Cuestión 5 del Orden del Día: **Evaluación de los requisitos operacionales para determinar la implantación de mejoras de las capacidades de comunicaciones, navegación y vigilancia (CNS) para operaciones en ruta y área terminal**

IMPLANTACIÓN DE REDES IPS NACIONALES

(Presentado por la Secretaría)

RESUMEN

Esta nota de estudio presenta la situación actual en la implantación de redes IPS nacionales y las metas esperadas a corto plazo para su implantación.

Referencia

- Plan de implantación del sistema de navegación aérea basado en rendimiento para la región SAM (Versión 1.3 Mayo 2013).

Objetivos estratégicos de la OACI:	*A – Seguridad operacional; y* *C – Protección del medio ambiente y desarrollo sostenible del transporte aéreo*

1. Introducción

1.1 La implantación de redes IPS (Suite de Protocolos Internet) a nivel nacional para soportar las aplicaciones aeronáuticas en apoyo al control del tránsito aéreo, representa una meta regional importante considerada en el *Plan de implantación del sistema de navegación aérea basado en rendimiento para la región SAM (PBIP).* Desde sus inicios, el grupo SAM/IG consideró la implantación de redes nacionales IPS como una mejora importante a implantar y, a este respecto, se elaboró una guía de orientación para la implementación de redes nacionales digitales en protocolo IP para apoyar actuales y futuras aplicaciones aeronáuticas, dentro del programa de mejoras de los sistemas CNS. Esta guía también ha sido un documento base para el estudio de la REDDIG II.

1.2 De la misma forma, para garantizar la seguridad en estas redes, se elaboró una guía de seguridad para la implantación de redes IP, la cual se presentó en la reunión SAM/IG/11 y se circuló a los Estados para su revisión.

1.3 Asimismo, con la contribución de los proyectos RLA/03/901 y RLA//06/901, se realizó un curso y dos seminarios/taller sobre redes IP.

1.4 Gracias a la guía de orientación y los eventos de capacitación, se establecieron recomendaciones a la hora de implantar redes IP nacionales. Se consideró como una recomendación que la red IPS debe ser exclusivamente privada. Cada Estado podrá seleccionar el proveedor de los elementos IPS que estime conveniente; sin embargo, deberá considerar que esa elección debe ser prácticamente definitiva, ya que no es recomendable de ninguna manera disponer de equipamiento con idéntico fin pero de diferentes marcas, ya que este hecho obligará a multiplicar innecesariamente, capacitación, repuestos, recursos humanos y gestión remota.

1.5 Asimismo, se consideró que es una decisión de cada Estado (basada en sus políticas técnicas y económicas) elegir si la red IPS deberá ser soportada por redes terrestres o satelitales (o bien un mix de ambas), una red de enlaces propios o arrendados a proveedores de servicios de comunicaciones, transportada sobre líneas dedicadas o conexiones conmutadas. Las conexiones conmutadas, a su vez, pueden ser de circuitos conmutados o de paquetes/celdas conmutadas. La red deberá ser instalada de forma tal de permitir la visualización y gestión remota de todos y cada uno de sus componentes.

1.6 Otra consideración importante que cada Estado podrá utilizar las direcciones y el esquema de direccionamiento que prefiera, pero es recomendable que las direcciones de red sean asignadas en bloques continuos, que la distribución de bloques de direcciones se realice en forma jerárquica, de forma tal de permitir la escalabilidad de ruteo y que sea posible poder configurar subredes, para poder aprovechar al máximo cada red asignada. Mayor información se puede encontrar en la guía y los eventos de capacitación que se encuentran en la página WEB de la Oficina Sudamericana de la OACI.

2. Análisis

Implantación de redes IPS nacionales

2.1 Con la implantación del AMHS, la mayoría de los Estados de la Región han mejorado sus enlaces utilizando protocolo IP, pero muy pocos han implantado redes IP nacionales con las características arribas indicadas. Prácticamente un solo Estado de la Región lo ha implantado de esa forma, los servicios que este Estado ha montado sobre la red IPS es el AMHS y datas radar y tiene previsto desplegar en la red otros servicios de datos como aplicaciones AIS y/o MET y servicios operacionales de voz (comunicaciones ATS directas o conmutadas).

