosting al Instituto Geofísico deslinda su responsabilidad sobre la precisión, y calidad del contenido de la información que le envían para publicarse en la página Web. No obstante esta empresa se responsabiliza de mantener con calidad, la integridad del mensaje original, y no añadir, ni cambiar nada de la información oficial.
- Tampoco el proveedor de ISP se responsabiliza por la contaminación de virus, ya que virtualmente no existe posibilidad de identificar al atacante, y para que haya una acusación particular debe existir el sujeto a quien demandar.
- Lo que se puede pedir a la empresa proveedora de ISP, es el incluir en su servicio, un antivirus actualizado, y el tomar en cuenta la seguridad de los datos dentro de la calidad del servicio.
- No se han presentado incidentes legales con esta empresa proveedora de ISP, ya que se ha provisto según el contrato firmado, los términos del acuerdo de nivel de servicio.

- **El servidor de correo interno.** – Se puede incurrir en delito informático cuando se simule cuentas de correo, o se violenten claves o sistemas de seguridad para acceder u obtener información protegida, personal o privada. Además puede alterarse el mensaje de datos y cometer falsificación electrónica.
- **Los Computadores Personales, PCs.** – Los Computadores Personales no están asegurados contra eventos naturales o catastróficos. No hay seguro contra incendio o inundación. Se debe pensar en la contratación de seguros para las máquinas y todo el hardware.
- El respaldo legal del hardware es el inventario que no se actualiza con programas a propósito. Los registros de cambios de hardware deben ser actualizados por lo menos mensualmente. De existir la pérdida, robo, destrucción no existe un respaldo escrito para hacer las denuncias legales ante las autoridades correspondientes. Igualmente el software instalado, las licencias y su caducidad, no ha sido respaldado oportunamente. En este aspecto hay un mayor control para el software, y felizmente hasta este día no se han presentado incidentes legales por plagio, piratería de sistemas o programas.

- **El Centro de Información y Respaldos, CIR,** en donde se guardan los respaldos de información relevante para estudios e investigación a futuro. Estos respaldos sirven de apoyo para la investigación sísmica y volcánica. Los respaldos de investigación, documentos e informes están sujetos a la Ley de Propiedad Intelectual para el tratamiento de los derechos de autor. De esta forma, si se hace una copia o se utiliza la elaboración científica de una persona, se debe obligatoriamente mencionar al autor de tales ideas, caso contrario constituiría un plagio intelectual sujeto a sanciones legales. Si existiese la sustracción o robo de documentos o información, se considera esto un delito común en caso de comprobarse. Lo que sí podría darse es la pérdida o destrucción involuntaria de información sensitiva, por negligencia o descuido. En ese caso se atentaría contra el profesionalismo con el

que se debe tratar este tipo de información. Esto atentaría contra el Art. 10 de la Ley de Transparencia y Acceso a la Información Pública, en donde se habla de la custodia profesional y técnica de esta información. En este caso las autoridades que gestionan la protección del Centro de Información y Respaldos, CIR, son responsables por omisión del cumplimiento de sus obligaciones, así como lo son también las personas encargadas de la custodia de esta valiosa información.

No hubo otras Notas o Ítems de Acción como resultado del Proceso S1.

2.2.1.2 Proceso S2: Crear Perfiles de Amenaza

Según los Pasos 5 al 16, el perfil de amenaza se determina con la identificación de los activos más indispensables para llevar a cabo la misión del Instituto Geofísico, y luego de identificado el requerimiento de seguridad más importante, se deben determinar las amenazas más notables en contra de ellos.

2.2.1.2.1 Actividad S2.1 Seleccionar los Activos Críticos

Paso 5

Se seleccionan de entre los activos de información, basados en su importancia relativa para la organización, aquellos tres a cinco activos considerados más relevantes para llevar a cabo la misión de la organización.

Paso 6

Se identifica el sistema crítico por su nombre.

Paso 7

Se menciona la razón para que el activo de información crítico, sea considerado como tal.

Paso 8

Se registra quién usa y quién es responsable del manejo del activo crítico.

Paso 9

Se registra cuáles otros activos están relacionados con el activo crítico.

Activos Críticos

A continuación los siguientes activos han sido considerados críticos y se mencionan además las razones para haberlos escogido como tales:

- **El Sistema de Información Sísmica y Volcánica SISV** – Los registros de información sísmico-volcánica son el 98% de la carga de volumen de datos que maneja el Instituto Geofísico. El **SISV** es el activo crítico más importante para el procesamiento e interpretación de datos para los informes oficiales para la población. La información sísmica y volcánica es la materia prima para la elaboración de informes, estudios, análisis estadísticos y las distintas tareas de vigilancia e investigación fundamental para el cumplimiento de la misión de Instituto Geofísico.

- **Información de Usuarios, de Investigación, Informes y Documental IUIID** – Es el resultado del procesamiento y análisis de la investigación sobre los datos de los registros de monitoreo sísmico y volcánico, tanto el Estado Ecuatoriano, como los organismos internacionales en convenio que requieran interpretación de registros antiguos y actuales para desarrollar investigación científica y por supuesto para elaborar los reportes para la población, tienen en IUIID un activo de vital importancia. Esta información es el resultado de estudios e investigaciones que tiene gran importancia para la publicación en la Web

- **La Subárea de Tecnología de Información en conjunto con el Personal de Monitoreo y Vigilancia, TI+PMV**. El personal de Tecnología de Información, TI, en colaboración con el Personal de Monitoreo y Vigilancia, PMV, constituyen el recurso humano más importante para el mantenimiento del funcionamiento de los sistemas de la red del Instituto Geofísico y el desarrollo e implementación de aplicaciones e interfaces de software para los sistemas.

  Por su relación directa y estratégica con la seguridad de la información, el personal de TI + PMV es también un activo crítico.

- **Los Computadores Personales, PCs** – Los Computadores Personales sirven al personal del Instituto Geofísico y a la vez sirven de dispositivos de almacenamiento en sus discos duros para la información de SISV. Además son importantes porque en ellos se realizan los informes y reportes para ser publicados o editados para la página Web. El personal maneja el correo interno a través de las PCs vía enlace al proveedor de ISP y también la conexión a Internet la realizan sobre sus propias estaciones de trabajo. Las PCs son la principal herramienta para el desarrollo de los científicos del Instituto Geofísico.

- **Centro de Información y Respaldos, al cuál de aquí en adelante se le denomina CIR** – El Instituto Geofísico tiene implementada una Sala de Lectura o centro de información, en donde se guardan los respaldos de información relevante para estudios e investigación en el futuro. Estos respaldos sirven de apoyo para la Investigación Sísmica y Volcánica. Por la relevancia de la información que contienen estos respaldos, también se considera a CIR como otro activo crítico.

2.2.1.2.2 Actividad S2.2: Identificar los Requerimientos de Seguridad de los Activos Críticos

Paso 10

Se identificaron los requerimientos de seguridad para cada activo crítico.

Paso 11

Se determinó que el requerimiento de seguridad más importante de los activos críticos del Instituto Geofísico es la **disponibilidad**, por tratarse de información pública que debe ser conocida por la población con celeridad, claridad y oportunidad. Por lo cual es fundamental el **mantener la continuidad de operaciones** y abierta 24 horas / 7días a la semana la **disponibilidad del servicio**. La disponibilidad es fundamental en el SISV, PCs, y TI + PMV.

Para los activos críticos IIUID y CIR el requerimiento más importante es la integridad, ya que se trata de informes y la creación de sus respaldos. Debe entenderse que la integridad de la información en estos activos garantiza la continua y adecuada disponibilidad de ella.

2.2.1.2.3 Actividad S2.3: Identificar las Amenazas a los Activos Críticos

En el **Anexo E**: de las Hojas de Trabajo, se encuentran las matrices de perfil de riesgo para cada activo crítico, las cuales se llenaron según los siguientes Pasos:

Paso 12

Se perfila al actor de amenaza y sus posibles consecuencias en el árbol y las ramas a base de la lógica causa – efecto.

Paso 13

Se registra el contexto de los actores de amenaza, es decir su entorno en la organización.

Paso 14

Se anota la opinión del equipo sobre la intensidad del motivo de amenaza por parte de su actor.

Paso 15

Se anota el historial de ocurrencia de amenazas en el pasado y el grado de confianza en esta estimación.

Paso 16

Se puntualizan áreas de atención en las que se dan ejemplos reales de cómo personas o situaciones clave, se constituyen en reales actores de amenaza.

A continuación se narran los resultados más notorios que dan un esbozo de amenaza para el perfil de riesgo de cada activo crítico:

I. Sistema de Información Sísmico y Volcánico, SISV

a) Actores humanos que accesan a la red de información

Todas las personas que accesan a la red de información del Instituto Geofísico son se las debe considerar con atención. Pocas veces ha sucedido el evento de modificación o pérdida de la base de datos de volcanes por descuido accidental del personal interno y nunca de manera deliberada, ya que las motivaciones de un atacante interno son bajísimas.

El año pasado ocurrió más de 20 veces la revelación de información de SISV a personas que necesitan realizar investigaciones; sin embargo estas revelaciones no se han dado más allá del Instituto Geofísico.

Desde fuera, varias veces se ha detectado que ingresa código malicioso accidentalmente por personas que envían mensajes o

archivos al correo electrónico. De manera deliberada, los atacantes generadores de Spam de correo han enviado miles de direcciones basura y han conseguido interrumpir las operaciones del Servidor Linux, con lo que se afecta la disponibilidad de operación de SISV.

b) Actores humanos que utilizan el acceso físico

Para SISV, se identificaron los tipos de personas, las cuales podrían ser consideradas como actores de amenaza. En caso de compartición de equipos o programas, puede ocurrir la revelación a información no procesada. No existe el debido control de ingreso a la oficina donde se encuentra el Servidor Linux, inclusive, algunas veces se la ha dejado sin candado.

Existen privilegios de acceso físico de acuerdo a la jerarquía de los cargos administrativos y puestos de trabajo, lo cual a veces impide el debido control en los sobretiempos.

c) Problemas de sistemas

Se reiteran las mismas amenazas para los actores humanos que accesan a la red de información en el literal a) anterior. Además, por defectos de software ha habido interrupción de operaciones momentáneas del SISV. Entre los defectos de software se incluyen problemas de interoperabilidad entre los utilitarios Microsoft y los programas de aplicación geofísica. Hay que notar que el tiempo de interrupción es menor del 1% de operación, lo cual puede ser considerado aceptable dentro del normal funcionamiento. Esto se puede notar en los vacíos que se encuentran en las imágenes de monitoreo sísmico que se encuentran en la página Web del Instituto Geofísico[62].

Se debe agregar que las interrupciones se deben más por deficiencias en el hardware, principalmente por obsolescencia de los equipos. Por ejemplo, el sistema de adquisición ACQ está todavía ligado a una plataforma muy antigua de hardware, como es el Procesador IBM 286 que funciona con el sistema operativo DOS.

[62] http://69.65.157.50/heli/sgram/index.html

Los virus han creado problemas en las aplicaciones que maneja el SISV, más por descuido del personal que ha introducido CD-ROMs o diskettes sin haberlos sometido primero a chequeo y limpieza de código malicioso, con programas que existen para el efecto. Hay que anotar que los registradores no sufren de ataques de código malicioso, pues son estaciones sólo de lectura.

d) SISV.- Otros Problemas[63]

- Problemas de fuente de energía: Los UPS no funcionan adecuadamente por interrupción del fluido eléctrico. La operación de la fuente de energía auxiliar se encarga al personal de mantenimiento de la EPN, en coordinación con el personal de operación de redes del Área Técnica
- Desastres naturales: En el caso de un evento sísmico en la ciudad de Quito no hay la adecuada protección para SISV. Sería muy grave perder la información y sobre todo no garantizar la disponibilidad de ella. Se sugiere replicar la información de respaldo en la estación Guadalupe en Tungurahua, aunque el analizar esta posibilidad rebasa el alcance del presente Proyecto de Titulación.
- Configuración física o disposición de edificios, oficinas o equipos: La disposición de los equipos en las oficinas y espacios no es funcional. La configuración física de las áreas de trabajo permite la revelación, la modificación no autorizada, pérdida o destrucción de información del SISV por los miembros del personal, así como usuarios externos que manejan Información del SISV.

  Actualmente se remodela la infraestructura física para instalar los equipos con una disposición más segura.

[63] Estos problemas son tratados con mayor profundidad en la Hoja Trabajo de Perfil de Riesgo de los Computadores Personales.

II. Información de Usuarios, Informes y Documental, IUIID

Actores humanos que utilizan el acceso físico

Algunos miembros del personal científico y estudiantes utilizan los informes y documentales de otros sin mucho cuidado. Por esa razón, a veces se pierden estos archivos. Se han cometido errores al manejar las bases de datos de volcanes. Dos veces el año pasado se ha perdido valiosa información. Afortunadamente existen respaldos y se ha podido recuperar esta base de datos. Más o menos se pierde por año un 5% de los IUIID. No han existido prácticamente eventos deliberados sobre pérdida de informes, más bien estas pérdidas han sido accidentales.

III. Personal de Tecnología de Información en conjunto con el Personal de Monitoreo, TI + PMV

Otros Problemas

El personal del Área Técnica sufre de inestabilidad laboral. No hay continuidad en la documentación que se deja para los relevos inmediatos o permanentes de puestos. Esto produce pérdida de tiempo, confusión y retardo en la recepción de órdenes y transmisión de información hacia las otras áreas. La ausencia temporal de personal técnico clave y la inestabilidad en los puestos a veces retrasa el trabajo para implementar nuevas herramientas y aplicaciones de TI.

La configuración física al no ser funcional dificulta el trabajo de TI + PMV. La humedad y el ambiente desordenado desmotivan al personal para un trabajo eficiente. Al no haber una distribución estándar de cableado estructurado, se dificulta el trabajo de toda el Área Técnica. Durante una crisis sísmica o volcánica, TI+PMV debe trabajar bajo presión con la presencia a veces impertinente de periodistas o personas curiosas.

IV. Computadores Personales, PCs

a) Actores humanos que utilizan el acceso a la red de información. No hay una buena política de contraseñas en la red interna del IGEPN, el control de acceso por contraseñas debe exigir que éstas por lo menos

tengan 8 caracteres, entre mayúsculas y minúsculas, números y símbolos.

Los estudiantes e investigadores con acceso ilegítimo a las PCs a veces prestan los contraseñas de acceso para ver información que no debería ser compartida.

Las estaciones de trabajo son vulnerables puesto que a veces los estudiantes o ingenieros investigadores se olvidan de salir del sistema, lo que facilita el fenómeno de "red compartida"; es decir, el acceso indebido y posible modificación o pérdida de información sensitiva.

b) Actores humanos que utilizan el acceso físico**:**

- Cuando usuarios internos del Instituto Geofísico utilizan el acceso físico: Cualquier miembro del personal interno puede conseguir acceso físico y utilizar las PCs dejadas activas inadvertidamente en los escritorios de trabajo. Básicamente se comparten las claves de acceso y por esto no se puede controlar la responsabilidad en cuanto a pérdidas de hardware y plagio de programas
- No hay políticas o procedimientos para regular la seguridad física y adecuada protección de las PCs. No se ha contratado un seguro para las PCs contra robo, incendio o desastres naturales.
- Cuando usuarios externos al Instituto Geofísico utilizan el acceso físico: Cualquier visitante o investigador externo tiene acceso físico a todo el equipo de TI una vez que ingresa por la puerta principal de ingreso con portero eléctrico. De esta manera, personas ajenas al Instituto Geofísico podrían ver o modificar accidentalmente la información cuando se las deja cerca de las PCs o estaciones de trabajo no desactivadas.
- Existe la mala experiencia de ladrones que han ingresado a las instalaciones y se han sustraído equipos con valiosa información, en especial LAPTOPS, que son equipos más transportables. En este año 2005 se sustrajeron del interior del Instituto Geofísico una laptop con un disco cargado con más de 80 GB de valiosa información.

c) Problemas de sistemas

- Defectos de software: En cuanto a seguridad de los programas en las PCs, se encuentra que aunque la mayoría de estaciones tienen Windows XP como sistema operativo, todavía se opera con sistemas operativos antiguos como Windows 95 e inclusive DOS. Además el software de aplicaciones Microsoft Office a veces presenta fallas, se dañan archivos, se pierde tiempo en recuperar los archivos. No existe una política adecuada de actualización de sistemas operativos ni parches de seguridad. La adquisición y el pago de licencias de software están sujetas a la aprobación del presupuesto anual del Instituto Geofísico, lo cual hace que haya demora en comprar o adquirir cualquier elemento para la red por causa de la lentitud de los trámites administrativos.

  El software no es tan amigable para las interfaces de aplicación y para la integración de las interfaces de control de instrumentación. No se han desarrollado aplicaciones específicas para servicios de información geoespacial, suficientemente funcionales para la red interna. Tampoco se ha desarrollado software de aplicación multiplataforma que se integre a futuro con las nuevas tecnologías multimedia e inalámbrica.

- Problemas de sistemas.- El código malicioso

  Los virus, gusanos, troyanos, puerta trasera han atacado más de 50 veces por año. Los computadores no tienen una protección segura, actualizada y automática de virus. No existe un control centralizado en el servidor Linux, para examinar los CD-ROMs y diskettes que van a ser ingresados a la red, para realizar un chequeo preventivo y/o limpieza de virus. La base de datos de registro de virus debe actualizarse diariamente, lo cual no se lo ha hecho por falta de gestión adecuada de TI para la compra de licencias de programas antivirus.

- Problemas de sistemas.- Vulnerabilidades en el servidor Linux. El único servidor tiene sistema operativo Linux CentOS 4.1 y sirve para toda la red. El servidor no tiene configuradas restricciones de superusuario que

debería tener por su finalidad eminentemente administrativa. No se cubren las brechas de seguridad, los servicios del servidor Proxy están mal configurados, hay puertos y servicios abiertos innecesariamente, lo que pone en peligro la seguridad de la red. Hay un constante e inminente peligro de sufrir ataques de Spamming de correo. Estos ataques provocan la multiplicación geométrica de réplicas de direcciones de correo, con lo que se saturan los servicios. El servicio FTP está disponible desde cualquier estación de la red por lo que cualquier usuario puede copiar información sensitiva; pues es conocida la política laxa de contraseñas de acceso.

Se descubrió que el personal de TI no monitorea adecuadamente los ataques externos. Si bien se monitorean las actividades sospechosas en el servidor de correo, por otra parte no se revisan las cuentas de acceso periódicamente. No se chequean los programas ejecutados con los respectivos usuarios y fechas, o tiempos. Se encontró que no están instaladas herramientas adecuadas y actualizadas para el monitoreo de red. No están documentadas las tareas de administración de la red, ni se elaboran reportes por lo menos semestrales para el Comité Técnico.

Los servicios habilitados en el sistema operativo del servidor Linux han sido reconfigurados en el firewall con IPTables[64]. Los servicios activos pueden permitir que un usuario no autorizado tenga acceso a sistemas que no estén bien configurados.

Una de las dificultades encontradas es lo complejo de la programación de las seguridades para el Servidor Linux. No se consultan a organizaciones de seguridad sobre los parches y actualizaciones contra las vulnerabilidades de los sistemas, tales como CERT[65] y SANS, y por ello la seguridad de la red se vuelve un problema de nunca acabar.

El hecho de mantener la red segura solamente protegiendo al servidor Linux no es una política completa ni actualizada de defensa, ya que

---

[64] Se presentaron fuertes problemas con el Spamming de correo entre Junio y Julio del 2005. Se contrató un técnico externo para que instale el SpamAssesin y ClamAv que tiene el propio Linux y reconfigure el Firewall con IPTables en Julio del 2005. Estas soluciones son solo parciales, y no cubren la mayoría de las las brechas y agujeros de seguridad del servidor Linux.

[65] http://www.sans.org/top20 ; http://www.cert.org/nav/html

este servidor es difícil de configurar, y los ataques a la red pueden ser múltiples y en diferentes estaciones. Del mismo modo algunos virus no son detectados por los programas antivirus que se tienen instalados en las PCs. Tal y como se encuentra la red, es muy vulnerable a ataques.

- Problemas de sistemas.- Defectos de hardware

  Cuando ha habido interrupción de operaciones, se debe en la mayor parte a defectos de hardware y software de aplicaciones. Los equipos obsoletos no se adaptan a las nuevas tecnologías, este hecho retrasa la instalación y el funcionamiento, por lo que todo el desempeño de la red se ve afectado. No hay una política de gestión ni de monitoreo automático de seguridad para defectos o fallas de hardware de. No se detectan anomalías en los equipos por esta falta de un adecuado sistema de monitoreo de red. El inventario de los equipos y programas no se halla actualizado y esto ha dificultado el análisis de la seguridad para cada estación de trabajo.

  No se han establecido las capacidades mínimas de almacenamiento con que se debe dotar a cada uno de los equipos PCs o estaciones de trabajo, sobre todo para grandes volúmenes de información.

  Solo se puede enviar a una estación PC el volumen de información que pueda soportar, y esto solamente se da con una adecuada gestión de sistemas y red.

  Los Computadores Personales como estaciones de Trabajo son susceptibles de amenazas en cuanto a seguridad física debido a que **son equipos que no cuentan con cableado estructurado bajo estándares ANSI/EIA/TIA.** Sin cableado estructurado, los equipos se hallan bajo un alto riesgo de cortocircuito, errores en las conexiones y las reparaciones se dificultan, puede haber aumento de carga estática y dificulta la realización de reparaciones, aumenta la carga estática en las PCs y se pueden dar retardos en la transmisión, daños en los discos, errores en los registros, etc. Tampoco se cuenta con equipos UPS para resguardar información en caso de pérdida del fluido eléctrico.