2.2 Otros Estados de la Región que tienen instaladas aplicaciones AMHS, datos radar en IP y voz en IP tienen montado las aplicaciones en diferentes redes dificultándose su integración y gestión. Algunos Estados de la Región tienen planificado redes IPS propias a corto plazo y otros mejorar las redes arrendadas a proveedores de servicios de comunicaciones.

2.3 A finales del periodo 2014-2016 se tiene previsto que el 80% de los Estados de la Región hayan implantado redes IPS nacionales con las características arribas citadas. La distribución de implantación en el periodo 2014-2016 sería: 2 para el 2014, 3 para el 2015 y 5 para el 2016. Para el 2018, está previsto el 100% de la implantación. La implantación de redes IP nacionales por Estado se presenta como **Apéndice A** de esta nota de estudio.

Guía de orientación de seguridad para la implantación de redes IP

2.4 La guía de orientación de seguridad para la implantación de redes IP fue presentada en la reunión SAM IG/11 y circulada a todos los Estados de la Región SAM a través de la carta LT 12/3.54 SA302 del 10 de junio de 2013. Se recibió comentarios de un solo Estado (Bolivia) los mismos fueron incorporados en la guía y se presenta como **Apéndice B** de esta nota de estudio.

3. **Acción sugerida**

3.1 Se invita a la Reunión:

a) Tomar nota de la información presentada
b) Analizar las metas de implantación de las redes IP nacionales indicadas en la sección 2 y el Aprendices A para su actualización en base a los planes nacionales establecidos al respecto;
c) revisar para su aprobación la Guía de orientación de seguridad para la implantación de redes IP que se presenta como Apéndice B de esta nota de estudio; y
d) analizar otras consideraciones al respecto que la reunión considere necesario.

- - - - - -

APPENDIX A / APENDICE A

IMPLEMENTATION OF NATIONAL IP NETWORKS / IMPLANTACION DE REDES IP NACIONALES

STATE/ESTADO	IP APPLICATIONS IMPLEMENTED/ APLICACIONES IP IMPLANTADAS	DATE IMPLEMENTATION NATIONAL IP NETWORK FOR ALL IP APPLICATIONS/ FECHA IMPLANTACION RED IP NACIONAL PARA TODAS LAS APLICACIONES EN IP
Argentina	AMHS, DATA RADAR, IP VOICE/VOZ IP	2005
Bolivia	AMHS	2016
Brazil/Brasil	AMHS, DATA RADAR, IP VOICE/VOZ IP	2015
Chile	AMHS	2015
Colombia	AMHS, RADAR	2016
Ecuador	AMHS, RADAR	2014
French Guiana (France) / Guyana Francesa (Francia)	No	2018
Guyana	AMHS	2018
Panamá	AMHS, RADAR	2016
Paraguay	AMHS	2014
Perú	AMHS, RADAR	2016
Surinam	AMHS	2018
Uruguay	IP VOICE / VOZ IP	2016
Venezuela	AMHS	2015

- - - - - - -

APENDICE B

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OFICINA REGIONAL SUDAMERICANA

GUÍA DE ORIENTACIÓN DE SEGURIDAD PARA LA IMPLANTACIÓN DE REDES IP

RESUMEN

Este documento provee una guía para que los Estados de la Región SAM puedan implementar las mejores prácticas de seguridad en las redes de comunicación de datos componentes de la ATN SAM.

Septiembre 2013

ÍNDICE

1. INTRODUCCIÓN

Este documento, es una guía para que los Estados y Organizaciones de la Región SAM, puedan implantar las redes de datos componentes de la ATN SAM con las mejores prácticas de seguridad de la información.