En caso de incendio por cortocircuitos, no hay extintores ni detectores de humo. Hay que notar como medida elemental de prevención, dentro de las instalaciones del Instituto Geofísico está prohibido fumar, beber o comer.

No hay suficiente espacio físico ni la ventilación requerida para asegurar los equipos contra la humedad o en caso de producirse un derrame de tintas de impresoras o registradores, no hay forma de proteger las estaciones de trabajo. No se ha contratado un seguro de equipos en el caso de que ocurran robos, averías causadas por fuerzas de la naturaleza, mal uso o fallas en el suministro de fluido eléctrico. Además, hay que anotar que el único Switch 3Com Baseline hacia el cual confluyen todas las PCs se encuentra sin protección física, no está en un rack, ni en un armario de acero, ni sujeto con fijadores. Este Switch está expuesto a ser manipulado por los usuarios, así cualquier persona lo puede desconectar si lo quisiese y esto constituye un hueco muy grande en seguridad. Igualmente el dispositivo Cisco LRE 575, carece de adecuada protección física.

d) Computadores Personales.- Otros problemas

Problemas de telecomunicaciones, fuente de energía, desastres naturales, configuración física o disposición de edificios, oficinas o equipos, La obsolescencia de los equipos ya se ha mencionado antes en el literal I. d) del Perfil de Riesgo del SISV - Otros Problemas.

Problemas de telecomunicaciones y con empresas tercerizadas proveedoras de servicios.

Este año 2005, por un accidente de tránsito, un vehículo destruyó el poste en donde se halla instalado el cableado de última milla de AccessRAM MEGADATOS, y por ello esta empresa interrumpió los servicios de Internet y Webhosting por dos días. Las PCs fueron afectadas por este evento pues se interrumpieron los servicios de actualización de la página Web y del correo interno. En ese sentido hay

mucha dependencia del Instituto Geofísico de su proveedor de ISP para mantener la continuidad de las operaciones.

Hay que notar que el canal compartido de ancho de banda es de tan sólo 200 Kbps, lo cual hace muy lenta la conexión a Internet. Esto vuelve lenta a la red, y el desempeño no es el adecuado para las necesidades actuales. El promedio de velocidad de descarga de información es de 56 Kbps, lo que nos indica que a lo sumo 4 estaciones podrían estar trabajando simultáneamente conectadas a Internet, antes que el ancho de banda de apenas 200Kbps se sature.

V. Centro de Información y Respaldos, CIR

a) Actores humanos que utilizan el acceso físico

Los respaldos se guardan bajo llave en un armario de madera y no de acero. Además, la configuración física actual de las oficinas no es funcional y al estar los respaldos en desorden y casi a nivel del piso, vuelven al CIR muy vulnerable de deterioro, destrucción o pérdida de información. Aunque solo personas autorizadas pueden acceder a esta información, en caso de rotura accidental o caída de las dos únicas copias de CD-ROM duplicados se produciría una pérdida irreparable de respaldos de información sensitiva. Los duplicados de respaldos deben estar en lugares distintos, de tal forma que si se pierde una copia, quede la otra disponible.

También las bandas de registros en papel son vulnerables y fácilmente degradables. Estas bandas deberían ser grabadas en CD-ROM, en especial los registros convertidos por el programa de aplicación Earthworm (Programa que convierte los registros sísmicos en imágenes de Internet), por el valor considerable de esta información para futuras investigaciones.

A veces los miembros del personal consultan la Sala de Lectura **sin el debido registro de identidad**, poniendo en peligro la integridad de valiosa y sensitiva información de utilidad para futuras investigaciones.

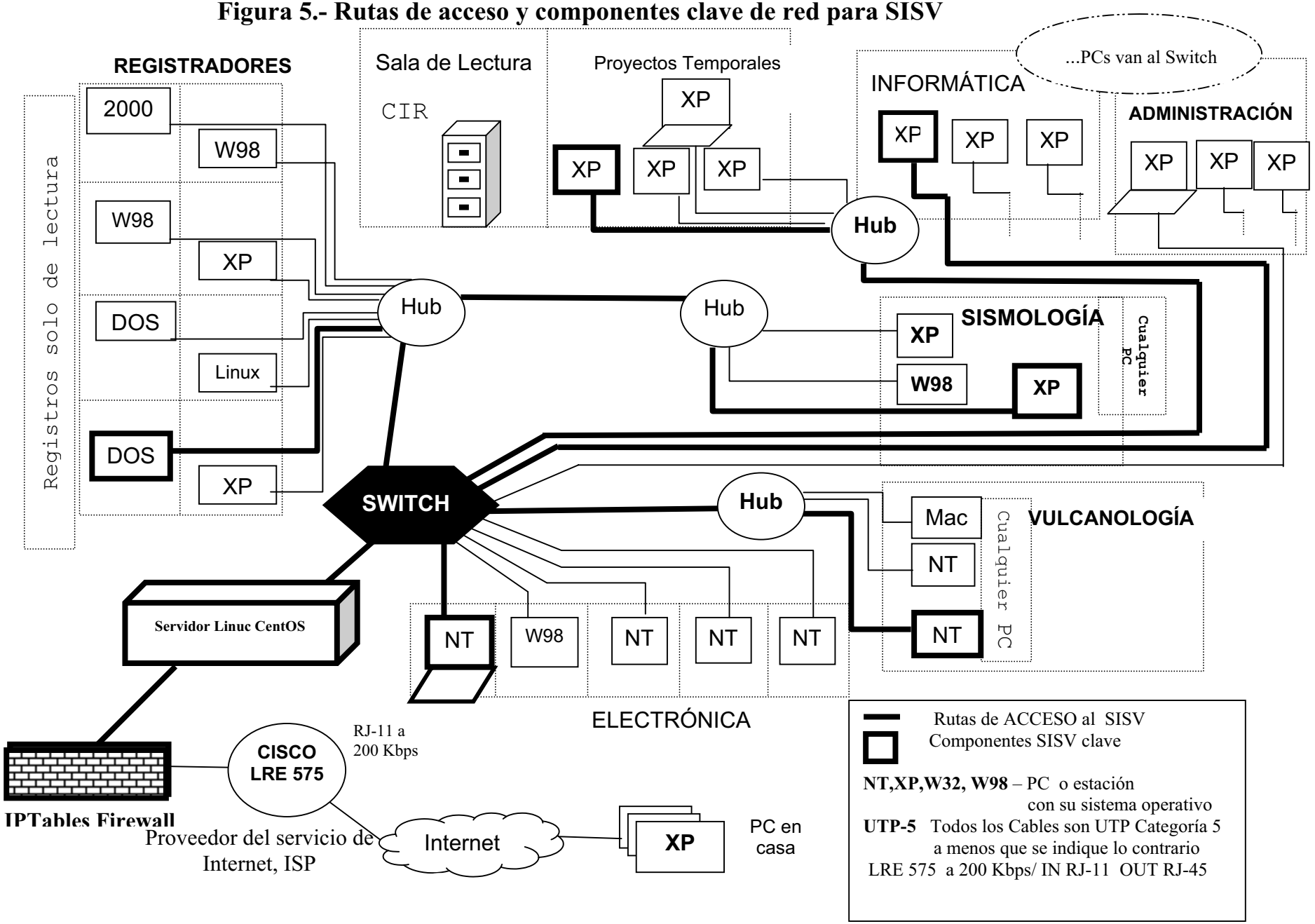
Debe **existir una codificación de los respaldos en sistema de base de datos tipo biblioteca[66].** Actualmente la mayoría de respaldos se hallan sin codificación, ni orden, lo que dificulta su recuperación, en caso de necesidad. Además hay una pérdida de tiempo en buscar y hallar un respaldo por su nombre o fecha. Los respaldos de información sensitiva y de alta importancia para futuras investigaciones, como por ejemplo los registros pluviométricos estacionales, deben re-grabarse de manera periódica, debido a que los medios digitales son de baja durabilidad, frágiles y vulnerables a las condiciones adversas del clima.

b) Centro de Información y Respaldos.- Otros problemas

En caso de descuido, si se perdiese información sensitiva, no hay forma de recuperarla, lo cual es perjudicial para el desarrollo de futuros proyectos. Las instalaciones de la Sala de Lectura son húmedas y los muebles actuales que guardan los respaldos se encuentran a nivel del piso. No existen armarios de acero para proteger los discos digitales que guardan información sensitiva. No hay un plan de evacuación en caso de desastre natural, o en el caso de destrucción accidental por cualquier causa, no se tiene un plan de contingencias o simplemente de resguardo físico seguro de backups. En caso de darse un procedimiento de evacuación al mover los respaldos en CD-ROM, mapas, diskettes, éstos pueden dañarse o perderse de manera permanente.

[66] http://www.dblib.org http://www-dglib.stanford.edu

Figura 5.- Rutas de acceso y componentes clave de red para SISV



2.3 RIESGOS TECNOLÓGICOS

En este acápite se siguen los Pasos 17 al 21 de la Hoja de Ruta, para identificar los riesgos desde el punto de vista tecnológico operativo. Entendiéndose lo tecnológico como todo aquello relacionado con los elementos y componentes de la red física.

2.3.1 FASE DOS: IDENTIFICAR VULNERABILIDADES EN LA INFRAESTRUCTURA

La infraestructura física de red comprende los componentes de hardware e interconectividad. Para identificar las vulnerabilidades en esta infraestructura computacional, primero se relacionan los componentes de red con los activos críticos y se establece cuál de ellos es el más importante, y se lo denomina el sistema de interés. Luego se determina el cómo se transmite la información de este activo crítico llamado sistema de interés, a través de las rutas de acceso de la red. Posteriormente se analizan los procesos relacionados con la tecnología computacional, al identificar responsables, sistemas y formas de almacenamiento de la información del sistema de interés.

2.3.1.1 Proceso S3: Examinar la Infraestructura Computacional en relación con los Activos de Información Críticos

2.3.1.1.1 Actividad S3.1 Examinar las Rutas de Acceso

Paso 17

SISV es en realidad el activo crítico más importante, ya que constituye el sistema más importante para llevar a cabo la misión del Instituto Geofísico. Por esta razón, SISV constituye el sistema de mayor interés en relación con la infraestructura computacional. Para un mejor análisis, como se puede ver en la Figura 5, se identificaron las rutas de acceso y los componentes clave de la red que están relacionados con este valioso sistema, SISV. A través del único Switch, la

información de SISV se transmite a las diferentes áreas mediante Hubs. El problema de la seguridad para la conexión a Internet se simplifica, ya que existe un único punto de acceso al servidor Linux, cuyos detalles se narran en el siguiente Paso.

Paso 18

En el **Paso 18a** se identifican los componentes clave de la red que son parte o están relacionados con el SISV como se puede ver en la Figura 5. Para las diferentes áreas se puede observar que el servidor Linux está conectado al único Switch 3Com. Para la Sala de Registradores hay un Hub que envía los registros de solo lectura hacia las áreas de Sismología y Vulcanología, las cuales tienen a su vez su propio Hub. De igual manera el área de Proyectos Temporales transmite y recibe información a través de su propio Hub. Las áreas de Informática y Electrónica se comunican directamente a través del Switch.

La Sala de Lectura, en donde está el Centro de Información y Respaldos, CIR, no tiene conexión directa con el SISV a través de la infraestructura de red.

Los computadores personales y laptops, configuradas con los sistemas operativos que se muestran en la Figura 5, constituyen también componentes claves de red, pues en ellos reside el SISV y se transmite entre ellas la valiosa información científica sísmica y volcánica. La IUIID se considera un producto de SISV, por lo cual es también parte del sistema de interés.

Hay que notar que en los pasos 12 a 16 de las Hojas de Trabajo de Perfil de Riesgo para Computadores Personales, ya se mencionaron ciertas vulnerabilidades de la infraestructura de red, y, sin que constituya una repetición, en los pasos 17-18 se complementa el análisis del Paso 16 literal IV, relacionando las PCs con el SISV y también se identificaron los responsables de cada componente.

El servidor Linux.

El SISV no reside en el servidor Linux, pero los servicios y puertos relacionados con este sistema son administrados mediante el firewall con IPTables. Hay que notar que el servidor está configurado en Linux debido a que la mayoría de ataques de código malicioso son más compatibles con Windows[67]. Así la vulnerabilidad a estos ataques desde fuera de la red disminuye al estar configurado el servidor con el sistema operativo Linux, además para la transmisión de datos, Linux se comporta mucho más rápido puesto que no tiene que resolver tantas utilidades en pantalla, que poseen los sistemas operativos Windows. Como los sistemas relacionados del SISV funcionan en su mayoría para sistemas operativos compatibles con Windows, la mayor vulnerabilidad del SISV se encuentra en la contaminación de código malicioso compatible con Windows.

Además, hay que tomar en cuenta que hay un único Switch para repartir los servicios y transmitir información por lo cual el problema de acceso hacia la red externa se hace más sencillo, debido a que existe un único punto de salida hacia la red externa o a Internet, y es a través del dispositivo CISCO LRE 575. La protección de ese único punto de acceso es una ventaja por el control centralizado a través del Servidor Linux, lo que no obsta que la contaminación ingrese desde dentro por los usuarios internos con discos o medios contaminados con código malicioso.

Dentro de la red interna, en el servidor Linux el firewal con IPTables asigna puertos y servicios a través el único Switch 3COM Baseline, lo cual facilita el las funciones de control de acceso de cada máquina, sin embargo en el caso de ingreso de código malicioso, solamente se direcciona la contaminación hacia determinada máquina, lo cual no es de ninguna manera una medida completa de seguridad. Esta medida reactiva lo que hace es focalizar la contaminación en determinadas máquinas, servicios o puertos, y luego de detectado el código malicioso, se procede a la limpieza, luego de que el daño está hecho.

---

[67] Esta apreciación es del personal de Tecnología de Información del Instituto Geofísico por su experiencia y conocimientos.

El **Paso 18b** se establece que para el análisis de los puntos de acceso intermedio se toman en cuenta solo a los elementos de la red interna. Si hubiese contaminación a través del Internet, la empresa proveedora del ISP no se responsabiliza de la contaminación de código malicioso a través de sus servicios, sino solamente de la correcta presentación de la página Web. La seguridad de la Página Web no se encuentra dentro del ámbito de responsabilidad de la red interna del Instituto Geofísico. Además los usuarios internos del Instituto Geofísico no pueden acceder al SISV desde fuera a través de Internet. Lo que sí puede haber es contaminación de virus hacia la red interna a través del único punto de entrada/salida a Internet. La limpieza de esta contaminación constituye una ardua tarea para el administrador de la seguridad de la red interna.

Existe además el problema que en la misma máquina en donde reside el Servidor Linux está el servidor de correo interno, lo que ocasiona que exista posibilidad de contaminación de código malicioso a través del correo que va y viene por Internet, y de esta se puede contaminar el servidor Linux y desde ahí a toda la red interna.

Entonces la posible contaminación con código malicioso se lo maneja como un problema dentro de la red interna, sin importar el punto de acceso por el que hubiese ingresado: sea por Internet, o a través de los medios magnéticos de los usuarios internos.

En **Paso 18c** se considera los usuarios humanos como personas que ingresan y utilizan las estaciones de trabajo en el local de la instalación. Generalmente estos usuarios son los científicos investigadores, ingenieros y estudiantes, con sus propias laptops.

En el **Paso 18d** se identifican en relación con el SISV, a todos los respaldos que tuviesen en máquinas los usuarios en CDs, videos, DVDs, cintas

En el **Paso 18e** se anotan los otros sistemas o componentes que están relacionados o accedan a información o aplicaciones de SISV, entre ellos principalmente están personal de tecnología de información, en conjunto con el personal de monitoreo, TI + PMV, y, como apoyo a la infraestructura de la red, están los otros sistemas relacionados con los otros activos críticos como son electrónica e instrumentación. Con excepción de CIR, todos los otros activos críticos están en directa relación con SISV, a través de la infraestructura de la red.

*2.3.1.1.2 Actividad S3.2***:** *Analizar los Procesos relacionados con la Tecnología*

Paso 19

Según el **Paso 19a,** se marca el camino en las ramas del sistema de interés, para cada clase seleccionada en los pasos 18a - 18e, y así mejor visualizar cuáles clases de componentes de red están relacionados con uno o más activos críticos**.** Después en el **Paso 19b,** se relacionan los activos críticos con cada clase. A más de lo dicho en el Paso 18, se debe añadir que los componentes instalados de otras instituciones en la red de información, su gestión no es responsabilidad del Instituto Geofísico.

Paso 20

Se asigna la responsabilidad de quien mantiene y se encarga de la seguridad de cada clase de componente de la red. Es preciso recalcar que las funciones están concentradas en administrador de red en conjunto con el personal de TI. La seguridad computadoras laptop portátiles son responsabilidad de su propio usuario. Además se debe mencionar que los componentes instalados por otras instituciones, funcionan de manera transparente al usuario, ya que reciben y transmiten información a nivel de capa 2 de red, y, aunque están indirectamente relacionados con la infraestructura física de la red interna, la gestión de la seguridad de estos datos está fuera de la responsabilidad del alcance del personal del Instituto Geofísico.

Paso 21

El personal de TI con su propia experiencia hizo una estimación de en qué grado se considera la seguridad al configurar y mantener estas clases de componentes. Se debe anotar que los medios de estimación son en su mayor parte informales. Hay que recalcar que ninguna clase de componente de la red se considera de mucha confiabilidad en cuanto a su configuración y mantenimiento. Es muy

incipiente el monitoreo de red y la actualización de parches de vulnerabilidad, más bien el personal de TI enfoca su análisis en la limpieza parcial de virus de las estaciones.

En el **Anexo E:** en las Hojas de Trabajo de Perfil de Riesgos se completaron los perfiles de los computadores personales y se completó el análisis del servidor Linux; se anotaron las características mencionadas ya en los pasos 18 al 21. Y así se completó el análisis de la Fase Dos.

No se identificaron otros Ítems de Acción, Notas o Recomendaciones para el Proceso S3.

3. CAPITULO TRES: PLAN DE SEGURIDAD

3.1 POLÍTICAS, NORMAS Y PROCEDIMIENTOS

Este acápite se lo ha elaborado para constituirse en una introducción a la Fase 3, en donde se desarrollan las estrategias y los planes de mitigación.

3.1.1 NORMAS

El Catálogo de Áreas de Práctica de Seguridad de OCTAVE-S constituye una síntesis de las normas actualizadas de los estándares internacionales[68], y ya se las ha utilizado en la Fase 1 en los **Pasos 3 y 4** para evaluar el cómo está la realidad del Instituto Geofísico frente a principios ya establecidos por las normas. De esta forma se conoce de primera mano cuán distante está la práctica actual, de la estricta norma sugerida.

Luego, en los **Pasos 12 a 16** se perfilaron las amenazas a los activos críticos del Instituto Geofísico. Las amenazas por sí mismas son el primer paso para definir el Perfil de Riesgo del Activo, pero falta la otra parte: para completarse el perfil de riesgo, debe hacerse la aproximación de la probabilidad de que ésta amenaza ocurra en el tiempo. Riesgo se define la probabilidad de ocurrencia de una amenaza. Pero, ¿cómo determinar la probabilidad de la manera más cercana a la realidad? Justamente en los **Pasos 22, 23 y 24** se intenta hacer una aproximación a esta probabilidad de ocurrencia y cualidad de su impacto. Para aquellas prácticas cuyo estado de alerta sea **Rojo**, R, y el impacto y la probabilidad de ocurrencia sea mayor, se seleccionan como prácticas de seguridad en donde se necesita más el aplicar la mejora o el establecimiento de una estrategia actual de protección. **No** se analizan **todas** las 15 Áreas de Práctica de Seguridad para analizar la estrategia de protección, sino solamente aquellas que están más descuidadas. Los pasos **25 al 30** ya se explicaron en el literal 1.4.2.4. Cabe añadir que las Áreas de Práctica de Seguridad son el **filtro**

---

[68] ALBERTS, Christopher, DOROFEE, Audrey, WOODY, Carol, "Seguridad de la información en pequeñas organizaciones", Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, Enero 2005, Página 54. en http://www.cert.org/archive/pdf/dorofee-v6.pdf
Tanto la BSI 7799, la ISO 17799, los estándares NIST- 800, están sintetizadas en el Catálogo de Áreas de Práctica de Seguridad. Sin embargo, este Catálogo puede aplicarse y adaptarse a diferentes instituciones y dominios de terminología. Cfr. Anexo A:Glosario de términos OCTAVE-S.

teórico-práctico en donde se criban y seleccionan solamente aquellas con mayor necesidad de seguimiento.

3.1.2 POLÍTICAS

Cuando una organización acepta como suyas las sugerencias sobre mejoras en las áreas de prácticas de seguridad, se vuelven éstas **sus políticas**. Los cambios en las estrategias de protección que constan en los planes de seguridad como actividades de mitigación pueden también ser considerados sus políticas, en caso de aprobarse y aceptarse el plan. De ser así, estas actividades sugeridas son aceptadas formalmente por la organización como políticas propias.

Las políticas que actualmente se siguen en el Instituto Geofísico son muy incipientes, así que si se aceptan las sugerencias del plan a desarrollarse, estas actividades de mitigación y sus áreas de práctica relacionadas pueden constituirse en un conjunto de políticas propias y formales para mejorar la seguridad de los datos.