1.1 Antecedentes

1.1.1 La necesidad de contar con una Guía de Orientación de Seguridad para la Implantación de Redes IP viene del programa de trabajo del Grupo de Tarea ATN del antiguo Subgrupo ATM/CNS del GREPECAS (Grupo de Planificación y Ejecución de las Regiones del Caribe y Sur América). Un primer documento inicial de la guía de orientación de seguridad para la implantación de redes IP fue presentado en la Primera Reunión de Coordinación del Proyecto de Aplicaciones Tierra-Tierra y Tierra- Aire de la ATN del Subgrupo CNS/ATM del GREPECAS (Lima, Perú del 19 al 20 de mayo de 2010). El Subgrupo CNS/ATM reemplazaba el Subgrupo ATM/CNS.

1.1.2 La Décimo Sexta Reunión del GREPECAS (Punta Cana República Dominicana del 28 de marzo al 1 de abril de 2011) aprueba una nueva organización para el GREPECAS desactivando todos los Subgrupos (órganos contribuyentes del GREPECAS) transformándolo en Programas y Proyectos (Decisión 16/45 y 16/47).

1.1.3 Todas las tareas relacionadas con la ATN, incluyendo la elaboración de una guía de orientación de seguridad IP, fueron incluidas en el Proyecto D1 Arquitectura ATN SAM, cuyo principal producto entregable es la implantación de la nueva arquitectura para la red digital de la Región SAM que reemplazará la actual REDDIG.

1.1.4 El seguimiento a las actividades para la implantación del proyecto D1, se están llevando a cabo en las Reuniones del Grupo de Implantación SAM (SAM/IG) y sometidas a la revisión del Grupo de Coordinación de Programas y Proyectos del GREPECAS cuya primera Reunión (CRPP/1) se llevó a cabo en la Ciudad de México, del 25 al 27 de abril de 2012.

1.1.5 Con referencia a la preparación de una guía de orientación de seguridad para la implantación de Redes IP, la reunión SAM/IG/10 (Lima, Perú, 1 al 5 de octubre de 2012) consideró la importancia de completar las guías de orientación de seguridad para la implantación de redes IP y de presentar las mismas para la reunión SAM/IG/11 (Lima, Perú, 13 al 17 de mayo de 2013). A este respecto la Sexta Reunión del Comité de Coordinación del Proyecto RLA/06/901 (Lima, Perú, noviembre 2012) aprobó la contratación de un experto a fin de preparar dicho documento.

1.2 Organización del Documento

1.1.6 Este documento se compone de 4 capítulos, que presentan la siguiente información:

Capítulo 1, contiene información introductoria de la guía de orientación y está descrita en la sección 1.1 del documento.

Capítulo 2, provee una descripción de los más importantes aspectos de seguridad de la información, con algunos conceptos contenidos en las Normas ISO/IEC 27000, que presentan a la seguridad como un proceso que requiere la existencia de un sistema de gestión.

Capítulo 3, hace un amplio abordaje acerca de las redes que componen la ATN SAM, con énfasis en la REDDIG II y sus interconexiones con las redes de los Estados de la Región SAM, así como en las aplicaciones que la utilizan.

Capítulo 4, presenta las prácticas de seguridad involucradas con los aspectos gerenciales, operacionales y técnicos. Estas prácticas pretenden el establecimiento de controles de seguridad, los cuales son implementados por medio de dispositivos tecnológicos y por procedimientos.

2. SEGURIDAD DE LA INFORMACIÓN

2.1 Introducción

2.1.1 La situación actual que está viviendo la humanidad, puede ser caracterizada como la Era de la Información, en la que los sistemas están altamente conectados en red, creando, procesando y distribuyendo gran cantidad de información a a altas velocidades.

2.1.2 Con el desarrollo de nuevas tecnologías, centrándose en el uso intensivo de las redes informáticas y de comunicación, el mundo se ha vuelto más pequeño generando una sociedad global basada en la información y conectada por redes complejas e interconectadas entre sí, haciendo de la información un activo de alto valor económico; un entorno donde la información viaja a velocidades crecientes y se accede por los diversos dispositivos y medios de comunicación, utilizados para diversos fines, generando nueva informacion que a su vez, incrementan nuevos mercados, en un ciclo de crecimiento económico y social;creando un cambio de paradigma de lo analógico a lo digital.

2.1.3 En este contexto, donde la información tiene un valor económico y estratégico para las organizaciones la cual debe estar disponible en cualquier momento en diferentes dispositivos conectados a la Internet, surge la necesidad de contar con mecanismos que garanticen la seguridad de la información, disponibilidad, integridad, autenticidad y confidencialidad, entre otros requisitos de seguridad de la información.

2.1.4 Se puede entonces decir que la Seguridad de la Información representa el área de conocimiento dedicada a la protección de los activos de información contra el acceso no autorizado, alteración indebida o su falta de disponibilidad.

2.1.5 Según la Norma ISO/IEC17799:2005, la información es un activo esencial para las actividades de una Organización y como tal debe ser protegida de forma adecuada, especialmente en los ambientes de negocio de hoy en día, los cuales están altamente interconectados, exponiendo la información a una gran variedad de amenazas y ataques.

2.1.6 La información está disponible en distintas formas, sea impresa, hablada o en medios electrónicos, enviada por correo electrónicoy almacenada en discos magnéticos u otros dispositivos de almacenamiento. Lo que importa es la necesidad de protección de todos los tipos de información, para garantizar las actividades de una Organización.

2.1.7 Por lo tanto, se puede describir a la seguridad de la información como la protección de toda información contra las amenazas y garantizar la continuidad de los negocios, la mitigación de los riesgos, la maximización del retorno de inversión (ROI) y posibilitar nuevas oportunidades de negocio.

2.1.8 En este contexto, la seguridad de la información es obtenida a partir de un conjunto de controles, que incluyen políticas, procesos, procedimientos, estructuras organizacionales y funciones de *hardware* y *software*.

2.1.9 La información como una actividad dinámica, con nuevas amenazas que aparecen cada día, es conveniente que sea tratada con una visión sistémica, basada en principios de gestión de procesos, ejecutando todo el ciclo PDCA (*Plan, Do, Check, Act*), buscando siempre la mejora continua de todo el sistema.

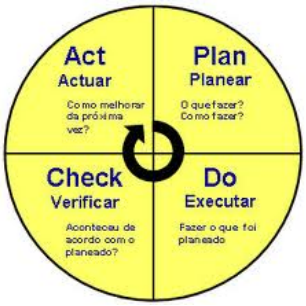


Fig. 1 – El Ciclo PDCA

2.1.10 La definición de los controles de seguridad están basadas en requerimientos legales y en las mejoras prácticas del mercado. Desde el punto de vista de la legalidad, los controles esenciales, básicos, incluyen:

a) La protección de los datos y la privacidad de la información personal;

b) La protección de registros organizacionales; y

c) Derechos de propiedad intelectual.

2.1.11 Los controles asociados a las mejoras prácticas de mercado incluyen:

a) El documento conteniente la política de seguridad de la información;

b) La atribución de responsabilidades;

c) La educación, concientización y entrenamiento en seguridad da información;

d) El procesamiento correcto en las aplicaciones;

e) La gestión de las vulnerabilidades técnicas;

f) La gestión de la continuidad del negocio; y

g) La gestión de incidentes de seguridad de la información y mejoras.