3.1.3 PROCEDIMIENTOS

Los procedimientos en realidad para la presente evaluación OCTAVE-S, son los Pasos ya seguidos del 1 al 21, y aquellos que faltan por seguir, es decir los Pasos 22 – 30, sirven para desarrollar las estrategias y los planes de mitigación del riesgo. No se pueden separar los 30 Pasos, ya que constituyen un solo sistema integral. Los procesos a seguir en caso de que el plan de seguridad sea aprobado e implementado, se definen en las actividades de mitigación seleccionadas, no se los debe confundir con todo el procedimiento OCTAVE-S. Puesto que las actividades de mitigación propuestas en el plan según el Paso 28 son el resultado de toda la metodología integrada en los Pasos 1 al 30.

3.2 FASE TRES: DESARROLLAR ESTRATEGIAS Y PLANES DE SEGURIDAD

En continuidad con los Pasos 1 al 21 anteriores, se completa la evaluación de la seguridad de la red de datos interna del Instituto Geofísico con el desarrollo, en los Pasos 22 al 30, de las estrategias de protección y planes de mitigación del riesgo. De esta forma se articula el análisis del riesgo, con el plan de mitigación, puesto que a mayor riesgo, se necesitan con más urgencia actividades de mitigación.

3.2.1 PROCESO S4: IDENTIFICAR Y ANALIZAR RIESGOS

Para analizar los riesgos encontrados en los Pasos 1 – 21, se necesita definir inicialmente la intensidad del impacto de las amenazas identificadas para dada uno de los activos críticos. El riesgo es la probabilidad de que una amenaza ocurra, por ello se debe determinar lo que se entiende como probabilidad, para luego utilizarla como referencia para identificar la mayor posibilidad de ocurrencia a futuro de eventos de una amenaza.

3.2.1.1 Actividad S4.1: Evaluar los Impactos de las Amenazas

Paso 22

Con los Criterios de Evaluación del Impacto ya obtenidos en **el Paso 1** se registra el potencial daño a la seguridad en las áreas ya indicadas en ese Paso, para los diferentes árboles de amenaza, en los correspondientes cuadros en las Hojas de Trabajo de Perfil de Riesgo de cada activo crítico.

El equipo de evaluación tomó muy en cuenta la experiencia del personal de TI, y del personal entrevistado para ayudar a estimar los valores de ciertas amenazas. El personal del Instituto Geofísico ha estado muy abierto a responder cualquier inquietud en materias de gestión pública.

Se han registrado los siguientes valores d impacto para los activos críticos del Instituto Geofísico:

a) Sistema de Información Sísmico y Volcánico, SISV

Los atacantes humanos que accesan a la red de información en general podrían tener un alto impacto en el área de disminución de la productividad sea por la pérdida, destrucción o interrupción del flujo de información. Para el Instituto Geofísico, las personas son seleccionadas por su honorabilidad y es muy baja la posibilidad que el atacante sea interno.

El posible impacto del actor humano que utiliza el acceso físico para atacar a la red se lo considera en general de bajo a medio. Hay que notar que solamente la disminución de productividad se vería afectada con alto impacto, debido a la pérdida y destrucción e interrupción de información.

Los problemas que se presentan cuando fallan la provisión de los servicios de las empresas tercerizadoras influyen sobre la pérdida de reputación y la baja en la productividad, lo que tiene un considerable impacto en caso de que se interrumpa el acceso al SISV. Se depende mucho del enlace de ISP para transmitir información del SISV hacia el exterior. Es verdad que actualmente hay medios alternativos como los medios inalámbricos, pero éstos no se los considera viables, por su elevado costo.

Los problemas de fuente de energía y los desastres naturales ocasionarían interrupción y pérdida de información, lo cual tendría un alto impacto en la baja de productividad. Los problemas de fuente de energía harían que el Instituto Geofísico tenga una mala imagen frente a la opinión pública. En contraste el efecto negativo de los desastres naturales serían más comprendidos por la opinión pública, puesto que su control generalmente rebasa cualquier previsión humana.

La deficiente configuración física actual tendría un alto impacto sobre la baja de productividad, pérdida financiera y la consiguiente pérdida de credibilidad de los usuarios. Por esta deficiente configuración, hay peligro de revelación, modificación no autorizada, y pérdida de información.

b) Información de Usuarios, Informes y Documental , IUIID

El posible impacto del actor humano que utiliza el acceso físico para atacar a la red se lo considera solamente desde dentro para IUIID. Hay que notar que solamente la disminución de productividad se vería afectada con un alto impacto por el atacante desde dentro, con la consiguiente modificación, pérdida e interrupción de esta información. Si el atacante viene de fuera se incluye la revelación no autorizada, junto con la modificación, pérdida e interrupción de la información como de medio a alto impacto, sobre el área financiera, así como en la disminución de la productividad.

c) Personal de Tecnología Informática en conjunto con el Personal de Monitoreo, TI + PMV

Las personas clave que toman permiso temporal o dejan permanentemente la organización pueden convertirse en actores de amenaza y ocasionar un alto impacto en la credibilidad de los usuarios y en la disminución de la productividad, al ocasionar revelación no autorizada, interrupción, pérdida, modificación o destrucción de información.

La configuración física de las instalaciones es muy incómoda, lo cual puede tener un impacto alto en la disminución de la productividad de las personas, además el prestigio de la institución puede verse afectado, y también puede haber pérdidas financieras por esa baja de productividad.

d) Computadores Personales, PCs

Los actores humanos que accesan a la red de información son el mismo personal interno del Instituto Geofísico. De darse un ataque, éste podría tener una tendencia de alto impacto en el área de disminución de la productividad y en la reputación de la Institución, sea por la revelación no autorizada, pérdida, destrucción o interrupción del flujo de información. Para el Instituto Geofísico, las personas son seleccionadas por su honorabilidad y es muy baja la posibilidad que el personal interno dañe deliberadamente a las PCs.

El posible impacto del actor humano que utiliza el acceso físico para atacar a las estaciones de trabajo o PCs, se lo considera en general de bajo a medio. Hay

que notar que solamente la disminución de productividad se vería afectada con un alto impacto, debido a la pérdida destrucción e interrupción de información en las PCs. .

En cuanto a los problemas de sistemas, como es el caso de los defectos de hardware y software, el código malicioso, la interrupción de operaciones del sistema, se consideró la pérdida de reputación y la baja en la productividad como de considerable impacto en caso de que se interrumpa el acceso a las PCs en caso de que haya pérdida, destrucción o interrupción de información en el normal funcionamiento de las PCs. En el caso de código malicioso en las PCs, puede haber revelación de códigos no autorizados, y también modificación de valiosa información, lo cual tiende a un impacto alto en la baja de productividad y reputación.

A los problemas ocasionados por fallas en la fuente de energía, en las telecomunicaciones y los desastres naturales, se añaden los problemas ocasionados por la interrupción de los servicios de las empresas tercerizadoras. Estos problemas ya fueron tratados en SISV más arriba. Sin embargo, para las PCs el impacto de la interrupción de los servicios de las empresas tercerizadoras es considerado cualitativamente bajo, ya que las PCs del Instituto Geofísico continúan sus operaciones con o sin ellas.

La deficiente configuración física actual también ya fue analizada en SISV, y la apreciación del impacto es similar para las PCs.

Los problemas ocasionados por la obsolescencia de los equipos y aplicaciones pueden ocasionar pérdida, destrucción o interrupción de las operaciones de las PCs. Esto es considerado de alto impacto para las áreas de pérdida de credibilidad o reputación, mayores costos financieros y baja en la productividad de las PCs. El mismo efecto de la obsolescencia se puede aplicar al presupuesto inflexible, esto se debe talvez a que la obsolescencia no puede superarse porque no existe presupuesto oportuno y adecuado a las necesidades actuales.

e) Centro de Información y Respaldos, CIR

Si bien es cierto el SISV es un activo de orden lógico o programas, el CIR es un activo más de orden físico, pues son respaldos en cintas, en discos y otros medios magnéticos y en papel, sin embargo se pueden aplicar los mismos

criterios de evaluación de impacto de los actores humanos que utilizan el acceso físico de SISV.

Igualmente se considera, al tratar sobre las personas clave que dejan temporal o permanentemente la organización, se aplican los mismos criterios ya analizados para TI + PMV.

Para los problemas de configuración física y de eventuales desastres naturales se aplican los mismos criterios de impacto ya mencionados para las PCs o computadores personales.

En las Hojas de Trabajo de Notas y Recomendaciones, se puntualiza que los criterios de evaluación deben ser más ampliamente revisados y aprobados por el Comité Técnico en un futuro cercano, ya que no se trata de valores exactos cuantitativos, sino más bien una apreciación cualitativa de acuerdo a la experiencia del equipo de análisis.

3.2.1.2 Actividad S4.2: Establecer Criterios de Evaluación de Probabilidad

Paso 23

Con la experiencia y habilidad del personal de TI se establecieron los Criterios de Evaluación de Probabilidad en la Hoja de Trabajo correspondiente Como no se tiene información histórica documentada de eventos de ataque contra la seguridad en el pasado, el equipo opina que si el número de veces de ocurrencia de un evento por año está **entre uno y cuatro**, se puede considerar una probabilidad de tipo medio, si es **mayor que cuatro veces** al año tiene una frecuencia **alta** de ocurrencia, y si es **menor de una vez** al año puede considerarse como **baja** la probabilidad de un evento.

3.2.1.3 Actividad S4.3: Evaluar Probabilidades de Amenazas

Paso 24

No se tienen datos históricos de pruebas de vulnerabilidad con herramientas de penetración de red, ni por escaneo o monitoreo, y en general no se posee información de las amenazas contra la red de información. Por ello se tiene poca confianza en las estimaciones de probabilidad. Sin embargo, para la mayoría de amenazas a los activos críticos se confía en la experiencia y el conocimiento del personal de tecnología de información para estimar de manera aproximada el número de ocurrencias de los eventos de amenaza en periodos de un año. Los eventos del pasado, sirven de indicadores para prevenir los probables ataques en el futuro

Así se estimó el número de ocurrencias de los eventos que para los diferentes activos críticos de la siguiente manera:

a) Sistema de Información Sísmico y Volcánico, SISV

Los atacantes humanos que accesan a la red de información han ocasionado pérdidas, destrucción e interrupción de información de manera accidental más de cinco veces al año. Más de 20 veces al año se ha revela de manera deliberada información sensitiva.

El número de ocurrencias por año del actor humano interno que utiliza el acceso físico se ha dado más de 10 veces, cuando se revela de manera accidental información sensitiva al dejar activos los programas para que los vean aquellos usuarios no autorizados para ello.

Más de 5 veces al año ha habido interrupciones por fallas en el SISV, aunque esto está relacionado más a problemas de hardware que de software.

Se han presentado más de 20 eventos de interrupción de los servicios de la proveedora del ISP, lo cual hace que se dificulte la comunicación por Internet para elaborar informes utilizando el SISV. Se depende mucho del enlace de ISP para transmitir información del SISV hacia el exterior.

Los problemas de fuente de energía han ocasionado más de cinco eventos de interrupción por año, lo cual indica una probabilidad considerable de ocurrencia y reiteración en el futuro.

La deficiente configuración física ha ocasionado más de 20 eventos de revelación no autorizada, y más de 10 de modificación y pérdida de información en un año. Lo cual es un indicador de que esta amenaza puede repetirse en el futuro con una alta probabilidad.

b) Información de Usuarios, Informes y Documental, IUIID

El posible impacto del actor humano que utiliza el acceso físico para atacar a la red se lo considera solamente desde dentro para IUIID. Se pueden perder o destruir archivos o información de manera accidental, pues en el pasado esto ha ocurrido más de 10 veces por año.

c) Personal de Tecnología Informática junto con el de Monitoreo Volcánico, TI + PMV

Las personas clave que toman permiso temporal de inasistencia en el pasado han ocasionado la interrupción de provisión de sus servicios por más de 6 ocasiones el año pasado. Este hecho indica que puede producirse nuevamente la interrupción por la no presencia del personal de TI + PMV de manera oportuna.

La deficiente configuración física ha ocasionado más de 10 eventos de interrupción de los servicios del personal de TI + PMV. En estos momentos se presenta el problema de que mientras se construye la nueva infraestructura, el personal no puede laborar normalmente, Así que la probabilidad de interrupción del servicio por ausencia del personal es relativamente alta.

d) Computadores Personales, PCs

Los actores humanos que accesan a la red de información son el mismo personal interno del Instituto Geofísico. Ha ocurrido más de 20 veces por año, la revelación no autorizada de información en las PCs, lo cual indica que la probabilidad de que estos eventos se repitan es alta, en caso de no aplicar correctivos de control de acceso a la red.

La ocurrencia de eventos de ataque por parte del actor humano externo que utiliza el acceso físico, quien de manera accidental revela información no autorizada ha sido de más 10 veces por año, lo cual indica que las débiles políticas de acceso físico fuera del horario normal de trabajo, hacen muy probable el evento que personas no autorizadas puedan accesar a las estaciones de trabajo o PCs,

En cuanto a los problemas de sistemas, se ha presentado interrupción de operaciones de las PCs por defectos más de hardware que de software, entre 10 y 20 eventos por año, lo cual es de consideración para tratar de corregir estos defectos para que disminuya la probabilidad de que estos eventos ocurran a futuro.

El código malicioso ha ocasionado por más de 50 veces la interrupción de operaciones de las PCs. Por el número de eventos, este tipo de ataque es el más problemático y de mayor probabilidad de ocurrencia.

La interrupción de operaciones de las PCs, ocasionada por fallas en la fuente de energía, en las telecomunicaciones y los problemas ocasionados por la falta de provisión de los servicios de las empresas tercerizadoras han ocurrido más de 10 veces por año, por lo cual son considerados de alta probabilidad de ocurrencia a futuro.

La deficiente configuración física actual ha ocasionado eventos de revelación no autorizada de información de las PCs, por más de 10 veces al año. Este hecho es similar al analizado en SISV, y la probabilidad de ocurrencia es similar para las PCs.

Los problemas ocasionados por la obsolescencia de los equipos y aplicaciones pueden ocasionar pérdida, destrucción o interrupción de las operaciones de las PCs.

10 veces por año han ocurrido de eventos de pérdida o destrucción de información de las PCs, debido la obsolescencia relacionada con el presupuesto inflexible que no ha permitido renovar los equipos y programas.

e) Centro de Información y Respaldos, CIR

Para el CIR, no se han registrado eventos de ataque, lo cual no obsta que se considere hacia futuro la protección física de los respaldos, ya que siempre

existe la probabilidad de desastres naturales, lo cual puede tomarse de las mismas recomendaciones que se haga para la seguridad física de las PCs, y aplicarse a CIR.

En las Hojas de Trabajo de Notas y Recomendaciones, se puntualiza que los criterios de evaluación deben ser más ampliamente revisados y aprobados por el Comité Técnico en un futuro cercano, ya que no se trata de valores exactos cuantitativos, sino más bien una apreciación cualitativa de acuerdo a la experiencia del equipo de análisis.

No se identificaron Acciones, Notas, o Recomendaciones adicionales durante el Proceso S4.

3.2.2 PROCESO S5: DESARROLLAR ESTRATEGIAS DE PROTECCIÓN Y PLANES DE MITIGACIÓN

3.2.2.1 Actividad S5.1: Describir Estrategia de Protección Actual

Paso 25

No todas las áreas de práctica de seguridad son defectuosas. Los siguientes procedimientos permitirán seleccionar solamente aquellas áreas más necesitadas de actividades concretas de mitigación. En este paso se transfieren los estados de semáforo, Rojo, Amarillo y Verde a las Hojas de Trabajo de Estrategias de Protección, puesto que existen sendas Hojas para las Áreas de Práctica de Seguridad. El método sugiere una Estrategia de Protección, para cada Área de Práctica de Seguridad. Pero se debe **optimizar el criterio**, al seleccionar solamente aquellas áreas más débiles, cuya seguridad de datos esté muy cuestionada. Parecería que el estado de semáforo Rojo nos daría una aproximación, pero se necesitan considerar otros factores. Se vuelven a revisar las Hojas de Trabajo de Práctica de Seguridad y se señalan con todo el conocimiento que se posee hasta este momento, cuáles serían las posibles áreas candidatas al plan de mitigación. Hasta este momento solamente se revisan las

áreas de práctica más débiles luego de haber recorrido los pasos 1 - 24 que se han seguido hasta este punto.

3.2.2.2 Actividad S5.2: Seleccionar Enfoques de Mitigación

Paso 26

Se transcriben los estados de semáforo de las Hojas de Trabajo de Áreas de Práctica de Seguridad a las casillas correspondientes a este Paso 26, en las Hojas de Trabajo de Perfil de Riesgo de cada Activo Crítico. **De esta forma se tiene una visión sinóptica** de la interacción de los árboles de amenaza, con las probabilidades encontradas y sobre todo con las Áreas de Práctica de Seguridad en esta matriz de aproximación de Perfil de Riesgo para cada uno de los Activos Críticos.

Paso 27

Tomando en cuenta que la alta probabilidad de ocurrencia, y también el alto impacto que puede tener una amenaza, se marca entonces la casilla “para mitigación”. Luego se dibujan círculos en las Áreas de Práctica de seguridad intersecantes con los eventos de amenaza considerados “para mitigación”. Según se puede ver en el **Cuadro 8**, de manera resumida se muestran las áreas de práctica de seguridad con mayor necesidad de mitigación. Las marcas con “x” corresponden a los círculos sobre las áreas de práctica de seguridad íntersecantes con las ramas de los árboles de amenaza en las Hojas de Trabajo de Perfil de Riesgo para cada activo crítico.

Activos Críticos \ Prácticas de Seguridad	1. Entrenamiento Alertas de Seguridad	2. Estrategia de Seguridad	3. Gestión de Seguridad	4. Políticas Regulaciones	5. Gestión Seguridad Colaborativa	6. Planeación de Contingencias	7. Control de Acceso Físico	8. Monitoreo de Seguridad Física	9. Gestión Sistemas & Red	10. Monitoreo de la Seguridad de TI	11. Autenticación & Autorización	12. Gestión de Vulnerabilidades	13. De encriptación	14. Arquitectura & Diseño de Seg.	15. Gestión de Incidentes
SISV	X X		X X		X	X	X X	X	X X		X				
IUIID			X				X	X							
SubÁrea de TI + PMV			X X				X	X						X	
PCs	X		X X			X	X	X	X	X	X			X	
CIR			X				X	X							

Cuadro 8.- Activos Críticos versus Áreas de Práctica de Seguridad con mayor necesidad de mitigación

El equipo de análisis definió los criterios de selección de las áreas con mayor necesidad de mitigación, según el siguiente orden de importancia:

1) Riesgos que por una mala práctica de seguridad pongan en **peligro de pérdida o grave afectación de información de los sistemas** del Instituto Geofísico. Por ejemplo, riesgos con un valor alto de impacto sobre el área de la "seguridad de los activos críticos". La reputación e impactos financieros, se consideran en este punto como factores secundarios en una relación directa con la misión del Instituto Geofísico.

2) Riesgos **que afectan al requerimiento más importante** de seguridad del activo crítico de mayor interés. Según indica en el Paso 10, la **disponibilidad** es el más importante requerimiento del Sistema de Información Sísmica y Volcánica.

3) Riesgos ligados con **áreas de atención específicas** del activo crítico. Como aquellas tratadas en las Hojas de Perfil de Riesgos de cada Activo Crítico.

Si se comparan dos riesgos similares se escoge el de mayor riesgo según su mayor impacto y precedencia según los criterios definidos en los literales anteriores 1), 2) y 3).

Solo en las estrategias de seguridad así escogidas, se sugerirán los procedimientos y actividades para mitigar cada riesgo y de esta forma la relación causa-efecto se revierta en favor de la seguridad.

Se seleccionaron las siguientes áreas de práctica de seguridad como áreas de mitigación:

I. **La Gestión de la Seguridad** incluye la práctica **de Avisos de Seguridad y Entrenamiento**, y además abarca todas las áreas en las cuales la organización representada en sus jefes, toma decisiones a favor de la seguridad de la información. Esto incluye la acertada gestión de todos los recursos humanos en relación con los sistemas. Esta práctica de seguridad es la que generalmente los planes de seguridad informática no la toman como principal y de la más grande importancia. La gestión adecuada de la seguridad incluye la **Gestión de Seguridad Colaborativa** que tiene que ver con las empresas contratadas para proveer servicios, los proveedores de hardware y software, y aquellas organizaciones que tengan convenios, y provean servicios o apoyo a la misión del Instituto Geofísico. Además la decisión para realizar planes de contingencia y seguridad de los datos también depende de la adecuada gestión del Comité Técnico y el Jefe de Departamento.

II. Más que **el Monitoreo y Auditoría de Seguridad Física** se debe incluir el **Control de Acceso Físico** como una necesidad inmediata para la seguridad de los equipos que guardan información sensitiva. Con respecto al Área de Seguridad Física, el Departamento de Servicios Generales de la EPN, contrata a la empresa que provee de guardias de seguridad para el ingreso

al campus de la EPN. Esta área también incluye el impacto de los desastres naturales, el fuego, la inundación, las pérdidas de equipos o información por robo o negligencia.

III. **La Gestión de Sistemas y Red de Información** es talvez el área que más se enfoca en la administración y monitoreo de la red. Se sugiere el uso de herramientas y mecanismos de monitoreo de red, para encontrar vulnerabilidades y aplicar las correcciones necesarias. **También dentro de la Gestión de Sistemas y Red de Información** está la práctica de **Autenticación y Autorización** en cuanto se gestionan los accesos mediante contraseñas y bitácora de cuentas de ingreso por parte del Administrador de la Red. Ya que no se emplean medios consistentes de control de acceso para sus sistemas y redes de información, esta área se la considera para mitigación.

IV. **Diseño y Arquitectura de Seguridad** se escoge como área de mitigación, ya que la topología de red no es óptima, y requiere cambios para implementar las seguridades sugeridas. Quienes gestionan la adquisición de hardware y software para la implementación de la seguridad son el Comité Técnico dirigidos por el Jefe de Departamento, bajo el asesoramiento del personal del Área Técnica. Quienes implementan la instalación, prueba y administración del nuevo software son los miembros del personal de TI, cuyas actividades en este caso tienen que ver más con la **Gestión de Sistemas y Red**. Si bien es cierto que la implementación de los planes de la nueva infraestructura de hardware son tercerizados a empresas locales, sin embargo una buena documentación del plan de seguridad de los datos puede facilitar el trabajo de la empresa a ser contratada.

*S*e documentaron las razones para seleccionar cada área en *las Hojas de Trabajo de Notas y Recomendaciones.*

3.2.2.3 Actividad S5.3: Desarrollar Planes de Mitigación del Riesgo

Paso 28

Los planes de mitigación se desarrollan para cada área de práctica de seguridad seleccionada en las Hojas de Trabajo del Plan de Mitigación. El plan para cada área seleccionada incluye las actividades específicas diseñadas para mitigar sus correspondientes riesgos. Cuando se define cada actividad de mitigación, también se registran las razones para escoger esa actividad particular para mitigar o mejorar, y quién deber ser responsable de ella, y cualquier gestión de acción adicional que podría ser requerida para implementarla.

3.2.2.4 Actividad S5.4: Identificar Cambios en la Estrategia de Protección

Paso 29

Con las Hojas de Trabajo de las Estrategias de Protección, se revisan cada una de las estrategias seleccionadas, y de haber cualquier cambio que afecte la estrategia de protección para la respectiva área de práctica de seguridad, se transcriben estas sugerencias de cambio a la casilla de las actividades dentro los planes de mitigación que se quieren implementar. Si la estrategia propone un cambio se lo incluye dentro de la actividad correspondiente. En este paso también se escriben Notas de cómo cambian las diferentes estrategias de protección interrelacionadas unas con otras.

PLAN DE MITIGACIÓN

A continuación se desarrollan las actividades de mitigación para las diferentes áreas seleccionadas de práctica de seguridad. Se asignan los responsables de la actividad, se explica también la razón para haberla seleccionado y el soporte adicional a futuro. Además se anotan las interrelaciones entre las diferentes actividades por áreas.

I. Área de Mitigación: Gestión de la seguridad

a) Roles y responsabilidad

El Jefe de TI debe promover el formalizar y documentar los roles y responsabilidades del personal de Tecnología de la Información sobre la seguridad de la información, actualmente esta actividad se lo lleva de manera informal y no documentada. Toda la responsabilidad del manejo de la seguridad de datos actualmente se concentra en el Administrador de Red, y esto es inaceptable, pues hay sobrecarga de trabajo y responsabilidades.

Hay que notar que esto cambiará la estrategia de Gestión de Sistemas y Red de Información, al otorgar mayor responsabilidad al personal de TI, bajo la supervisión del Jefe de Área.

Se deben también documentar los relevos y los ingresos a nómina, y correlacionarlos con la responsabilidad de la seguridad de la información que maneja cada persona. Es por ello que se debe formalizar un *acuerdo de responsabilidad* sobre la información a cargo de cada uno de los miembros del Instituto Geofísico para aumentar su compromiso sobre la información que manejan. Este acuerdo debe ser firmado por el personal actual y por el personal nuevo en el momento en que firman sus contratos de trabajo con la Escuela Politécnica. El Jefe de Departamento supervisará esta actividad para todo el personal.

b) Gestión de presupuesto

El Jefe de Departamento y el Comité Técnico, en coordinación con el Departamento Financiero de la EPN deben incluir en el presupuesto anual una partida explícita para actividades de seguridad de la información diferente de

aquella destinada a la de tecnología de información. El nivel de gestión de los fondos se determinará utilizando procesos formales de evaluación de riesgos. La información sísmica y volcánica es de mucha importancia, por lo cual se debe considerar en gran medida la evaluación formal y documentada de los riesgos de la información sísmica y volcánica, para una mejor gestión del presupuesto para seguridad de datos.

c) Procedimientos de recursos humanos

El Área Administrativa en coordinación con el Departamento de Recursos Humanos de la Escuela Politécnica y el Jefe de Departamento, deben diseñar procedimientos formales y documentados para incluir consideraciones sobre seguridad en los procesos de contratación de personal, como por ejemplo, chequeos de antecedentes, y también para la terminación de contratos, sea por ejemplo, quitar el acceso a todos los sistemas e información a los empleados despedidos o que hayan renunciado.

Estos procedimientos actualmente son muy superficiales y el quitar los privilegios de acceso está muy descuidado.

Nótese que al quitar los accesos a los ex – empleados, se modifica en algo la estrategia de protección para Área de Autenticación y Autorización. El Administrador de Red deberá actualizar la lista de cuentas de usuario y correlacionarla con la lista de nómina aprobada por el Jefe de Departamento.

También se sugiere que el Administrador de Red actualice el listado para ser utilizado por el personal de monitoreo de quiénes son los miembros oficialmente en nómina, los estudiantes y tesistas autorizados para el manejo de información, y de esta manera formalizar un registro escrito de responsables de la seguridad de la información y los equipos que ellos manejan.

Un programador del personal de TI actualizará la información sobre la distribución del personal por áreas de manera periódica en el WebSite del Instituto Geofísico. De esta forma se puede conocer en línea quién pertenece y quién es el responsable de la seguridad de la información en las diferentes áreas, cada vez que existan cambios o remoción de personal.

d) Gestión de riesgos

El personal de TI en coordinación con su jefe, formalizará y documentará la gestión de riesgos de seguridad de la información. También se debe formalizar y

documentar el proceso de esta gestión de riesgos. En especial en las Áreas de Sismología y Vulcanología.

Se debe anotar que el documentar y formalizar la Gestión de Riesgos cambia la estrategia del Área de Gestión de Sistemas y Red de Información, ya que con una adecuada documentación, se informa mejor al Comité Técnico y al Jefe de Departamento, y de esta forma se motiva a tomar conciencia de la importancia de proteger información valiosa y sensitiva como la de Vulcanología y Sismología. En especial, si está bien documentada la gestión de riesgos sirve de documento de apoyo para la gestión de presupuesto. Además, este Plan de Seguridad puede servir de base para la documentación de futuras políticas de seguridad, una vez que sea aprobado por el Comité Técnico.

e) Alertas al personal

Un miembro del personal de TI designado por su respectivo jefe, debe desarrollar un programa de entrenamiento básico en alertas de seguridad que incluya información actualizada acerca del proceso de gestión de la seguridad. Esto debe hacerse por lo menos una vez al año. El personal de TI debe asistir a la Facultad de Sistemas de la EPN para recibir cursos de actualización en seguridad de datos. A su vez, la persona de TI encargada de adaptar el curso de entrenamiento en seguridad de datos tomará en cuenta que las personas del Instituto Geofísico no son informáticos, y tratará de sintetizar lo más importante de los contenidos para aplicarlos de manera sencilla, a la práctica diaria de la prevención y mitigación de riesgos de la información que manejan.

Para los nuevos miembros del personal, y como parte de sus actividades de orientación se les debe proveer de un documento básico de entrenamiento en alertas de seguridad de datos. Este documento puede estar disponible en el correo interno, para que todo el personal tenga acceso a él, cuando así lo requiera. Como material adicional puede hacerse un manual de alertas de seguridad, que incluya formas de limpiar de virus, y procedimientos a seguir en caso de fallas en los programas y sistemas. La elaboración del documento y su envío al correo interno estarán a cargo de la persona de TI designada por su respectivo jefe

Hay que anotar que esta actividad ocasiona un cambio de Estrategia de Protección para el Área de Avisos de Seguridad y Entrenamiento

f) Alertas para la gestión

Se debe implementar un mecanismo formal para proveer a los Jefes de Área y de Departamento con resúmenes de información de importancia sobre seguridad de los datos por lo menos trimestralmente. Es por ello que el Administrador de Red elaborará una plantilla de resumen ejecutivo sobre seguridad de información y la distribuirá por cualquier medio magnético o escrito a los Jefes de Área y Departamento. Los Jefes de Área y de Departamento deben interesarse en esta actividad. Ellos deben leer este resumen ejecutivo, en donde constarán las políticas básicas de seguridad, manejo de cuentas de usuarios, chequear al personal autorizado, cambios frecuentes de contraseñas, formas de eliminación de virus, métodos de protección de material sensitivo, etc.

II. Área de Mitigación: Gestión de la Seguridad Colaborativa

a) Colaboradores y socios

En cada uno de los convenios que el Instituto Geofísico realiza con otras instituciones como el Instituto Geográfico Militar, Empresa Municipal de Alcantarillado y Agua Potable, el Ilustre Municipio de Quito, etc., así como en los acuerdos de cooperación con organismos internacionales como el BGR[69], JICA[70], etc., se deben documentar las políticas y procedimientos de seguridad de la información, y establecer la categoría de disponibilidad, sea ésta pública o confidencial, de los datos que se manejan según los lineamientos del ODEPLAN[71]. El Jefe de TI, junto con el Jefe del Área Técnica, tomarán a su cargo la elaboración de este documento para que luego de ser aprobado por el Jefe de Departamento, se anexará a la firma de estos convenios de manera obligatoria.

i. Contratistas y subcontratistas

Si bien es cierto, en el WebSite del Instituto Geofísico se hallan documentados los requerimientos de protección de información para los contratistas y subcontratistas, sin embargo estas políticas son informales y no documentadas, así como procedimientos son muy laxos para proteger otros tipos de información.

---

[69] BGR es el Organismo de Geociencias y Recursos Naturales de la República Federal de Alemania.
[70] JICA es el convenio de desarrollo con Japón.
[71] El ODEPLAN se encarga de definir y normar estándares de producción de información geográfica y protocolos de intercambio de datos. Cfr. Literal 1.1.6 La información del Instituto Geofísico en la infraestructura de datos espaciales.

Cuando se ha contratado a personas o empresas independientes para tareas delicadas sobre seguridad de información, no se ha documentado ni acordado la responsabilidad sobre lo que este personal externo maneja. Es por ello que el Jefe de TI, en conjunto con el Jefe del Área Técnica, elaborará también documentos de responsabilidad y confidencialidad de la información, los cuales, luego de ser aprobados por el Jefe de Departamento, se anexarán a la firma de los contratos con personal externo al Instituto Geofísico.

II. Proveedoras de servicios

De la misma manera que con los contratistas y subcontratistas, el Jefe de TI junto con el Jefe del Área Técnica, y bajo la supervisión del Jefe de Departamento procederán a elaborar documentos de responsabilidad y confidencialidad, los cuales se anexarán luego de ser aprobados, a la firma de contratos con las empresas proveedoras de servicios.

De esta forma se puede ejercer control y tener respaldo legal en caso de que se den abusos de la información que manejan estas empresas. Así, la proveedora de ISP se responsabiliza de la integridad de la publicación en la Web del mensaje enviado, y por la no divulgación de direcciones, protocolos e identidades del personal del Instituto Geofísico, tampoco puede comercializar las imágenes o resultados de investigaciones sin el permiso de sus autores. Igualmente las empresas que venden licencias de software deben guardar la confidencialidad de estos datos privados y personales del Instituto Geofísico. Las empresas proveedoras de mantenimiento de hardware y cableado estructurado no podrán divulgar ni peor comercializar las configuraciones, formas de instalación, mapas de la red interna, sin la autorización escrita del Jefe de Departamento.

b) Requerimientos y verificación del cumplimiento

En los documentos de confidencialidad antes mencionados se deben comunicar los requerimientos de protección de información sensitiva a todo el personal externo que haya sido contratado. Para ello el Jefe del Área Técnica se reunirá cada dos meses con el Jefe de TI y el miembro de su Área con mayor experiencia en mantenimiento en hardware para elaborar y aprobar la lista de requerimientos de seguridad de información. Esta lista se añadirá al documento de acuerdo de confidencialidad y responsabilidad. Luego que se hayan firmado los contratos, el jefe del Área Técnica verificará el cumplimiento de estos requerimientos de

seguridad, mientras y después se otorga el servicio, e informará por escrito al Jefe de Departamento sobre este particular.

Hay que anotar que esta actividad cambiará la estrategia de Gestión de la Seguridad, puesto que se asignarán mayores responsabilidades al Jefe de TI y al Jefe del Área Técnica.

III. Área de Mitigación: Control de Acceso Físico

a) Responsabilidad

La responsabilidad de control de acceso fuera del horario normal de trabajo no está asignada de manera formal. Actualmente el llevar el registro de admisión, no se lo correlaciona con el personal encargado por turnos, en especial en la noche cuando el personal administrativo no está presente. Es por ello que la responsabilidad del control de acceso a las instalaciones debe ser reasignada y redistribuida. Durante el horario normal de trabajo el personal administrativo controla el ingreso de manera verbal, y sin llevar registro escrito. El Jefe del Área Administrativa bajo la supervisión del Jefe de Departamento, debe asignar los turnos para personal administrativo encargado del registro de control en horarios normales de trabajo. El Jefe del Área Administrativa bajo la supervisión del Jefe de Departamento presentará las listas semanales tanto de los turnos de los empleados administrativos, como el registro escrito de control.

Y fuera de los horarios normales de trabajo, se asigna la responsabilidad de control de acceso físico, al personal de monitoreo que esté de turno, mediante la verificación de listas de personas autorizadas para el efecto.

Los turnos del personal de monitoreo autorizado para trabajar en feriados, fines de semana y en la noche, lo supervisará directamente el Jefe de Departamento con listas de personas quienes le solicitarán por escrito la autorización para quedarse en ese horario en las instalaciones, y se responsabilizan inclusive pecuniariamente de los bienes a ellos encomendados. El Jefe del Área Administrativa recogerá la copia de la lista del personal de monitoreo autorizada para el ingreso, en la oficina del Jefe de Departamento y la verificará con la copia que este personal debe firmar en la puerta de ingreso, y que la tendrán los guardias de seguridad.

Se debe anotar que esta actividad provocará cambios en la estrategia de Monitoreo de Seguridad Física.

b) Procedimientos

Actualmente, los procedimientos de control de acceso físico se los lleva de manera muy laxa. No hay registro escrito de admisión, y fuera de los horarios de trabajo se manejan listas de acceso de manera muy informal. Formalizar los procedimientos ayudaría a asegurar que éstos sean aplicados coherentemente por todos los miembros del personal asignado. Se deben documentar procedimientos formales para controlar el acceso físico para el ingreso a las instalaciones, a las áreas de trabajo, y la consiguiente proximidad de personas ajenas con equipos delicados e información sensitiva. Se elaborará el registro escrito de la hora de ingreso, motivo y cédula de identidad de los visitantes o personas ajenas al Instituto Geofísico. El distintivo o escarapela de visitante puede servir de identificación provisional durante su periplo. Además los visitantes deben estar siempre guiados y acompañados por algún miembro del personal del Instituto Geofísico. El Jefe del Área Administrativa bajo la supervisión del Jefe de Departamento asignará la tarea de elaboración del registro de visitantes a un empleado administrativo. El Jefe del Área Administrativa se encargará de documentar los procedimientos para control de acceso físico.

c) Asuntos colaborativos

La responsabilidad del control de acceso físico es asignada al Área Administrativa y a la empresa contratada de guardias de seguridad del campus de la Escuela Politécnica Nacional, bajo la supervisión del Departamento de Servicios Generales. Las actividades no están actualmente coordinadas entre estos dos estamentos. Al asignar un elemento de enlace y para trabajar en conjunto con con el personal del grupo de guardias de seguridad, debería mejorar la comunicación de los requerimientos y el cómo se gestiona el control de acceso físico. Como ya se mencionó en los procedimientos, las listas de control de acceso fuera de los horarios normales de trabajo, serán verificadas por el Jefe del Área Administrativa en coordinación con los guardias de seguridad.

El Jefe del Área Administrativa será responsable de comunicar los nuevos procedimientos para el control de ingreso del personal fuera de los horarios

normales de trabajo al Departamento de Servicios Generales para los guardias de seguridad sean informados sobre este particular.

Se debe anotar que esto cambiará la estrategia de monitoreo de la Seguridad Física del IGEPN

IV. Área de Mitigación: Monitoreo y Auditoría de Seguridad Física

Se debe recalcar que todo lo que se ha establecido referente a Control de Acceso Físico en el punto anterior, se lo puede aplicar dentro del Monitoreo y Auditoría de Seguridad Física, ya que la seguridad física incluye al control del acceso físico.

a) Responsabilidad

Los Jefes de las Áreas Administrativa y Técnica gestionarán la adquisición de los seguros y equipos de seguridad física ante el Comité Técnico, para que una vez que sea aprobado, sean incluidos en el presupuesto del siguiente año. Todo esto bajo la supervisión del Jefe de Departamento.

b) Procedimientos

El formalizar los procedimientos de monitoreo seguridad física, ayudaría a asegurar que éstos sean aplicados coherentemente por todos los miembros del personal, y así aumentaría el control frente para evitar pérdidas de información o equipos por cualquier causa. Por ello, el documentar planes y procedimientos formales para monitorear el acceso físico a todo el hardware de TI y a los medios de software se vuelve una necesidad imperiosa. De ahí que las actividades que se proponen en a continuación, de ser aprobadas por el Comité Técnico pueden constituirse en un documento formal de gran ayuda para implementarlas:

c) Actividades:

El Administrador de la Red en conjunto con el Jefe de TI, se encargarán de llevar el registro y monitoreo bimensual del inventario de los equipos y del software existente, para así tener inventarios actualizados de manera periódica.

Si bien existen herramientas de control de inventario por software, también puede elaborarse manualmente el control de inventario con la ayuda de programas utilitarios para el efecto.

Nótese que esta actividad tiene que ver con la estrategia de Gestión de Sistemas y Administración de la Red, en cuanto se utilicen herramientas automáticas para el control de inventarios.

Actividades adicionales:

- Gestionar la compra de armarios de acero con candado para respaldos de información a por lo menos 50 cm. del suelo para proteger las copias de los respaldos. Esta actividad se la puede gestionar a través del Departamento de Adquisición e Inventario de Bienes de la Escuela Politécnica Nacional.
- Elaborar letreros de No-Fumar en los baños y en las áreas de trabajo. Alertas para separar sustancias peligrosas como tintas inflamables de las personas y los equipos. Se encargará de esto a miembros del Área Técnica en conjunto con el Área Administrativa.
- Ampliar los requerimientos a nivel de control de acceso físico, al impedir el acceso de personas con cigarrillos encendidos o en estado etílico dentro de las instalaciones.

Hay que anotar que el impedir el acceso a personas con cigarrillos o en estado etílico le corresponde al Jefe del Área Administrativa informar y ordenar al personal encargado, se incluya este particular en los nuevos procedimientos de Control de Acceso Físico.

A manera de sugerencia, todos los miembros del Instituto Geofísico deberían asistir a cursos de entrenamiento en seguridad física, procedimientos de evacuación, control de incendios, etc. Existe en la EPN, la posibilidad de seguir cursos de seguridad industrial. De ser posible, en las mismas empresas que venden los equipos de seguridad física, se pueden seguir los cursos de entrenamiento que ofrecen para sus clientes.

d) Actividades relativas a asuntos colaborativos

Contactar y elaborar un presupuesto con empresas proveedoras de equipos de seguridad anti-incendio, alarmas anti-robo y de dispositivos electrónicos de control de ingreso en la ciudad de Quito, para instalar los siguientes equipos:

- Ventiladores, detectores de humo y
- extintores de fuego cerca de los equipos y las áreas de trabajo,

- una alarma contra incendios
- control de acceso por tarjetas magnéticas.

Contactar y elaborar un presupuesto para la posible contratación de seguros anti-incendio, robo o desastres naturales para los equipos.

e) Verificación

En caso se ser aprobada la adquisición de equipos de seguridad y la contratación de seguros, el presentar informes de cumplimiento ayudaría en gran manera a las actividades de control, para verificar el cumplimiento de los requerimientos por parte de las empresas proveedoras de equipos de seguridad. Es por ello que el Jefe del Área Técnica bajo la supervisión del Jefe de Departamento, elaborará informes de cumplimiento ante las autoridades del Departamento de Adquisición e Inventario de Bienes

V. Área de Mitigación: Gestión de Sistemas y Red de Información

a) Responsabilidad

Estas actividades otorgarán mayores responsabilidades al Jefe y a todo el personal de TI, bajo la supervisión del Jefe de Departamento, ya que son los primeros responsables del Área de Gestión de Sistemas y Red de Información. Estas actividades a su vez son parte de las estrategias de protección del Área de Gestión de la Seguridad de Información. La mejora en la administración de los recursos de sistemas y red, coadyuvará también con las estrategias de protección para el Área de Monitoreo y Auditoría de la Seguridad Física.

b) Procedimientos

El documentar y formalizar los procedimientos de administración de la red y de sus sistemas ayudarían a asegurar que éstos sean aplicados coherentemente por todos los miembros del personal de TI, y así aumentaría la eficiencia de la gestión en esta área.