2.2 Conceptos Básicos

2.2.1 Para mejor comprensión de los aspectos involucrados en la seguridad de la información, se presentará a continuación algunos conceptos básicos, basados en las Normas ISO/IEC 27000:2007.

a) **Activo:** se considera cualquier cosa que tenga valor para la Organización. Por lo tanto, cada Organización determinará que es importante y necesario proteger.

b) **Amenaza:** se puede definir como la causa potencial de un incidente no deseado que pueda causar daño en un sistema u Organización. También cualquier persona, entidad, software malicioso, que pueda tener motivación para explorar una vulnerabilidad.

c) **Vulnerabilidad:** Es una fragilidad de un activo que puede ser explorada por una o más amenazas.

d) **Probabilidad del Riesgo:** Se caracteriza por la posibilidad de que una amenaza pueda explorar alguna vulnerabilidad y comprometer uno o más principios de la seguridad.

e) **Impacto:** Es el grado del daño que puede ser causado a un activo cuando una amenaza potencial explora una vulnerabilidad. Es relativo, pues depende de la percepción del valor de la información por sus propietarios.

f) **Criticidad del Riesgo:** Consiste en la evaluación combinada de la probabilidad del riesgo a ocurrir y de su impacto. La criticidad depende de tres factores: de las amenazas y probabilidades – que determinan la probabilidad del riesgo – y del impacto. Con la criticidad definida, es posible establecer los controles de seguridad para la protección del activo.

g) **Riesgo:** Es la combinación de la probabilidad de un evento y de sus consecuencias.

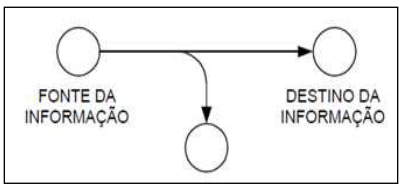
h) **Incidente: U**na o más serie de eventos de seguridad de la información no deseados o no esperados, que tengan una gran probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.

i) **Evento: E**s la ocurrencia identificada de un estado del sistema, servicio o red, que indica una posible violación de seguridad de información, la falta de controles o una situación previamente desconocida que puede ser relevante para seguridad de la información. Tome nota que un evento de seguridad de la información es cualquier cosa que merezca investigación por parte de los responsables de la seguridad de la información. Sin embargo no todo evento es un incidente de seguridad de la información.

2.3 Principios de Seguridad de la Información

2.3.1 Según la Norma ISO/IEC 27002:2007, las propiedades más importantes de la información, también llamados principios de seguridad de la información, qué necesitan deprotección son:

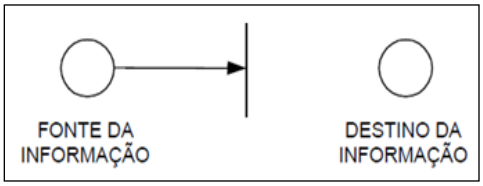
a) **Confidencialidad:** Capacidad de un sistema, para impedir que usuarios no autorizados tengan acceso a determinada información que fue delegada solamente a usuarios autorizados. La pérdida de la confidencialidad puede ser obtenida por medio de la interceptación. La figura siguiente ilustra dicha situación:



Fuente: SANTOS (2011)

Fig. 2– Pérdida de la Confidencialidad

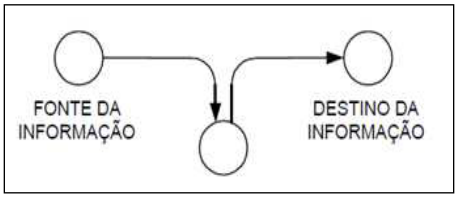
b) **Disponibilidad: I**ndica la cantidad de veces que el sistema cumplió una tarea solicitada sin fallas internas, para un número de veces en que fue solicitado a ejecutar la tarea. La pérdida de la disponibilidad pode ocurrir por medio de una interrupción.



Fuente: SANTOS (2011)

Fig. 3 – Pérdida de la Disponibilidad

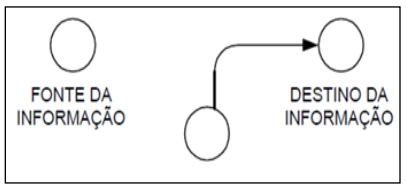
c) **Integridad:** atributo de seguridad que indica si una información puede ser alterada solamente de forma autorizada. La pérdida de la integridad puede ocurrir por modificación.