Es por esta razón que el Administrador de Red documentará las tareas administrativas de la red y tendrá un control estricto de inventario de software y hardware de los dispositivos que conforman la red de datos, el mismo que será

actualizado permanentemente, inclusive con herramientas de monitoreo. Esta actividad ya fue sugerida como parte del Control de Seguridad Física.

c) Actividades:

El personal asignado de TI se encargará de:

- Almacenamiento seguro de información sensitiva, como por ejemplo, respaldos cada fin de semana o backups guardados fuera de las instalaciones.
- Mantener los sistemas operativos actualizados con respecto a revisiones, parches, y recomendaciones de asesores de seguridad para evitar violaciones a la seguridad de la red de datos.
- Instalar y configurar herramientas de monitoreo y administración de red, una vez recibido el entrenamiento sobre ellas y pagado las correspondientes licencias de software. Las herramientas deben analizar los servicios mal configurados, puertos y servicios que puedan encontrarse abiertos y que causan brechas en la seguridad. La gestión del pago de las licencias de los programas la realiza el Jefe de TI via presupuesto del Instituto Geofísico.
- Se debe adquirir e instalar un programa antivirus automático y actualizado.
- Gestionar de una manera un poco más estricta las claves de acceso, cuentas, y privilegios.

  Nótese que esta actividad tiene que ver con el Área de Autenticación y Autorización.
- Instalar y configurar un sistema inspector de contenido por hardware o por software.

Hay que anotar que esta actividad tiene que ver con el Área de Arquitectura y Diseño de la Seguridad.

d) Entrenamiento

Los miembros del personal de TI deben asistir al entrenamiento para gestionar la seguridad de sistemas y redes, y en la utilización de herramientas de gestión de sistemas y redes de información, en los cursos ofrecidos por la Facultad de Sistemas o el Centro de Estudios de la Comunidad de Escuela Politécnica Nacional. El Jefe del Área Técnica bajo la supervisión del Jefe de Departamento

debe patrocinar esta actividad, y así gestionar oportunamente el costo de los cursos de entrenamiento vía presupuesto.

Se debe anotar que las empresas que venden equipos y programas de seguridad de datos ofrecen también cursos de entrenamiento. En caso de adquirir esos equipos, el personal de TI debe asistir de manera obligatoria a los cursos de entrenamiento.

VI. Área de Mitigación: Autenticación y Autorización

a) Responsabilidad

Estas actividades otorgarán mayores responsabilidades al Jefe y a todo el personal de TI, en especial al Administrador de Red, ya que son los primeros responsables del Área de Autenticación y Autorización del ingreso a la red. Estas actividades complementan las estrategias de protección del Área de Gestión de la Seguridad de Información.

b) Procedimientos

Si bien es cierto, el Administrador de Red elabora las listas de cuentas autorizadas de acceso y las presenta al Jefe de Departamento cada semestre, sin embargo no existen procedimientos documentados formalmente sobre los procesos de autenticación y autorización de acceso de usuarios.

El Administrador de Red y el Jefe de TI se encargarán de elaborar el documento sobre las actividades sugeridas en esta Área de Autenticación y Autorización, y que servirá de apoyo para una mejor comprensión y facilidad de implementación de estos procedimientos para el personal de TI.

c) Actividades:

El Administrador de Red debe participar en la mejora del control de acceso a la red y también en la verificación de la identidad de los usuarios del link de correo interno en el WebSite. Existe el préstamo de cuentas y contraseñas de acceso como un abuso de lo que se entiende como “red compartida”, también las cuentas y contraseñas de personas que se ausentan con mucha frecuencia vuelven difícil la administración del acceso a la red. Se debe poner un mayor cuidado en la administración de la bitácora que registra el ingreso al sistema de las cuentas de usuario (log-in), para detectar cualquier actividad inusual o sospechosa. Las listas

de cuentas de acceso a veces no están actualizadas, y hay muchas cuentas caducadas o inútiles.

El Administrador de la Red se encargará de:

- Instalar una programa monitor que haga que las estaciones de trabajo dejadas activas inadvertidamente, automáticamente se desconecten del sistema luego de un periodo de tiempo prudencial (log-off automático).
- Implementar controles de acceso (p.ej, permisos para abrir archivos, impedimentos de cambio no autorizado de configuración de red) y exigir la autenticación de usuario (por ejemplo; claves de acceso, screening o exploración del perfil de usuarios) para restringir al usuario común el acceso a información, sistemas sensitivos, aplicaciones y servicios específicos, y conexiones de red.
- Chequear permanentemente los ingresos realizados a la red por los distintos usuarios, log-in, y monitorear las cuentas de acceso, log-monitoring. Investigar de esta forma cualquier tipo de actividad sospechosa. Actualizar mensualmente las listas de cuentas de acceso de usuario autorizadas, y dar de baja las cuentas caducadas o inútiles.
- Implementar el uso de contraseñas de ocho caracteres mínimo, obligar a combinar letras mayúsculas y minúsculas, números y símbolos, y que cada usuario maneje su propia clave de acceso de manera exclusiva.

d) Entrenamiento

No todo el personal de TI ha asistido a cursos de entrenamiento sobre las medidas para desarrollar procedimientos formalizados para restringir el acceso indebido de usuarios. Para asegurar que tales procedimientos sean consistentemente entendidos y aplicados por todos los miembros del personal de TI, todos ellos deben asistir a cursos de entrenamiento sobre implementación de medidas tecnológicas para restringir el acceso no autorizado a la red. Generalmente solo el Administrador de Red ha asistido personalmente a cursos de entrenamiento, y esto es por demás insuficiente. Todos los miembros del personal de TI deben asistir obligatoriamente a estos cursos de entrenamiento.

VII. Área de Mitigación: Arquitectura y Diseño de la Seguridad

a) Responsabilidad

Estas actividades otorgarán mayores responsabilidades al Jefe y a todo el personal de TI, en especial al Administrador de Red, ya que son los primeros responsables de Arquitectura y Diseño de Seguridad de Información. Estas actividades se hallan bajo la supervisión del Jefe del Área Técnica y del Jefe de Departamento. Todo cambio en la arquitectura de la red debe ser aprobado por el Comité Técnico.

b) Procedimientos:

Nunca se ha hecho de manera organizada e integral el diseño y arquitectura de la seguridad de la red de información. Es por ello que no hay diagramas que muestren la arquitectura de la seguridad de la red en la topología actual. Como una alternativa, **el Sistema Tecnológico de Seguridad** [72]propuesto y documentado en el presente Proyecto de Titulación, puede ser utilizado como base para el análisis y mejora de esta Área. El documentar formalmente las prácticas y procedimientos de Arquitectura y Diseño de Seguridad de la Información, facilita la presentación de propuestas ante las autoridades y agilitan su gestión.

c) Entrenamiento:

Casi ningún miembro del personal de TI tiene experiencia en diseño y arquitectura de redes seguras. Con excepción del Administrador de Red, cuyo entrenamiento en esta materia ha sido gestionado por cuenta propia. Por ello se sugiere que todos los miembros de TI deben asistir a cursos de entrenamiento en el diseño de sistemas y redes seguras que se dictan en las Facultades de Sistemas y Eléctrica en la Escuela Politécnica Nacional.

d) Asuntos colaborativos:

Todo el personal de TI, y en especial el Administrador de la Red, revisarán el material presentado en **el Sistema Tecnológico de Seguridad**, analizarán las propuestas de diseño y sugerirán mejoras o enmiendas a la arquitectura de seguridad. Se propondrán nuevos controles de seguridad en sistemas y redes. Con el diseño propuesto, indagar y contactar empresas de seguridad de datos que vendan equipos que puedan realizar las siguientes funciones:

[72] En el lit. 3.3 se desarrolla el Sistema Tecnológico de Seguridad

- Implementar un Firewall que soporte VPN para que los usuarios puedan realizar acceso remoto a través del Internet.
- Instalar un servidor Proxy para proteger las direcciones IP de la red de datos.
- Implementar un sistema inspector de contenido Web, para optimizar el uso del ancho de banda de Internet.
- Implementar un sistema de detección de intrusiones, NIDS, para impedir el acceso de usuarios no autorizados y maliciosos.
- Implementar el servicio NAT, Network Address Translation, o traducción de direcciones de red, en el mismo firewall.

e) Requerimientos y verificación:

Para la adquisición de equipos y el pago de licencias de software, con las empresas proveedoras de servicios de seguridad informática, diseño de redes e instalaciones de cableado estructurado, El Jefe del Área Técnica y el Jefe de TI gestionarán la aprobación del **Sistema Tecnológico** sugerido ante el Comité Técnico. La comunicación formal de los requerimientos a las empresas va incluida en el plan aprobado por el Comité Técnico.

El Jefe de Departamento, luego de la aprobación del Comité Técnico, gestionará el financiamiento de estos equipos y servicios, ante las autoridades de la Escuela Politécnica Nacional.

Los informes de verificación del cumplimiento de los requerimientos, la presentarán los Jefes del Área Técnica y de TI al Jefe de Departamento, para el adecuado control del desempeño de las empresas contratadas.

3.2.2.4.1 Lista de acciones inmediatas

Mientras se elaboraba el plan, se identificaron los siguientes dos puntos de acción durante el proceso S5, considerados de mayor urgencia, y se los anotó en *las Hojas de Trabajo de Lista de Acciones:*

- *Reenviar alertas sobre seguridad básica.* El personal de TI ha enviado emails para todo el personal del Instituto Geofísico, sobre alertas de seguridad básica. Este Ítem de Acción provee un mecanismo de avisos a corto plazo sin

mucha inversión, y con buenos resultados. Las alertas se refieren a hecho de recordar a los usuarios el correr un programa antivirus cuando se vaya a ingresar a las estaciones de trabajo un diskette o CD con información proveniente de fuera de la red.

- *Cambio de la configuración física en la oficina del servidor Linux y donde están instalados los equipos del SISV.* Uno de los problemas de seguridad física identificados durante la evaluación era la deficiente configuración física de todo el 6to Piso del edificio de la Facultad de Ingeniería Civil en la Escuela Politécnica Nacional. La mayoría de estaciones de trabajo están en áreas sin candado, y sin implementación de cableado estructurado, además el Switch y el Servidor no tienen suficiente protección física. Hay muchos cables que no están en orden y no hay racks o armarios de acero en donde se coloquen estos equipos delicados. Se recomienda la urgente instalación de cableado estructurado, y reorganizar la oficina del servidor.[73]

3.2.2.5 Actividad S5.5: Identificar los Pasos Siguientes

Paso 30

Utilizando *la Hoja de Trabajo de los Pasos Siguientes,* se identificaron varios puntos requeridos para apoyar la implementación de los resultados de OCTAVE-S, **en caso de ser aprobado por el Comité Técnico y el Jefe de Departamento**. Primero, los Jefes de Área deben hacer de la seguridad de la información una prioridad y no un asunto secundario. Segundo, gestionar el financiamiento para implementar el Plan de Mitigación, luego de que éste sea aprobado. También se anotaron los siguientes puntos a ser completados dentro de los tres meses siguientes:

[73] Desde Agosto del 2005 se remodela la infraestructura física de las instalaciones del Instituto Geofísico. En las obras civiles, se toma en cuenta la nueva distribución de las computadoras, lo cual es un paso adelante en la seguridad. Cfr. El Ing. Paul Gachet ha elaborado el plano de la nueva infraestructura física, y está disponible en la oficina del Jefe de Tecnología de Información.

- Las personas a quienes se le hubiere asignado responsabilidad para implementar el plan de mitigación proveerán documentación **detallada** para ser revisada.
- Todos los riesgos diferidos serán revisados dentro de tres meses.
- Se hará una comparación entre las práctica de seguridad analizadas en esta evaluación OCTAVE-S con las sugerencias analizadas en el "Marco legal de la información geoespacial del Instituto Geofísico "[74], y de esta forma determinar si hay cualquier actividad adicional que necesite ser añadida o mejorada para cumplir con las regulaciones técnicas y legales vigentes, en especial aquellas sugeridas en el ODEPLAN[75].

También se recomienda conducir otra evaluación OCTAVE-S en cerca de 12-18 meses, dando suficiente tiempo para la implementación de las acciones de mitigación en el plan que se acaba de desarrollar.

[74] Cfr. Literal 1.1.5 y en el Paso 5, para la Gestión de Incidentes en la Práctica de Seguridad 15.
[75] El ODEPLAN se encarga de regular los asuntos técnicos y administrativos de la gestión de la información geoespacial en el Ecuador. Cfr. Literal 1.1.6 sobre La información del Instituto Geofísico dentro de la Infraestructura de Datos Geoespaciales.

3.3 SISTEMA TECNOLÓGICO DE SEGURIDAD

En el **Plan de Mitigación propuesto, en los Pasos 28 y 29**, se analizaron las estrategias de protección más adecuadas para el Área de Diseño y Arquitectura de la Seguridad, en donde se propusieron **actividades para la adquisición de equipos de seguridad informática**. Es por ello que en este acápite se desarrolla un **Sistema Tecnológico de Seguridad** como **parte de las actividades del Plan de Mitigación**, y puede también considerarse como parte de los Pasos 28 y 29.

Con esa finalidad primero se realiza un estudio de los criterios de diseño desarrollados según las necesidades o requerimientos técnicos de seguridad de la red de datos del Instituto Geofísico. Luego se seleccionan productos ofertados en el mercado cuyas especificaciones se adecuen a los requerimientos de estos criterios de diseño. La posterior evaluación de estos productos comerciales seleccionados se realiza mediante un análisis comparativo entre ventajas y desventajas de las características tecnológicas de cada uno. Finalmente se desarrolla un presupuesto referencial y se comparan los costos, para sugerir la adquisición de aquel o aquellos que sean más convenientes desde el punto de vista técnico y económico.

3.3.1 CRITERIOS DE DISEÑO

En la red de Información del Instituto Geofísico, se espera un crecimiento significativo aproximado del 50% en el número de estaciones en los próximos dos años, por lo que su manejo como visualización aumentará en complejidad y volumen[76].

Hay 36 PCs, 7 computadoras laptop y 1 servidor[77] en la Red de Información del IGEPN. Lo que significa que en la red de datos se tienen 44 computadores o estaciones de trabajo, más 22 que es el 50%, totalizarían aproximadamente 66 estaciones de trabajo para los próximos dos años, en los años subsiguientes se tendrán casi 100 estaciones.

Este número nos ubica en la categoría de seguridad entre una organización de tipo pequeño a mediano, según la Cisco VPN Security Reference

[76] FLORES y FONSECA, op.cit, p.35.
[77] Ibid., p.31.

Guide[78]. En esta Guía de Referencia, se recomienda utilizar el firewall Cisco Pix 515-U o equivalente para este tipo de red como herramienta fundamental para definir la seguridad en los siguientes aspectos:

Como el IGEPN debe definir la red interna como una Intranet[79], los puertos necesarios para las conexiones son:

a) Un puerto para consola de administración del Firewall.

b) Un puerto para configurar la zona desmilitarizada, **DMZ,** en donde se conectará mediante el Switch 3COM Baseline ya existente, el Servidor de Correo separado del Servidor Proxy.

Actualmente residen en el mismo servidor, el Firewall con IPtables, el Servidor de Correo Interno y la configuración Linux Proxy, lo cual no es una garantía de seguridad, pues basta que se contamine el correo interno y ésta se extiende a toda la red. Es también recomendable tener en una PC aparte, instalado un Inspector de Contenido dentro de la misma DMZ.

c) Otro puerto para conectar a la salida del Firewall mediante un segundo Switch Capa 2 para conectar los servidores propuestos por el Plan Informático: un servidor para DataWarehouse, otro para base de datos, y un tercero de aplicaciones.

Por las necesidades a), b) y c) anteriores, se necesitan por lo menos **tres interfaces** Fast Ethernet 10/100 Base TX.

Actualmente la red funciona con Ethernet 10 Base T lo que significa un máximo de velocidad de transmisión de 10 Mbps. Se prevé en el futuro el aumento de la velocidad a 100 Mbps para poder servir a todas las 100 estaciones, utilizando cable UTP categoría 5 para la interconexión entre ellas.

El Firewall debe tener la posibilidad de definición de VPNs. Inclusive para la nueva definición de arquitectura de red propuesta[80], se sugiere la segmentación del tráfico en VLANs.

El Firewall también debe disponer de servicio NAT, Network Address Translation, o traducción de direcciones de red, para proteger las direcciones IP.

---

[78] www.cisco.com/go/evpn documento SEC_VPN_Guide.pdf, pp.50-51.

[79] FLORES y FONSECA, op.cit. p. 80.

[80] FLORES y FONSECA, op.cit. p. 83.

Además se debe implementar un sistema de seguridad de contenido, para examinar los archivos que se descargan por correo, o applets de Java, Active X. Debe implementarse una facilidad de escaneo de Internet. Esta implementación puede ser complementaria al firewall o instalarse por software en una estación que se dedique solamente al filtrado del contenido. Debe haber servicio de AntiSpamming de correo, y contar con un antivirus que se actualice, de ser posible, en línea y de manera automática.

En cuanto a los eventos de administración, en caso de instalarse una estación como consola para ese efecto, deben realizarse de preferencia encriptadas, y todos los accesos deben ser autenticados. Se debe tener una bitácora de cuentas de acceso fallidas. Se debe también replicar la gestión en una estación remota que guarde pistas de auditoría que resulten transparentes al atacante.

Debe implementarse un Sistema de Detección de Intrusiones (IDS), para terminar las conexiones intrusas e inclusive, identificarlas y neutralizarlas a futuro para que no hagan más daño.

Se sugiere adquirir un UPS para cada estación, para salvaguardar la información en caso de fallas de energía eléctrica, o mientras se conecta la toma auxiliar. Además para la puerta de ingreso, se puede instalar un portero electrónico con tarjetas magnéticas con reconocimiento de códigos de claves de acceso.

La conexión a AccessRAM MEGADATOS puede sufrir alguna vez alguna interrupción prolongada por lo que se sugiere conectar en el acceso a Internet con una toma auxiliar a la POLINET, que tiene su propio proveedor de ISP.

3.3.1.1 Planeación a futuro

Según se puede ver en la Figura 6, el Esquema del Diseño del Sistema Tecnológico de Seguridad para la Red de Datos del Instituto Geofísico, muestra los dispositivos que se conectan separados: Antes del firewall[81] se conecta un Detector de Intrusiones, NIDS y se configura la Zona Desmilitarizada, DMZ, y, para aprovechar esta protección a la salida del firewall, se puede

[81] Cfr. VINUEZA RHOR, Mónica de Lourdes, "Estudio y diseño de un Sistema de Seguridad para la red de datos del Colegio los Pinos", Directores: Ing. Pablo Hidalgo y Ing. Nelson Avila, Proyecto de Ingeniería, Código: 010646, Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito, 2003. En el Capítulo I, se describen las ventajas y desventajas de un firewall. El firewall es el dispositivo fundamental para la seguridad de los datos, pues en él se configura la Zona Desmilitarizada, DMZ.

conectar el Switch 3COM Baseline Capa 2[82] ya existente en la red actual, para proteger los Servidores de Correo, Proxy y de Administración de Contenido, que son los más vulnerables de sufrir ataques. Al Switch Capa 3 de 24 puertos que proponen Flores y Fonseca [83], se lo puede conectar a la salida del firewall y así también proteger los Servidores de Base de Datos, DataWarehouse y de Aplicaciones. Para detectar y bloquear la posible contaminación desde las estaciones de la red interna, se conecta otro Detector de Intrusiones, NIDS a la entrada de este Switch Capa 3.

Es importante la velocidad de conmutación de paquetes en el Switch, para el Switch Capa 2 es de 9 Mpps[84], el de Capa 3 puede conmutar más de 4 veces más rápido a 40 Mpps, lo cual optimiza la eficiencia de la red interna.

Actualmente el Switch Capa 2 existente satisface la carga total de la red. De aumentar las estaciones, se requiere instalar el otro Switch Capa 3. El Firewall debe aproximarse por lo menos a 100 Mbps, para poder servir simultáneamente a todos los puertos de los dos Switches propuestos.

Para la adecuada implementación, y de acuerdo con las necesidades más urgentes, se sugiere instalar en una primera etapa el Firewall, luego el detector de intrusiones, NIDS, y finalmente el Inspector de Contenido. Conforme la red siga en crecimiento y la nueva infraestructura física permita la instalación del cableado estructurado, se instalarán los equipos que se escojan como más adecuados y de mejor desempeño.

---

[82] FLORES y FONSECA, op.cit., Anexo C. En este proyecto, se detallan las características de los Switches 3COM capas 2 y 3.

[83] FLORES y FONSECA, op.cit., Anexo D.

[84] Mpps = Millones de paquetes por segundo.

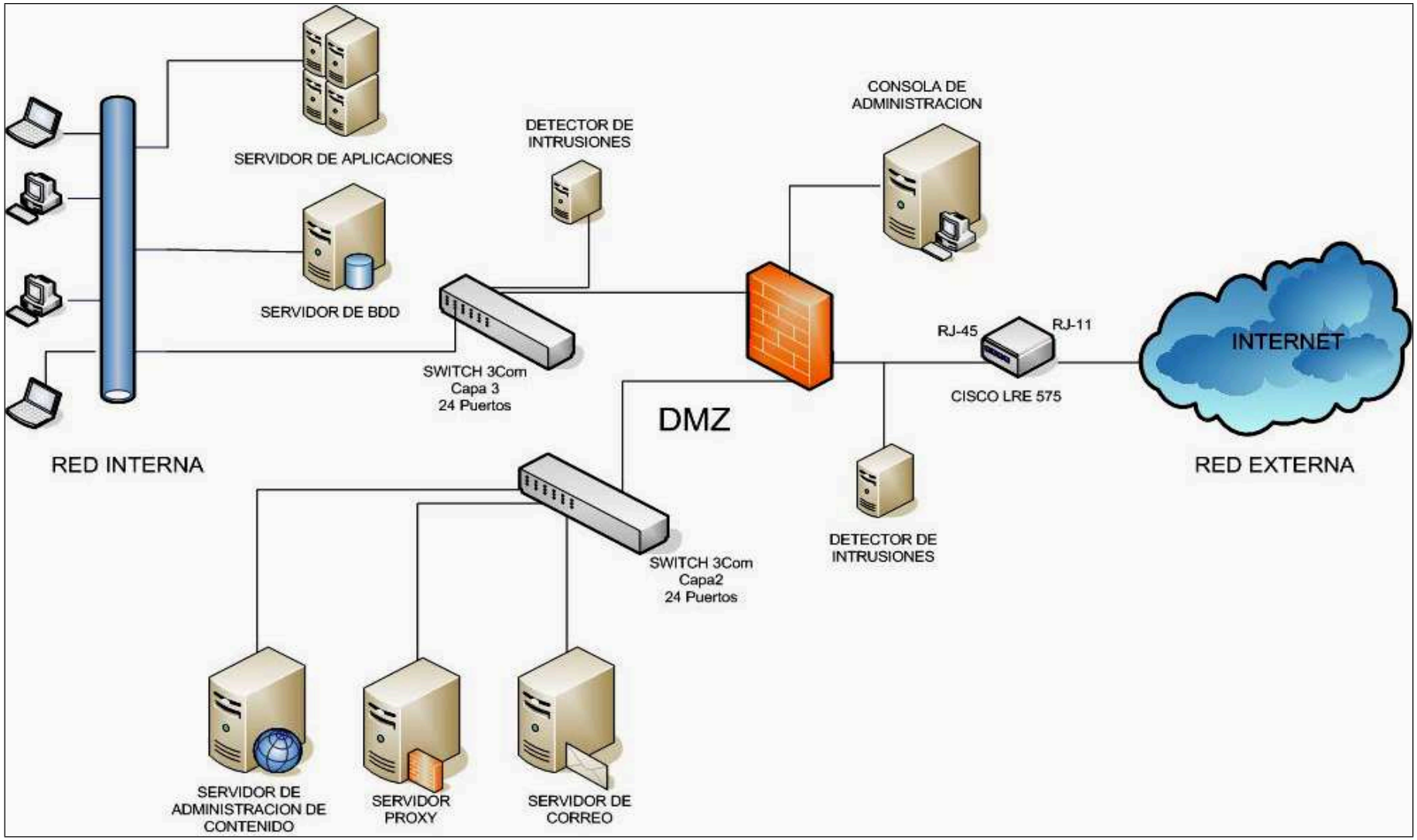


Figura 6.- Esquema del Diseño del Sistema Tecnológico de Seguridad para la Red de Datos del Instituto Geofísico de la Escuela Politécnica Nacional

3.3.2 ESPECIFICACIONES TÉCNICAS REQUERIDAS

a.- Firewall

- Por lo menos tres interfaces hasta 100 Mbps con capacidad de expansión hasta 6.
- Uso efectivo del ancho de banda o throughput de por lo menos 100 Mbps.
- Uso efectivo del ancho de banda o throughput de por lo menos 60 Mbps para VPN.
- Por lo menos encriptación DES, 3DES en VPN.
- Soporta VPN de sitio a sitio con IPsec, SSL, PPTP.
- Consola de administración amigable al usuario y con formato de ventana Web.
- Que soporte un servidor DHCP por lo menos para 100 direcciones.
- Inspección stateful de paquetes.
- Filtrado automático de contenido en la capa de aplicación.
- NAT, Network Address Translation, para proteger las direcciones IP.
- Mecanismos flexibles de autenticación.
- Proveer la capacidad de implementar VLANs.

b.- Sistema de Detección de Intrusiones en la Red, NIDS, o Network Intrusión Detection System

- Al menos una Interfaz de monitoreo estándar y una para control y comandos.
- Implementar por lo menos 4 interfaces para olfatear, o sniffing dentro de varios puntos de ingreso a la red.
- Desempeño de detección de Intrusiones de por lo menos 60 Mbps.
- Velocidad total de inspección de por lo menos 80 Mbps.
- Por lo menos 200 nuevas conexiones TCP por segundo
- Por lo menos 200 transacciones HTTP por segundo.
- Mantener una Base de Datos de la Red y poder comunicarse con los centros de información para eventos de ataque.
- Acciones activas de respuesta como terminación automática de sesión.
- Monitoreo y administración centralizada del detector de Intrusiones.

c.- Inspector y Filtro de Contenido Web

- Filtrado y actualización de grupos de URL.
- Bloquear el espionaje electrónico, o spyware, sitios ofensivos y código malicioso móvil.
- Prevenir el compartir archivos P2P, peer-to-peer.
- Gestionar los mensajes instantáneos y los archivos o ventanas adjuntas a los mensajes de Internet.
- Gestionar el uso de medios que ocupen mucho ancho de banda como video-en-línea, o música-en-línea.
- Programas actualizados antiSpamming, antiVirus, antitroyanos, antigusanos.

3.3.3 ANÁLISIS COMPARATIVO DE LAS ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS

En el Cuadro 9, se puede observar que se proponen tres alternativas para hacer el análisis, en dónde se puede anotar que hay en realidad dos posibilidades de implementación:

1. Adquirir los dispositivos de manera separada, para luego integrarlas; y

2. Adoptar las soluciones con dispositivos que ya vienen integrados.

Propuesta	Descripción	Tipo
ALTERNATIVA 1	Integración del CISCO PIX 515 E Unrestricted(UR) con el IDS 4215 y Websense Enterprise	Soluciones independientes que pueden ser integradas.
ALTERNATIVA 2	APPLIANCE[85] ISS Proventia M30	Dispositivo integrado de seguridad
ALTERNATIVA 3	CISCO ASA 5520	Dispositivo integrado de seguridad.

Cuadro 9.- Alternativas de los equipos comerciales[86]

A continuación se utilizan los cuadros del Anexo F: Especificaciones Técnicas de los Equipos y Productos Comerciales[87] para hacer un análisis comparativo entre las tres alternativas, y sugerir desde el punto de vista técnico, cuál de ellas se adecua más a las necesidades de la seguridad de la red del Instituto Geofísico.

a.- Firewall

- Por lo menos tres interfaces hasta 100 Mbps con capacidad de expansión hasta 6. El dispositivo Cisco Pix 515 E y el ISS Proventía M30 cumplen con el número de interfaces mínimo, pero el ASA 5520 los supera en velocidad a 4 interfaces Gigabit Ethernet más 1 FastEthernet.
- Uso efectivo del ancho de banda o throughput de por lo menos 100 Mbps. Esta es talvez la característica **más importante** para el desempeño de la red. Tanto el dispositivo Cisco Pix 515 E como el ISS Proventía M30 superan la velocidad mínima con un throughput

[85] Appliance es un dispositivo de aplicación específica. Esto se explica en el DOCUMENTO TÉCNICO PDF de Internet Security Systems, Diciembre de 2005, en http://www.virtual.com/product_sheets/ISS_Proventia_Integrated_Security_Appliance_ds.pdf

[86] Fuente: El autor del presente proyecto.

[87] El Anexo F ha sido traducido y elaborado por el autor del presente proyecto de titulación de las fuentes bibliográficas de los documentos técnicos de ISS, CISCO y Websense Enterprise.

de cerca de 200 Mbps. El ASA 5520 también los supera en esta característica con un máximo de 450 Mbps.

- Uso efectivo del ancho de banda o throughput de por lo menos 60 Mbps para VPN. Esta característica es muy parecida en el Cisco Pix 515 y en el ISS Proventía M30, con un troughput de VPN entre 60 y 140 Mbps aproximadamente, dependiendo esta velocidad del tipo de encriptación y de la aceleración por hardware. El Cisco ASA 5520 puede trabajar con VPNs hasta 225 Mbps, sin aceleración de hardware.
- Como característica de VPN, se pide por lo menos encriptación DES, 3DES en VPN. El Cisco Pix 515 E y el Cisco ASA 5520 soportan encriptación de 56, 168 bits para asegurar la privacidad de los datos. El ISS Proventía M30 posee encriptación DES, 3DES y AES sin mucha variedad en el tamaño de bits. El Cisco ASA 5520 posee encriptación RC4 adicional.
- VPN de sitio a sitio con IPsec, SSL, PPTP. La autenticación de ruteo MD5 , RIP v.2, SHA-1 para el Cisco Pix 515 E y el ISS Proventía M30 respectivamente, le dan una característica adicional de protección de VPN del Cisco ASA 5520.
- Los tres dispositivos poseen consola de administración amigable al usuario y con formato de ventana Web. Así el Cisco Pix Device Manager Para el Cisco Pix 515 E, el ISS Site Protector para el ISS Proventía M30 y el Cisco Adaptive Security Device Manager para el Cisco ASA 5520.
- Tanto el Cisco Pix 515 E como el ISS Proventía M30 soportan sobre 250 direcciones IP de interfaz VPN dinámicamente para el servidor DHCP. El Cisco ASA 5520 los supera ampliamente al permitir hasta 700 IPSec con la licencia VPN plus.
- Los tres dispositivos soportan sobre 100.000 sesiones concurrentes de conexión simultánea para inspección stateful de paquetes.
- Filtrado automático de contenido en la capa de aplicación no está incluido en el ISS Proventía M30, pero puede integrarse con software compatible adicional. Para el Cisco ASA 5520 esta

característica es opcional, con software para el efecto. Solo el Cisco Pix 515 tiene incorporada esta característica.

- La facilidad de NAT/ PAT , Network / Protocol Address Translation para proteger las direcciones IP y los protocolos adjuntos. el Cisco ASA 5520 la tiene para más servicios como el FTP y el SIP. El ISS Proventía M30 soporta NAT reverso. El Cisco Pix 515 E tiene capacidades estáticas y dinámicas.
- Mecanismos flexibles de autenticación. Los dispositivos Cisco Pix 515 E y ASA 5520 integran los servicios AAA, TACACS+ y RADIUS. El ISS Proventía M30 hace la autenticación de VPN por base de datos interna o por RADIUS.
- Los dispositivos Cisco Pix 515 E y ASA 5520 soportan hasta 8 y 25 interfaces lógicas 802.1 para VLANs respectivamente. El ISS Proventía M30 no posee esta capacidad, pero puede definirse con el software de ISS Real Secure.

b.- Sistema de Detección de Intrusiones de red, NIDS

- El Cisco IDS 4215 posee una interfaz 10/100 Base-Tx para monitoreo y otra igual para control y comandos. Esta facilidad para monitoreo estándar y control no la poseen integrada ni el ISS Proventía M30, ni el Cisco ASA 5520, pero pueden ser configuradas por software con el ISS Site Protector y con el Cisco ASDM respectivamente.
- En el Cisco IDS 4215 se pueden Implementar por lo menos 4 interfaces para olfatear o sniffing de intrusiones dentro de varios puntos de ingreso a la red. El Cisco ASA 5520 y el ISS Proventía M30 integran IDS, Intrusion Detection System e IPS, Intrusion Prevention System para sus puertos.
- El Cisco IDS 4215 detecta las intrusiones a una velocidad tan solo un poco superior a la mínima requerida de 60 Mbps, lo cual lo vuelve muy lento para esta función. En cambio los dispositivos ISS Proventía M30 alcanzan a 200Mbps con Firewall, IPS y filtrado Web

inclusive. Mucho más el Cisco ASA alcanza 225 Mbps inclusive con el firewall y los servicios en línea de Anti-X.

- La velocidad total de inspección del Cisco IDS 4215 es de máximo 80 Mbps, el ISS Proventía alcanza 84 Mbps, si se integran simultáneamente el antivirus al IPS, y filtro Web. El Cisco ASA 5520 **supera ampliamente en velocidad a los dos dispositivos anteriores por la capacidad aceleradora por hardware del dispositivo integrado AIP-SSM 10. Esta característica es una ventaja para impedir la sobresaturación de la red.** El dispositivo AIP-SSM 10 es una máquina inteligente reactiva y se adapta más hacia el trabajo simultáneo sin interrumpir el desempeño de la red. Evita los molestosos escaneos u olfateos que distraen las operaciones, y no pone en riesgo la disponibilidad de la red o de su ancho de banda. U*n sistema de seguridad muy intrusivo podría sobresaturar el uso efectivo del ancho de banda de la red, con la consiguiente baja en la disponibilidad.*
- Las conexiones TCP y las transacciones HTTP por segundo son para el Cisco IDS 4215, 800 por segundo, para el ISS Proventía son de 4,100 conexiones nuevas por segundo, y el Cisco ASA 5520 supera a los dos dispositivos anteriores por la capacidad de resolver hasta 9000 conexiones nuevas por segundo.
- El Cisco IDS 4215 puede comunicarse con la base de datos de seguridad de la red y obtener asesoría en línea para confrontar los diferentes ataques. Igualmente el ISS Proventía puede contactarse con la X-Force Security Intelligence y se pueden actualizar los sensores en forma remota. El Cisco ASA 5520 le permite al administrador contactarse con soporte en línea y recibir asesoramiento sobre la calificación del riesgo de los ataques, para que tome acciones de mitigación específicas. También Cisco da soporte para la prevención en línea de los ataques, en http:// www.cisco.com. Se da a los administradores la información para control granular, y se proveen herramientas adecuadas para afrontar ataques de firmas específicas.

- El Cisco IDS 4215 realiza el registro de paquetes sospechosos. Y frente a esta amenaza de conexiones intrusas, realiza acciones activas de respuesta como la terminación automática de sesión. En el ISS Proventía M30 se bloquean más de 600 de las amenazas más conocidas. Se bloquean worms, troyanos, intrusiones y paquetes ofensivos. Tiene también las facilidades Block y Reset Connection.
- El Cisco ASA 5520, a través de las facilidades del Cisco Meta Event Generator (Generador de Meta Eventos), se identifican y detienen las nuevas amenazas y opcionalmente se reduce el número de eventos de ataque con los sistemas de monitoreo centralizado.
- En el Cisco IDS 4215, el Secure IDS Director, se monitorea de manera centralizada la actividad de varios sensores ubicados en segmentos de red locales o remotas. Tanto en el ISS Proventía M30 como en el Cisco ASA 5520, el monitoreo y administración centralizados se los realiza por medio de software compatible, con las facilidades del ISS Real Secure Site Protector y del Cisco ASDM respectivamente.

c.- Inspector y Filtro de Contenido Web

- El software del Websense Enterprise Master Database ofrece el servicio de base de datos de URLs de más de 6 millones de sitos Web clasificados en 80 categorías. Esta base de datos de URLs, contiene los sitios accesados más frecuentemente, de esta manera se provee filtrado de Internet de grupos indeseables. En el ISS Proventía M30, la base de datos de X-Force® Security Intelligence puede ser consultada por el software del ISS Site Protector®, para priorizar las vulnerabilidades encontradas en Internet. Los agentes de protección por software de ISS Real Secure® pueden ser configurados para activar el proceso Virtual Patch ® que protege contra las vulnerabilidades catastróficas listadas en el manual de la X-Force CRI, que contiene 20 millones de URL en 58 categorías. Y se realizan más de 100.000 actualizaciones diarias de URLs. Se

proveen también técnicas avanzadas de clasificación de URLs: tipo texto, imagen, objetos, OCR, listas negra y blanca, capacidad de autoaprendizaje, envío automático de URLs a ISS para su clasificación. El Cisco ASA 5520 permite la utilización y control óptimos de la gestión de Web mediante la integración con las soluciones Websense- y SecureComputing/N2H2- basadas en filtrado de URLs. Además el Cisco ASA 5520 soporta filtrado HTTPS y solicitud FTP Web mediante la integración ampliada con el software de Websense Enterprise.

- Con el software de Websense Entreprise Websense Enterprise Security PG® bloquea el acceso a sitios de espionaje electrónico y código malicioso móvil. Detiene la transmisión de información sensitiva a los servidores espías. En el ISS Proventía M30Puede instalarse el ISS Real Secure Desktop, que tiene la facilidad Antispyware Control que detecta e impide la ejecución de programas spyware.
- En el Cisco ASA 5520, se provee la prevención avanzada de intrusiones con los servicios Anti-X, para ataques conocidos y desconocidos de capas de red y aplicación, ataques de negación de servicio o DoS, malware, worms,virus, troyanos, spyware, y adware
- Para gestionar los mensajes instantáneos y los archivos o ventanas adjuntas a los mensajes de Internet se puede anotar que dentro de las facilidades del software de Websense Entreprise, está el programa administrador, Websense Enterprise IM Attachment Manager® (IMA), el cual bloquea la posibilidad de contaminación de virus o gusanos en la transferencia de archivos de mensaje P2P. En el ISS Proventía M30, la consola por software del ISS Site Protector, se pueden bloquear bajo AUDITS, la categoría IM Instant Messaging, se pueden también gestionar los archivos P2P de compartición de archivos y ventanas adjuntas de Internet. En el el Cisco ASA 5520, se proveen servicios de inspección avanzados para detectar y opcionalmente bloquear aplicaciones de IM

mensajeo instantáneo, compartición de archivos P2P, peer-to-peer, y otras aplicaciones en túnel a través de puertos de aplicación Web.

- Para gestionar el uso de medios que ocupen mucho ancho de banda como video-en-línea, o música-en-línea, para Websense Entreprise, el software optimizador de ancho de banda, Websense Enterprise Bandwidth Optimizer®, BWO prioriza el enlace con sitios relacionados con los fines de la institución. Se bloquea así la actividad o el uso de la aplicación cuando está fuera del uso del ancho de banda del límite permitido por los administradores de red. El Websense Enterprise Bandwidth PG® filtra los sitios de descarga de archivos de video, radio y TV en línea. En el ISS Proventía M30, con la interfaz provista por ISS Site Protector, se pueden gestionar recursos y bloquear sitios que sirvan de descarga de video, radio y TV en línea. Se pueden bloquear las URLs no deseadas con las técnicas de clasificación de URLs provistas por el Proventía M3B0. Para el Cisco ASA 5520, y dentro de la calidad de servicio QoS, con soporte para LLQ y sus políticas para priorizar el tráfico de red, se limita la utilización del ancho de banda de las aplicaciones, solamente a aquellas especificadas por el administrador. El ASA 5520 soporta el estándar de compresión Lempel-Ziv, LZS para optimizar el desempeño sobre conexiones de bajo ancho de banda.
- El servicio AntiSpamming no está provisto con el Websense Enterprise, pero puede ser instalado los programas más conocidos en cada estación, p McAffe, Symantec, o el ISS Desktop. En el ISS Proventía M30, la tasa de detección de antiSpam está sobre el 95%, con una base de datos de más de 200,000 direcciones. Para el Cisco ASA 5520. el servicio de máquinas de inspección inteligentes AntiSpamming realizan la tarea de impedir esta amenaza.
- Los programas contra algunos tipos de código malicioso de las empresas McAffe, Symantec, o el ISS Desktop se pueden instalar en cada estación, junto con el Websense Entreprise. En el ISS Proventía M30, con el ISS Desktop, se protege de código malicioso a los protocolos HTTP, FTP, SMTP, POP3, se realiza inspección de

archivos adjuntos y comprimidos. ZIP, MIME/UU, TAR, LHA/LZH, TAR, GZIP, ARJ,CAB, Pklite, LZEXE. Se realiza además inspección de entrada/salida, y de archivos anexados, y también se pone en cuarentena archivos contaminados. Si se instala el AntiSpyware Control se bloquea también el espionaje electrónico. En el Cisco ASA 5520, mediante el servicio de máquinas de inspección inteligentes antivirus, y defensa Anti-X, se previenen los ataques de fuerza bruta o denegación de servicio, que incluyen el spyware, malware, adware.

3.3.4 EVALUACIÓN DE LOS PRODUCTOS COMERCIALES

Las especificaciones técnicas de los equipos cumplen en gran medida los requerimientos de los criterios de diseño de seguridad. Además, para escoger una u otra solución se deben tomar en cuenta las tendencias actuales de la seguridad de datos, las ventajas y desventajas de la una u otra alternativa[88]. De esta forma se tiene una visión más amplia para evaluar de mejor manera las ofertas actuales de equipos de seguridad de datos.

3.3.4.1 Análisis de ventajas y desventajas[89]

- Las tres soluciones, el Cisco Pix 515 E, el ISS Proventía M30, y el Cisco ASA 5520 tienen sistema operativo propietario, es decir que su código fuente es transparente al atacante, lo cual es una ventaja para proteger al sistema. Los sistemas operativos-propietario son fáciles de instalar y mantener, si se siguen los lineamientos dados en los manuales que se dan en los cursos de capacitación a los administradores con poca experiencia.