Fuente: SANTOS (2011)

Fig. 4 – Pérdida de la Integridad

d) **Autenticidad:** capacidad de garantizar que un usuario, sistema o información es el **mismo que se dice ser; y**



Fuente: SANTOS (2011)

Fig. 5 – Pérdida de la Autenticidad

e) **No rechazo:** o no repudio, es la capacidad del sistema de proveer pruebas de que un usuario ejecutó una acción en el sistema. Por lo tanto, el usuario no puede negar la autoría de la ejecución.

2.4 Escenario Actual

2.4.1 La dinámica del mundo moderno impone a los administradores de los sistemas de información una serie de amenazas, que pueden impactar de forma significativa en los negocios de las Organizaciones. Tales amenazas buscan explorar las vulnerabilidades existentes en las redes y en las aplicaciones. Por lo tanto, es importante conocer las amenazas, pero es mucho más importante que se conozcan las vulnerabilidades y que se apliquen los controles para mitigar dichas vulnerabilidades.

2.4.2 El escenario actual es influenciado por las características de las redes modernas, de entre las cuales se destacan:

a) **Automatización:** las redes de hoy estan altamente interconectadas lo que ha cambiado la forma de actuación de los ataques, los que ocurren de forma distribuida, con el uso de miles de computadoras para hacer en minutos algo que tomaría años en un solo equipo. Un ejemplo es la ruptura de la encriptación DES (*Data Encryption Standard*) antes de lo previsto.

Fig 6 – La automatización multiplica el poder del atacante

b) **Acción Remota:** El avance de la interconexión de las redes eliminó barreras físicas y acortó distancias, posibilitando que un ataque sea comandado a miles de distancia del activo atacado, que dificulta la identificación de la toma de acciones punitivas, por involucrar aspectos jurídicos de diferentes Estados.

c) **Anonimato:** La sensación de anonimato, de estar invisible", atrae a los chicos malos para la práctica de actos criminales, o que resulta en un gran cantidad de ataques, de distintos propósitos.

d) **Colaboración:** Hoy en día es mucho más sencillo compartir informaciones, por medio de las redes interconectadas. Esto posibilita la divulgación, rápida y de gran alcance, de vulnerabilidades existentes en redes, aplicaciones y sistemas operativos y, a partir de ellas, desarrollar una aplicación que explora una determinada vulnerabilidad (un *exploit*) y difundirla para todos.

2.5 Amenazas, Ataques y Vulnerabilidades

2.5.1 Las vulnerabilidades son fragilidades presentes en sistemas de información, procesos, equipamientos y redes, que pueden causar impactos a las organizaciones, afectando sus negocios.

2.5.2 Según el CERT, de la *Carnegie Mellon University*, 99% de los casos de intrusión a redes son el resultado del ataque en contra de vulnerabilidades conocidas o errores de configuración solucionables. La empresa Secunia (Computer Security - Software & Alerts) publicó un reporte conteniendo las 6 más importantes clases de impactos ocurridos en la mitad del 2010, presentados a continuación:

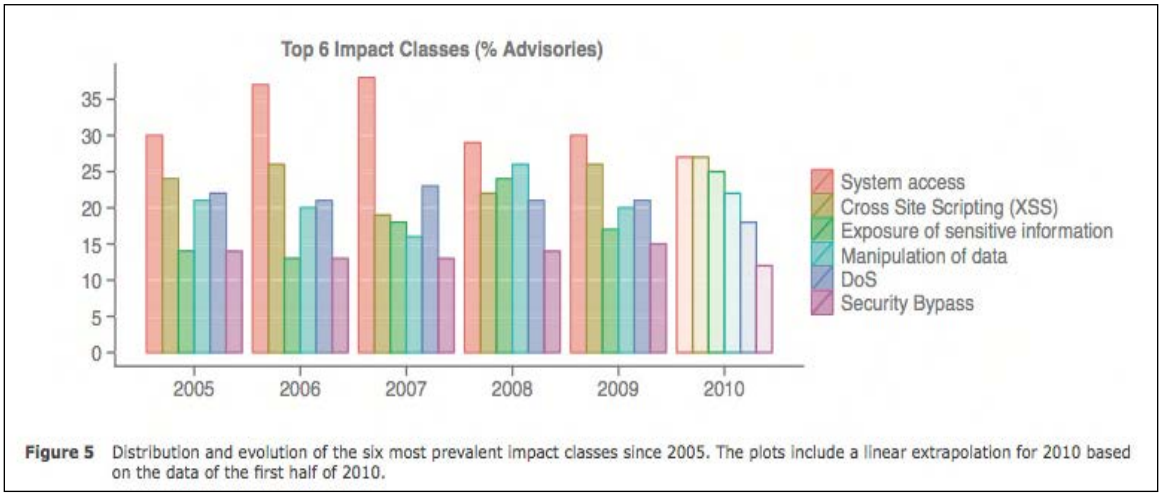


Figure 5 Distribution and evolution of the six most prevalent impact classes since 2005. The plots include a linear extrapolation for 2010 based on the data of the first half of 2010.

Fuente: Secunia - Half Year Report, 2010

2.5.3 Las vulnerabilidades pueden ser clasificadas en los siguientes tipos:

a) Física: son aquellas asociadas a las instalaciones, como el control de acceso, energía, climatización, incendios, inundación, etc.

b) Hardware y Software: están relacionadas a fallas en los equipamientos y en las aplicaciones.

c) Comunicación: involucran las fragilidades relacionadas con los sistemas de comunicación de datos; y

d) Humana: están relacionadas a las fragilidades en concientización, capacitación y formación de los técnicos y operadores de los sistemas y equipamientos.

2.5.4 Los ataques, exploran las vulnerabilidades con el objetivo de causar daño a alguna organización, afectando a uno o varios de los principios de seguridad de la información, sea para interrumpir su operación, obtener información estratégica o para modificar un documento financiero. A continuación se presentan algunos daños:

a) Acceso no autorizado a la red;

b) Exposición de información confidencial;

c) Daño o distorsión de la información;

d) Proveer de datos para el hurto o secuestro de identidad;

e) Exponer secretos organizacionales;

f) Desencadenar fraudes;

g) Paralizar las operaciones del negocio; y

h) Desencadenar accidentes con riesgo de vidas.

2.5.5 Los ataques pueden ser hechos en los datos, en las líneas de comunicación (redes), en el *hardware* y en el *software*.

a) Datos: ataques a los datos afectan los siguientes principios de seguridad: confidencialidad, integridad, autenticidad y no repudio;

b) Redes: ataques a las redes afectan los siguientes principios de seguridad: disponibilidad, confidencialidad e integridad;

c) *Hardware*: ataques al hardware que afectan principalmente el principio de la disponibilidad; y

d) *Software*: ataques al software que afectan los siguientes principios de seguridad: confidencialidad, integridad, autenticidad.

2.5.6 La tabla siguiente presenta un resumen de los tipos de amenazas a los principios de seguridad:

AMENAZA	**PRINCIPIO DE SEGURIDAD**			
	DISPONIBILIDAD	**INTEGRIDAD**	**CONFIDENCIALIDAD**	**NO REPUDIO**
HARDWARE	Robos de equipamientos Desactivación Interrupción de energía Incendio Inundación Calentamiento	NA	NA	NA
SOFTWARE	Programas apagados	Modificación de un programa en ejecución	Copia no autorizada	Archivo de *logs* apagado
DATOS	Archivos apagados	Creación de nuevos archivos Modificación de archivos existentes	Acceso no autorizado	Modificación de las propiedades del archivo
REDES	Mensajes apagados o destruidos	Mensajes modificados	Acceso no autorizado a mensajes	Archivo de *logs* apagado

Tabla 1 – Amenazas a la Seguridad

2.5.7 Los atacantes pueden ser externos o internos a la Organización. Los externos hacen uso de las conexiones externas de las redes de la organización y los internos tienen acceso directo a los sistemas, redes, hardware y datos de la organización.