[88] Las ventajas y desventajas se hallan sintetizadas en el Anexo G, el cual ha sido traducido y elaborado por el autor del presente proyecto de titulación de las fuentes bibliográficas de los documentos técnicos de ISS, CISCO y Websense Enterprise.
[89] Anexo G.

- Además, la plataforma no es dependiente de otros sistemas operativos, lo cual les da mayor amplitud para adaptarse, de esta forma pueden trabajar para Linux, para Windows sin ningún problema.
- Como contraste de lo anterior, cuando el software depende del hardware y viceversa, el instalar nuevos servicios y facilidades encarece el costo del hardware, pues se necesita adquirir máquinas adicionales. Para el Cisco Pix 515 E y el ASA 5520 se necesita una máquina adicional para instalar el software de Websense Enterprise. También en el ISS Proventía M30 para instalar los módulos de ISS Real Secure Web Filter, Web Mail , Proventía Desktop, Internet Scanner, Server Sensor necesitan una estación adicional configurada con Microsoft Windows 2000 Server y Base de Datos MS Server.
- El Cisco Pix 515 E tiene alianzas con otros fabricantes, lo que le da versatilidad para implementar servicios adicionales, para reportes e inspección de contenido. Se puede adaptar sin problemas con los dispositivos Cisco IDS e IPS.
- El ISS Proventía M30, es compatible con la amplia gama del software ISS Real Secure, algunas de cuyas facilidades se adaptan al Windows 2000 Server y a la Base de Datos MS Server. Hay que notar que los módulos de ISS Real Secure Web Filter, Web Mail y Desktop pueden ser instalados sin necesidad de adquirir el dispositivo Proventía. El Cisco ASA 5520 tiene alianzas con Websense Enterprise para implementar mejoras en la inspección y filtrado de contenido.
- Las tres soluciones, el Cisco Pix 515 E, el ISS Proventía M30, y el Cisco ASA 5520 tienen integrada la capacidad de trabajar con VPNs.
- Además como gran ventaja, los tres equipos tienen sistema contra fallos incorporado. El Cisco Pix 515 E tiene incrustado el filtro de aplicaciones Java a través de http incrustado en el firewall y para el Cisco ASA 5520 esta característica es opcional. En el ISS Proventía M30 se puede instalar este filtro de aplicaciones Java con software adicional.
- Sólo el Cisco ASA 5520 tiene antivirus y antiSpam incluido en el equipo. El ISS Proventía M30 solo tiene el antiSpam incluido. El Cisco

Pix 515 E no tiene instalados programas antivirus y antiSpam, lo cual encarece el costo por el la licencia de software adicional que hay que pagar.

3.3.4.1.1 Las tendencias actuales de los dispositivos de seguridad de datos

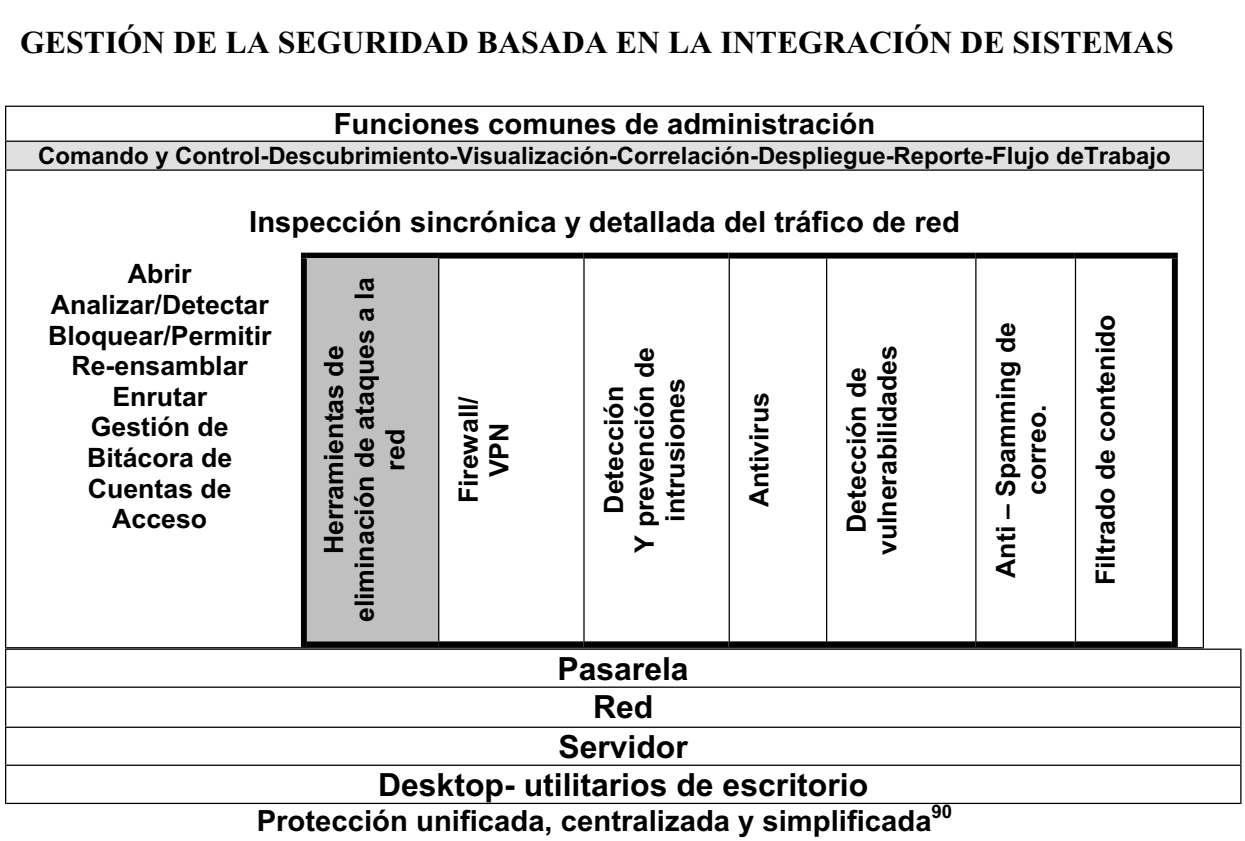


Figura 7.- La gestión de la seguridad basada en integración de sistemas

La tendencia actual de la tecnología de equipos de seguridad informática es la de integración de sistemas: Como se puede ver en la Figura 7, al manejar múltiples sistemas independientes como el Detector de Intrusiones, Firewall, Antispam, Antivirus y a la vez el Filtrado de Contenido Web, se vuelve problemático para la configuración, administración y mantenimiento simultáneo. Las ofertas actuales de los productos, en este caso el Cisco ASA 5520 e ISS Proventía M30, tienden a integrar en un solo dispositivo varias aplicaciones de seguridad. Es mucho más eficiente el administrar un solo dispositivo que integre las aplicaciones, que manejar sistemas múltiples, separados e independientes, con lo cual existe un

[90] ANÓNIMO, Documento de ISS, Proventía™, "La Bala de Plata en la Seguridad de la Información? Documento técnico en formato PDF, Internet Security Systems, Diciembre de 2005, en http://documents.iss.net/whitepapers/ProventiaVision.pdf, página 5.

ahorro en costos y personal requerido para la correcta gestión de la seguridad de la red. De esta forma no se maneja un montón o paquete de dispositivos desorganizados, sino un solo dispositivo integrado y de fácil configuración.

3.3.4.1.2 El enfoque proactivo-preventivo

El futuro de la gestión de la seguridad está en la prevención[91]:

También los productos Cisco ASA 5520 y el ISS Proventía M30 integran la prevención de amenazas con la reacción frente a ataques. Esto es una ventaja puesto que el prevenir las amenazas es mejor que reaccionar tardíamente contra ellas: La protección contra las vulnerabilidades debe ser proactiva, es decir, prevenir el ataque contra una vulnerabilidad ya detectada antes de que se éste se produzca. Hay que detener la amenaza desde la misma raíz del problema, se debe poner el parche o la vacuna antes de que se produzca el ataque, puesto que de darse el ataque y una vez que el daño esté hecho, los perjuicios para la red y sus datos son mucho mayores que si éste se hubiera prevenido. Con la protección reactiva, se espera que el ataque se dé a conocer, y se produzcan daños a veces irreparables sobre la información, y solo entonces se pone el remedio o se busca la mitigación para la amenaza. **La metodología solo reactiva para las condiciones actuales de desarrollo de la tecnología informática, puede considerarse incompleta y obsoleta.**

Los antivirus actuales funcionan con una base de datos de código malicioso en constante crecimiento, la cual debe ser actualizada de ser posible, todos los días. Actualmente las amenazas son híbridas multi-capa, y la sofisticación de los hackers alcanza al conocimiento de todas las capas de la red, por lo cual resultan insuficientes las simples combinaciones de firewall con antivirus.

El parcheo de emergencia de sistemas operativos y aplicaciones se requiere para cientos de aplicaciones y el personal de Tecnología de Información no alcanza a mantenerse al tanto de las múltiples vulnerabilidades que se presentan, por lo cual se hace necesario un mecanismo que proteja al sistema o aplicación de manera automática antes de que se produzca un ataque mediante software actualizable en línea.

---

[91] Cfr.,John Cajas, "Detener las amenazas antes que impacten sobre el negocio, IDS E IPS de Internet Security Systems ", ISS, TECSINFO_16112004.ppt, documento en Power Point, subsidiaria de la empresa ISS en el Ecuador.

Como alternativa en el mercado actual de la seguridad se ofrece la alimentación en línea de la base de datos de antivirus y el pre-parcheo de vulnerabilidades, gestionado de manera automática.

Respuestas proactivas y reactivas.

- El Cisco IDS 4215, es un sistema detector de intrusiones como respuesta tan solo reactiva, característica que lo pone en desventaja frente al ISS Proventía M30 y al Cisco ASA 5020. La base de datos de seguridad de la red, NSDB, a la cual accesa el Ciscos IDS 4215, solo sirve para acceder a la información específica de los ataques, sus enlaces y métodos potenciales para contrarrestarlos. El Cisco IDS 4215 no actúa de manera proactiva, ni previene ataques a futuro. Este dispositivo Cisco IDS 4215 solamente da respuestas reactivas a ataques ya acaecidos y que ya han hecho daño: La terminación de sesión sirve para detener las conexiones intrusas, acciones como el registro de cuentas de acceso a sesiones IP, replay y de paquetes“gatillo” múltiples que podrían desencadenar eventos sospechosos, sirven solo para detectar posibles ataques. En realidad el Cisco IDS 4215 no previene ataques, solamente los detecta.

Además se deben analizar otros **aspectos de los dispositivos integrados** que **complementan sus ventajas**, y los hace superiores a los simples detectores de intrusiones:

- En **el ISS Proventía M30** se puede consultar la base de datos del X-Force® Security Intelligence, donde ISS presta soporte para la correlación de patrones y severidad de ataques de los múltiples eventos identificables como tales. En este Appliance M30, los sensores son **actualizables en forma remota.** El administrador de red puede analizar la correlación de eventos con productos de administración de vulnerabilidades y recibir las sugerencias de parcheo y dónde y cómo obtener esas facilidades. Estas sugerencias sirven para contrarrestar las amenazas en el futuro, y así hacer un parcheo proactivo preventivo, que protege la red antes de que la amenaza ocurra. Se pueden bloquear más de 600 amenazas conocidas con las facilidades del Proventía M30.
- En el **Cisco ASA 5520**, mediante las facilidades del Cisco Meta Event Generador, o Generador de Meta Eventos, se identifican y detienen las

nuevas amenazas y opcionalmente reduce el número de eventos enviados para su análisis a sistemas de monitoreo centralizado. Con la tecnología de del tasación del riesgo, o Cisco Risk Rating, se incorporan la severidad del evento, la fidelidad de la firma, valor de activos, y la relevancia del ataque para calificar un riesgo. Luego de obtener esa calificación, el administrador puede llevar a cabo las acciones de mitigación más adecuadas para ese riesgo. También con el Cisco ASA 5520, se da soporte "en-línea" tanto para la prevención como para la detección de ataques. Esta asesoría en línea proporciona a los administradores de red, control granular de los protocolos, y provee herramientas adecuadas al cliente para afrontar a firmas específicas. Se puede actualizar "en-línea" útil información de amenazas en http://www.cisco.com. Hay que notar como ventaja que este dispositivo Cisco ASA 5520, es el de mayor velocidad de uso efectivo de ancho de banda o throughput.

Por las ventajas expuestas anteriormente, se colige que es preferible y puede considerarse la opción más favorable, el adquirir los dispositivos que integren varios sistemas en uno solo, así como también elegir aquellos productos que tengan acciones reactivas frente a los ataques conjuntamente con la prevención del daño antes de que éstos últimos ocurran. Como se ha visto en este análisis, estas características de prevención proactiva-reactiva están presentes en los dispositivos integrados ISS Proventía M30 y Cisco ASA 5520, por lo cual su desempeño es más ventajoso que aquel de los dispositivos no integrados.

Filtrado de contenido

Las características del filtrado e inspección de contenido ya fueron analizadas en el acápite anterior 3.3.3 literal c.-, de donde **se sigue que las especificaciones que cumplen los productos de seguridad ya analizados, se vuelven verdaderas ventajas para quien las utilice.** Hay que mencionar como desventaja que **toda solución por software no incorporada a los dispositivos debe instalarse en máquinas adicionales, lo cual encarece el costo de su**

hardware e instalación. Este hecho es mucho más notable en los dispositivos no integrados.

Hasta este punto se puede indicar que, las ventajas de las Alternativas 2 y 3 integradas superan ampliamente el desempeño de la Alternativa 1 no integrada, en cuanto al cumplimiento de las especificaciones requeridas**.**

3.3.5 PRESUPUESTO REFERENCIAL Y ANÁLISIS DE COSTOS

Si las Alternativas 2 y 3 superan a la Alternativa 1 en el cumplimiento de las especificaciones desde el punto de vista técnico, sólo se debería escoger entre una de ellas, la 2 o la 3. Pero para el limitado presupuesto del Instituto Geofísico, es preciso también **analizar el costo** de cada una de ellas para escoger cuál sea más conveniente desde el punto de vista económico**.** De manera esquemática el siguiente análisis se lo puede ver en el Cuadro 10.

Alternativa 1

El costo total de la Alternativa 1 es de US$ 22.923, este es un precio elevado debido a que los dispositivos no están integrados en una sola solución, lo cual crea problemas en la configuración e instalación. El Cisco IDS 4215 para las necesidades del Instituto Geofísico tiene un precio no tan asequible. Hay que tomar en cuenta que se podría pagar la licencia del ISS Real Secure Desktop, que tiene servicios de firewall, detección de intrusiones y antivirus incluidos. La desventaja de contratar una solución adicional al Software del Cisco Pix Firewall, es que al definirse un firewall para el servidor Linux con Cisco Pix, se desperdician recursos al definirse otro firewall para las aplicaciones con ISS Real Secure Desktop. Hay que tomar en cuenta que la licencia de Desktop para cerca de cien estaciones está sobre los $10,000.00, además estas facilidades de software necesariamente se instalan en conjunto con el Windows 2000 Server y Base de Datos MS Server. Para una solución por software del firewall con Cisco Pix en combinación con ISS Real Secure Desktop se tiene la facilidad del ISS Site Protector Third Party Module, que provee la interfaz de software para trabajar con las aplicaciones Cisco Pix y el ISS Real Secure Desktop. Las desventajas de

esta solución por software de ISS combinado con el firewall Cisco Pix 515 E se presentan en el momento de integrar el Servidor Windows 2000 Server y la base de datos MS Server, con el servidor Linux ya existente. Se desperdician los servicios de Firewall y los costos se elevan por el hardware adicional que se debería comprar para instalar el ISS Real Secure Desktop con el Windows 2000 Server.

Cisco Pix 515 E UR	US $ 6.955,00
más SMARTnet Onsite 8x5xNBO-Categoría 9 de Checkpoint para Firewall-1	1.138,00
Total Cisco Pix con Checkpoint sin IVA	8.093,00

Más solución por software	
ISS Real Secure Desktop (Antispyware, firewall, IPS, IDS) 50 estaciones	US$4,779.50
Instalación y configuración	400.00
Total ISS RealSecure Desktop sin IVA	5,179.50

La posible combinación ISS RealSecure Desktop con el firewall Cisco Pix 515 E UR es US $ 8,093 + 5,179.50 = 13,272.50 que es muy parecido al precio del dispositivo Proventía M30 más el respectivo IVA. Pero la necesidad de compra de hardware adicional para instalar el ISS RealSecure Desktop encarecería los costos. Las licencias y hardware para el Windows MS Server harían que los costos de esta alternativa superen a los costos del Cisco ASA 5520, que sin instalación y configuración son de US $ 12,495.00 Definitivamente la solución de integrar ISS RealSecure Desktop con firewall Cisco Pix 515 E UR es más cara que el dispositivo ISS Proventía M30 o la alternativa del Cisco ASA 5520. Por ello la Alternativa 1 o la combinación del Cisco Pix firewall 515 E UR con ISS RealSecure **se rechaza por el desperdicio de costos y recursos**, y esto es obvio por la falta de integración de sistemas y dispositivos. Nótese que no se ha tomado en cuenta el precio de la licencia de software de filtrado de contenido Web. El software de Websense Enterprise debería integrarse a esta alternativa, lo cual encarece mucho más el costo de licencias por año. En el Instituto Geofísico el personal se concentra en la investigación, y el acceso a Internet no es utilizado con fines maliciosos. El filtro de URLs no deseadas se las puede hacer manualmente, con el peligro de entorpecer el trabajo de los computadores

personales a través de Internet. Más bien se debería proveer la disponibilidad de enlaces a Intranets científicas o relacionadas con geociencias.

Alternativa 2

Proventía M30 no tiene incluida la licencia antivirus. La licencia antivirus para el Proventía M30 es de US $ 1,797.00 sin IVA, con lo cual aumenta el precio del dispositivo. US $ 11,828 + 1,797.00 =13,625.00 La licencia de protección antivirus puede ser reemplazada por un antivirus más económico, como el Norton de Symantec[92] , McAffe[93]. Aunque estas licencias tienen la dificultad que sólo funcionan en medio ambiente Windows. Si el servidor está en Linux y sufre contaminación, no funcionarían los antivirus Symantec y McAffe sino una vez que los códigos maliciosos de los virus hayan contaminado a las estaciones con Windows XP. Con ello se tendría una solución no preventiva, ni proactiva, sino reactiva a ataques de código malicioso. Hay que tomar en cuenta que el soporte y actualizaciones para el segundo y tercer año del dispositivo Proventía M30, es de US $ 7,042.00. Lo cual eleva el costo a tres años de esta alternativa a los US $ 20,667 sin IVA. Este elevado costo de las actualizaciones y parches hace de esta Alternativa 2 muy dependiente de la empresa Internet Security Systems. Esta empresa tiene actualizaciones diarias y prevención de ataques antes de que estos sucedan, esto a la larga ahorrará los costos de los inconvenientes causados por posibles ataques a futuro. Al prevenir los ataques de manera proactiva y preventiva, se ahorran costos de recuperación y tiempo perdido de disponibilidad de servicio.

Alternativa 3

El dispositivo ASA 5520 junto con el AIP-SSM -10 tiene un precio sin IVA de US$ 12.495,00, al cual se debe añadir el costo de instalación y configuración es que es de $ US 2,500.00. Este costo de instalación y configuración es elevado. Se han dado datos para el primer año de contrato, pero no se especifica el costo de licencia por año adicional. En este precio tampoco se toma en cuenta la

[92] http://www.symantec.com/
[93] http://us.mcafee.com/support/default.asp

licencia adicional del software de Websense Enterprise para facilidades adicionales que se necesitan para filtrado de contenido. Este dispositivo sigue la línea de parcheo preventivo, e integra los dispositivos de hardware como el AIP-SSM -10 para los servicios contra ataques de fuerza bruta Anti-X. **Podría considerarse al Cisco ASA 5520, como el equivalente en desempeño al Proventía M30** en Cisco. Hay que notar que el énfasis de ISS Real Secure está en el desarrollo de software de seguridad. La actualización y programas específicos de seguridad de datos hacen a esta empresa ISS **más robusta** para prevenir los ataques contra las vulnerabilidades. CISCO más bien se ha concentrado en el desempeño de la red en general, y no había enfatizado antes la integración dispositivos en seguridad de datos. La competencia con ISS ha obligado a CISCO a ir hacia la integración de varios dispositivos de seguridad en uno solo, como el ASA 5520 para estar a tono con la competencia de los Appliances Proventía, la empresa CISCO también ha comenzado a desarrollar el software preventivo contra amenazas potenciales y reales, y además proveer soporte en línea de actualizaciones. **ISS en esa área de desarrollo de software de seguridad de datos, tiene más experiencia que CISCO**. El mantenimiento preventivo, CISCO solamente lo ha implementado desde el año pasado para sus productos integrados, más por presión de sus competidores. En cambio ISS tiene más de doce años en el desarrollo de software de seguridad de prevención proactiva[94], pues fue la primera empresa que desarrolló la idea de la protección antes del día Cero, es decir, antes de que el ataque ocurra.

[94] CAJAS, John, "Detener las amenazas antes que impacten sobre el negocio, IDS E IPS de Internet Security Systems ", ISS, Subsidiaria, TECSINFO_16112004.ppt, Documento Técnico en Power Point, Quito, Diciembre de 2005, páginas 13-16.

Descripción / Ítem	ALTERNATIVA 1 Integración del CISCO PIX 515 E UR , IDS 4215 y Websense Enterprise	ALTERNATIVA 2 ISS Proventia M30	ALTERNATIVA 3 CISCO ASA 5520
Fuente:	UNIPLEX	TECSINFO	UNIPLEX
Técnico Responsable:	Ing. Fabián Suárez	Ing. John Cajas C.	Ing. Fabián Suárez
Descripción del dispositivo	Firewall Cisco Pix 515E-UR Chasis, Software para Unrestricted, 2 FE, VAC +	Appliance integrado de seguridad. Firewall, Antispam, Detector de Intrusiones Filtrado de contenido, VPNs, hasta 500 nodos. Soporte y actualizaciones directas del fabricante	Cisco ASA 5520 Adaptive Appliance con AIP-SSM-10, Software dedicado, 300 Prs. VPN, 4 Puertos Giga Ethernet + 1 Fast Ethernet Encriptación 3DES/AES
Precio del dispositivo	6.955,00	10.628,00	12.495,00
SMARTnet Onsite 8x5xNBO-Categoría 9 de Checkpoint para Firewall-1	1.138,00		
Dispositivo NIDS	Cisco IDS 4215 Sensor, 80 Mbps		
Precio del dispositivo Cisco IDS 4215	7.295,00		
SMARTnet Onsite 8x5xNBO-Categoría 7 de Checkpoint para Firewall-1	744,00		
Detalle de curso de capacitación	5 personas		16 horas tipo hands-on incluido en el costo de instalación y configuración.
Cursos de capacitación sobre los equipos y sistemas	2.485,00		
Instalación y configuración	1.850,00	1.200,00	2.500,00
Total antes de IVA	20.507,00	11.828,00	14.995,00
IVA 12 %	2.460,84	1.419,36	1.799,00
Costo Total	22.923,04	13.247,36	16.794,40

Cuadro 10.- Cuadro comparativo de los precios de los productos comerciales

Se deduce desde el punto de vista económico, que la Alternativa 1 debe ser desechada por su elevado costo.

Quedan entonces las Alternativas 2 y 3 como posibles candidatas a ser escogidas ya que cumplen con las especificaciones técnicas casi con igual desempeño.

Se sigue del análisis anterior de ventajas y desventajas, y desde el punto de vista económico, que la Alternativa 2 es la más conveniente para el Instituto Geofísico.

4. CAPÍTULO CUATRO: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

a) Se ha cumplido con el principal objetivo que es la elaboración de un plan de seguridad informática en la red de datos del Instituto Geofísico.

b) Con la evaluación se confirma que el orden de los activos críticos de mayor a menor importancia relativa es la siguiente:
Como se puede ver en el Cuadro 11, primero es el Sistema de Información Sísmico y Volcánico, SISV, segundo, la información de Usuarios, Informes y Documental, IUIID, tercero, el Personal de Tecnología de Información con el Personal de Monitoreo, TI + PMV, cuarto, los Computadores Personales, PCs, y finalmente en quinto lugar, el Centro de Información y Respaldos, CIR.
Para una más clara explicación de las conclusiones c, d, e f, g, h, se puede ver en el Cuadro 11, de manera sinóptica y sintética la interrelación entre las áreas de mitigación y los activos críticos correspondientes.

Principal área de mitigación	Área asociada	Subárea	Activo crítico	Activo principal asociado	Orden por criticalidad
Gestión de la Seguridad	Gestión de Sistemas y Red	Autenticación Autorización	SISV	IUIID	1
Gestión de la Seguridad	Gestión de Sistemas y Red	Autenticación Autorización	IUIID	SISV, TI+PMV	2
Gestión de Sistemas y Red	Autenticación y Autorización	Arquitectura y diseño de la seguridad.	TI + PMV	PCs, SISV	3
Diseño y Arquitectura de Seguridad	Gestión de la seguridad	Gestión de la seguridad colaborativa	PCs	SISV, IUIID, TI + PMV	4
Control de Acceso Físico	Monitoreo y Auditoría de Acceso Físico	Gestión de seguridad colaborativa	CIR	IUIID, PCs	5

Cuadro 11.- Resumen de la interrelación entre las principales áreas de mitigación y los activos críticos.

c) De acuerdo con la evaluación de OCTAVE-S, se confirma que el Sistema de Información Sísmico y Volcánico, SISV es el activo de mayor criticalidad y constituye el principal sistema de interés, pues los otros activos críticos colaboran directamente con éste para la continuidad de las operaciones de la red.

d) Se determinó que para el Sistema de Información Sísmico y Volcánico, SISV, la principal área de mitigación encontrada es la de Gestión de la Seguridad, que incluye a la de Gestión de Sistemas y Red, y a la de Autenticación y Autorización. Esto indica que para asegurar este valioso sistema, los Jefes de Área y sobre todo el personal de Tecnología de Información, deben tomar mayor conciencia que son los principales responsables de administrar y gestionar la seguridad con las actividades propuestas por el plan de mitigación.

e) Se encontró que el activo crítico de Información de Usuarios, Informes y Documental, IUIID, se lo considera también crítico pero dependiente de SISV y de TI+PMV, pues es el resultado del procesamiento de sistemas junto con el trabajo de todo el personal científico y técnico. Del mismo modo que para el Sistema de Información Sísmico y Volcánico, SISV, las áreas de Gestión de la Seguridad, Gestión de Sistemas y Red, Autorización y Autenticación, deben también mejorar.

f) Para el activo crítico constituido por el personal de Tecnología de la Información y de Monitoreo, TI + PMV, se encontró que el área de mitigación que compromete a las personas en el plan de seguridad principalmente es la correcta Gestión de Sistemas y Red que incluye a su vez las áreas de Autenticación y Autorización, y de Arquitectura y Diseño de la Seguridad, pues son las personas las que autorizan el ingreso a los sistemas que residen en las computadoras y gestionan los cambios en la topología e infraestructura de red.

g) Se determinó que por las falencias en la topología e ínterconectividad, la mejora en las áreas de mitigación de riesgos de Arquitectura y Diseño de la Seguridad solo se consigue con una adecuada Gestión de la Seguridad en lo que se refiere a la contratación de empresas proveedoras de cableado estructurado, hardware y software de seguridad para proteger en definitiva a las computadoras personales, en donde residen los sistemas, y a través de las cuales se transmite valiosa información.

h) El Centro de Información y Respaldos se protege de los peligros de robo, incendio, inundación, etc., con las actividades sugeridas en el Plan, que se refieren más a las áreas de Control de Acceso, Monitoreo y Auditoría de Seguridad Física, pues obviamente este activo no es de tipo lógico, sino físico. Esta protección física se extiende también hacia las computadoras y hacia las personas que laboran en la red.

i) Seguir las Hojas de Trabajo de OCTAVE-S ha servido de entrenamiento al personal de Tecnología de Información, sobre las políticas o el "deber-ser" de la seguridad. Además estas Hojas han clarificado al personal de TI, la importancia de los activos críticos frente a la misión del Instituto Geofísico.

j) Las actividades sugeridas por el Plan de Mitigación para el área de diseño y seguridad, nos llevaron a la elaboración del Sistema Tecnológico de Seguridad que puede servir de utilidad para la implementación de las nuevas instalaciones del Instituto Geofísico, cuya infraestructura ya se ha comenzado a construir.

k) La presentación del presente plan de seguridad de datos se muestra de manera organizada y con ello se facilita la futura toma decisiones y la adecuada gestión de presupuesto. Este proyecto puede ser utilizado como documento de apoyo para la contratación de empresas proveedoras de servicios y equipos de seguridad de información.

4.2 RECOMENDACIONES

a) Se recomienda implementar, controlar y monitorear las actividades sugeridas en el Plan de Seguridad planteado por el autor de la presente investigación, y de esta forma completar el ciclo de Gestión del Riesgo de una manera integral, continua en el tiempo y definida en sus procesos.

b) En los activos críticos se debe tomar mayor conciencia de la prioridad de los mismos para garantizar la continuidad de las operaciones y la calidad del servicio.

c) OCTAVE-S es proactivo, no sólo reactivo; así el plan de seguridad sirve para crear una base para prevenir posibles daños a futuro, y utiliza también la experiencia de ataques anteriores y pasados para detenerlos e inutilizarlos para que no puedan hacer nuevamente daño a la red de datos
En caso de aprobarse el sistema tecnológico de seguridad, se pueden

integrar las políticas reactivas de las máquinas y personas, con una mejor prevención. Entendiéndose la prevención no sólo a nivel de parcheo de vulnerabilidades en línea, sino también la prevención en las acciones de las personas como un avance en la gestión que comprometa a todos los miembros de la organización en la difícil tarea de la seguridad de datos.

d) El Área de Práctica de Gestión de la Seguridad debe mejorar; esto indica que el personal de Tecnología de Información y los Jefes de Área deben tomar mayor conciencia que son los principales responsables de administrar y gestionar la seguridad de una manera eficiente, efectiva y económica.

e) Se determinó que hay falencias en la topología e ínterconectividad de la red, por lo cual se recomienda mejorar la gestión de la seguridad en lo que se refiere a la contratación de empresas proveedoras de cableado estructurado, hardware y software de seguridad para proteger en definitiva a las computadoras personales, que son en realidad la principal herramienta de trabajo de los investigadores y en donde residen los sistemas que manejan información sensitiva.

f) Se debe proteger con mayor cuidado el Centro de Información y Respaldos con las actividades sugeridas por el Plan de Mitigación, hay que notar que la protección física debe extenderse hacia las personas y las computadoras. Es por ello que se deben contratar seguros para las personas que laboran en la red, para las máquinas y equipos.

g) Se recomienda que las nuevas instalaciones del Instituto Geofísico implementen los equipos sugeridos en el Sistema Tecnológico de Seguridad desarrollado en el Plan de Seguridad del presente estudio.

h) Antes de la presente aplicación de OCTAVE-S se había tratado como dos entidades separadas a la organización y la tecnología, las máquinas versus las personas. En la visión integradora de OCTAVE-S se trata de integrar a

la organización con la operación, la gestión con la tecnología, las personas con las máquinas y sistemas. Por lo tanto, la gestión estratégica se debe integrar con la operación de los sistemas tecnológicos.

i) Se recomienda desarrollar una cultura de seguridad de la información en todo el personal de la institución. Para conseguir aquello, el plan de mitigación sugiere asistir a cursos de entrenamiento y desarrollar alertas de seguridad.

   Muy particularmente, el personal de Tecnología Informática debe ser adecuadamente capacitado en el tema de la seguridad de datos, y sobre todo en el manejo de herramientas actualizadas de administración de seguridad, en el desarrollo de configuraciones seguras y gestión de vulnerabilidades, sobre todo en el servidor Linux.

   El entrenamiento oportuno del personal de Tecnología Informática en administración, gestión y operación de la seguridad de los datos, constituye la mejor prevención de los ataques contra la red de información y sus sistemas.

j) Los riesgos de la red de información son también riesgos de toda la organización. Se debe comprometer a todos los miembros del Instituto Geofísico en la puesta en marcha del plan de seguridad de los datos, y no sólo sea ésta una responsabilidad del personal de Tecnología de Informática. Además, las responsabilidades del Administrador de Red no deben estar concentradas solo en él, y por lo tanto se debe descentralizar el trabajo asignado por funciones para mejorar el control y la misma seguridad.

k) Se recomienda la auto dirección para las futuras evaluaciones; es decir, quien más conoce a la organización es la persona que trabaja en ella, por lo cual su experiencia y habilidad de experto es la que más sirve para la evaluación, esto no significa que se prescinda de consultas a expertos de fuera de la organización.

l) OCTAVE-S ha servido para dar una idea del cómo integrar políticas que estaban desordenadas y no sistematizadas en el Instituto Geofísico, por lo tanto, se sugiere al Comité Técnico, la aprobación del Plan de Seguridad desarrollado en el presente proyecto, y que junto con ello, las políticas propuestas por la evaluación OCTAVE-S se acojan como obligatorias. Las actividades sugeridas pueden convertirse en políticas propias.

5. BIBLIOGRAFÍA

MÉTODO DE EVALUACIÓN OCTAVE-S

ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, "Lista de documentos guía del método OCTAVE-S", Carnegie Mellon University , Software Engineering Institute, Pittsburgh, PA, Enero 2005, se encuentran comprimidos en
http://www.sei.cmu.edu/community/octave-s/OCTAVE-s.zip

LISTA DE DOCUMENTOS GUÍA DEL MÉTODO OCTAVE-S

v01_octave_s_intro v1.doc, introducción al método;
v02_preparation v1.doc, preparación antes de la evaluación;
v03_guidelines v1.doc, normas de aplicación de la evaluación;
v04_org_ws v1.doc, hojas de trabajo organizacionales;
v05_info_asset_ws v1.doc, hojas de trabajo de información de activos críticos;
v06_sys_asset_ws v1.doc, hojas de trabajo de activos críticos de sistemas;
v07_app_asset_ws v1.doc, hojas de trabajo de activos críticos de aplicaciones;
v08_ppl_asset_ws v1.doc, hojas de trabajo de activos críticos de personas;
v09_P1_strat_ws v1.doc, hojas de trabajo de planes y estrategias;
v10_example v1.doc, escenario completo de ejemplo.

INTRODUCCIÓN A OCTAVE-S

ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, "Introducción al enfoque OCTAVE-S", Programa de supervivencia de sistemas en red, Carnegie Mellon University , Software Engineering Institute, Pittsburgh, PA, Agosto 2003, en http://www.cert.org/octave/approach_intro.pdf

ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, "Visión general de OCTAVE", Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 2003, en
http://www.cert.org/archive/pdf/octave_Alt_Exec_Session.pdf

ALBERTS, Christopher, DOROFEE, Audrey, "Criterios de OCTAVE" , Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, Diciembre 2001 en http://www.cert.org/archive/pdf/01tr016.pdf

ALBERTS, Christopher, DOROFEE, Audrey, ALLEN, Julia H., "Catálogo de Prácticas OCTAVE" ,Versión 2, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, Octubre 2001, en
http://www.cert.org/archive/pdf/01tr020.pdf

ALBERTS, Christopher, DOROFEE, Audrey, WOODY, Carol, "Seguridad de la información en pequeñas organizaciones", Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, Enero 2005, en
http://www.cert.org/archive/pdf/dorofee-v6.pdf

DOCUMENTOS NIST

EQUIPO DE CSRC, "Índice de documentos técnicos sobre normas de seguridad de la información", National Institute of Standards and Technology, familia de normas NIST 800, Computer Security Division, Computer Security Resource Center, CSRC, Departamento de Comercio de los Estados Unidos de Norteamérica, Washington DC, Diciembre 2005, en http://csrc.nist.gov/publications/nist/index.html

NORMA ISO 17799

GLENDALESYSTEMS, "Manual ISO 17799", RUSecure(tm), GlendaleSystems.com Ltd, 5 Bridge Street, Leatherhead. Surrey KT22 8BL, United Kingdom, 2001, en http://www.iso17799Software.com/index.htm; http://iso-17799-security-world.co.uk/def.htm;

LUCENT TECHNOLOGIES, "La ISO 17799", Lucent Technologies Inc., Murray Hill, New Jersey, USA, 2005 en http://www.lucent.com/security/ISO17799Summary_White_paper.pdf

DOCUMENTOS DE WEBSENSE ENTERPRISE

"Visión general del producto", 2005 http://www.websense.com/docs/Datasheets/en/v5.5/WebsenseEnterprise_ProductOverview.pdf

"El Administrador de Archivos Adjuntos de Websense", 2005, http://www.websense.com/docs/Datasheets/en/v5.5/Websense_IMAttachmentMgr.pdf

"El Optimizador de Ancho de Banda Websense", http://www.websense.com/docs/Datasheets/en/v5.5/Websense_BandwidthOptimizer.pdf

DOCUMENTOS DE INTERNET SECURITY SYSTEMS, ISS

"Hoja técnica del ISS PROVENTIA M30 Y M50", Atlanta, Georgia, 2005 http://documents.iss.net/literature/proventia/ProventiaM50andM30_Datasheet.pdf

"Guía de Administración de Escritorio ISS PROVENTÍA", Atlanta, Georgia, 2005 http://documents.iss.net/literature/proventia/ProventiaDesktop_AG.pdf

"ISS Site Protector", Atlanta, Georgia, 2005 http://documents.iss.net/literature/SiteProtector/TPM_Datasheet.pdf

"Documento técnico de sistemas de detección de intrusiones de ISS", TECSINFO, documento Word, Especificaciones técnicas.doc, Febrero 2005, Quito.

DOCUMENTOS TÉCNICOS DE CISCO

"Visión general de la solución Cisco Asa 500 Series, Dispositivos adaptativos de seguridad", 2005, http://www.cisco.com/en/US/products/ps6120/products_data_sheet0900aecd802930c5.html

"Hoja técnica del software del CISCO ASA VERSIÓN 7.0", 2005, http://www.cisco.com/application/pdf/en/us/guest/products/ps6120/c1650/cdccont_0900aecd802c1d00.pdf

"CISCO IDS – Característica del software de detección de intrusiones", 2005 http://www.cisco.com/warp/public/cc/pd/sqsw/squidsz/prodlit/_sp_netra_ds.pdf

"Cisco Pix 515-E UR", 2005, http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/ps515e_ds.pdf

"Sensores de prevención de intrusiones Cisco IPS de la Serie 4200" http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_data_sheet09186a008014873c.html

"Hoja técnica de Firewall-1 de CheckPoint" http://www.checkpoint.com/products/downloads/firewall-1_datasheet.pdf

LEYES

"Constitución Política de la República del Ecuador", Gaceta Constitucional, Ed. Germán Arias Barriga, Gráficas Universal, Quito, 2000

"Ley Orgánica de Defensa del Consumidor, Reglamento y Leyes afines", No. 2000-21 Registro Oficial 116 del 10 de julio del 2000, Edi-Gab, Quito, Julio 2003.

"Reglamento a la Ley Orgánica de Defensa del Consumidor", Registro Oficial No. 287 Año II – Quito, Lunes 19 de marzo del 2001 http://www.dlh.lahora.com.ec/paginas/judicial/paginas/Leyconsumidor.htm

"Ley Orgánica de Transparencia y Acceso a la Información Pública" Ley: 2004-34 http://www.hoy.com.ec/pagshtm/ley_de_transparencia.htm http://www.aedep.com/paginas/reglaleytransparencia.htm

"Ley de Comercio Electrónico, Firmas y Mensajes de Datos",

Ley No. 67. Registro Oficial Suplemento 557 de 17 de Abril del 2002.

"Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", trascripción realizada por CORPECE, Quito, 2005 http://www.corpece.org.ec a partir del original publicado en el Registro Oficial No. 735 del Martes 31 de Diciembre del 2002.

"Ley de Propiedad Intelectual",
Ley No. 83. Registro Oficial No. 320 de 19 de Mayo de 1998.

"Reglamento a la Ley de Propiedad Intelectual"
Decreto Ejecutivo No. 508. Registro Oficial No. 120 de 1 de Febrero de 1999.

"Ley de Cartografía Nacional", Registro Oficial No. 643 del 17 de Julio de 1978
"Reglamento de la Ley de Cartografía Nacional" Registro Oficial No.828, Diciembre 9, 1991

5.1 REFERENCIAS DE LOS ANEXOS

ANEXO A:GLOSARIO DE TÉRMINOS OCTAVE-S

ALBERTS, Christopher, et al., " Guía de aplicación de la evaluación ", Documento Word, v03_guidelines v1.doc, Carnegie Mellon University , Software Engineering Institute, Pittsburgh, PA, Enero 2005, se encuentra comprimido en formato ZIP en http://www.sei.cmu.edu/community/octave-s/OCTAVE-s.zip, traducido y adaptado por el autor del presente proyecto de titulación.

ANEXO B: VOLÚMENES DE INFORMACIÓN DEL INSTITUTO GEOFÍSICO

Personal de Tecnología de Información del Instituto Geofísico, “Cuadros B -1, B - 2, B - 3 de Volúmenes de Información”, Documento Técnico del “Proyecto de Desarrollo Informático del Instituto Geofísico", Instituto Geofísico, EPN, Abril de 2005.

ANEXO C: INVENTARIO DE HARDWARE Y SOFTWARE

Personal de Tecnología de Información del Instituto Geofísico, “Cuadros C -1, C - 2, C – 3, C – 4, C - 5 del inventario de elementos de conectividad de la red computadoras, impresoras y software”, Documentos Técnicos del Área Técnica del Instituto Geofísico", Instituto Geofísico, EPN, Abril de 2005.

ANEXO D: PROCESOS Y ACTIVIDADES DE OCTAVE-S

ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, "Introducción al método", Documento Word, v01_octave_s_intro v1.doc, en la “Lista de documentos guía del método OCTAVE-S, op.cit., traducido y adaptado por el autor del presente proyecto de titulación.

ANEXO E: HOJAS DE TRABAJO

ALBERTS, Christopher, et al., “Escenario completo de ejemplo”, en el documento Word, v10_example v1.doc, comprimido en la “Lista de documentos guía del método OCTAVE-S”, op.cit., traducido y adaptado por el autor del presente proyecto de titulación.

ANEXO F: ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS Y PRODUCTOS COMERCIALES

Cfr. Documentos técnicos de Cisco, ISS y Websense Enterprise.

ANEXO G: VENTAJAS Y DESVENTAJAS DE LOS EQUIPOS Y PRODUCTOS COMERCIALES

Cfr. Documentos técnicos de Cisco, ISS y Websense Enterprise.