2.5.8 Básicamente, un ataque es hecho en dos etapas:

a) Búsqueda por vulnerabilidades; y

b) Exploración de las vulnerabilidades.

2.5.9 Por lo tanto, es importante conocer algunas técnicas de recolección de informaciones e utilizadas por los atacantes, así como algunas aplicaciones que exploran dichas vulnerabilidades.

Técnicas de Recolección de Informaciones

2.5.10 Existen hoy día, varias técnicas para recolección de información acerca de la infraestructura de las redes y de los sistemas de información. Serán listadas algunas de ellas, las más comunes, a saber:

- **Ingeniería Social**

2.5.11 Es una técnica que no requiere muchos conocimientos de redes y de aplicaciones, ya que usa la persuasión, explorando la ingenuidad o la confianza del usuario para obtener información que puede ser importante para la violación de la seguridad de un sistema. El foco de atención del atacante son, por lo tanto, las personas y no la tecnología.

- ***Phishing***

2.5.12 La idea de esta técnica es la obtención de informaciones por medio del envío de un mensaje no solicitado por la víctima, intentando hacer que la comunicación sea una información legítima de una institución financiera conocida, un órgano del gobierno, una empresa multinacional o un sitio popular. Asociado a ella, sigue un link que direcciona un sitio falso muy parecido con el sitio de la institución, llevando el usuario a suministrar datos como su l*ogin* y *password*.

- ***Packet Sniffing***

2.5.13 Son herramientas de software instaladas en equipos conectados a una red, en modo promiscuo, que permiten la captura de datos existentes en los paquetes de los mensajes tramitados por la red.

2.5.14 Esta técnica de recolección también es utilizada por los administradores de las redes, como forma de analizar su desempeño, siendo conocidos como analizadores de protocolos.

2.5.15 La búsqueda por vulnerabilidades es hecha por herramientas de *software* que identifican las características de las aplicaciones y sistemas más utilizados en las organizaciones. La técnica consiste en la obtención de respuestas suministradas por el sistema para algunas interrogaciones hechas por el *scanner*. Se puede obtener, por ejemplo: informaciones contenidas en los paquetes, como usuarios y claves y deducir otras características del tipo de tráfico (horas pico, los tipos de paquetes, número de direcciones y conexiones, etc.)

2.5.16 Es una técnica utilizada por los atacantes para la búsqueda de información acerca de los servicios disponibles en una red o sistema, por medio de los puertos de comunicación utilizados por los protocolos de comunicación, a ejemplo del TCP/IP.

2.5.17 Conociendo un puerto abierto, el atacante puede invadir la red y obtener la información o interrumpir la operación de una red o sistema. No hay como impedir la identificación de los puertos abierto, pues la técnica consiste en el envío de solicitudes de conexión, similar a una solicitud de un usuario legítimo de la red.

- ***Scanning* de Vulnerabilidades**

2.5.18 La búsqueda de vulnerabilidades es hecha por herramientas de *software* que identifican las características de las aplicaciones y sistemas más utilizados en las organizaciones. La técnica consiste en la obtención de respuestas suministradas por el sistema para algunas interrogaciones hechas por el *scanner*.
Se puede obtener, por ejemplo:

a) Tipo y versión de sistema operativo;

b) Fabricante de la interfaz de red;

c) Dirección de red (IP) o de enlace (MAC);

d) Puertos de comunicación abiertos;

e) Versiones de software; y

f) *Passwords defaults* en los activos de red y de seguridad.

***Exploits* o códigos maliciosos**

2.5.19 Más conocidos como *malwares*, son los software que inician la secuencia de eventos para la exploración de vulnerabilidades y el consecuentemente comprometiendo la seguridad de la red o sistema.

2.5.20 Algunos *malwares* son presentados a continuación:

- **Virus**

2.5.21 Es un programa de computadora que infecta una máquina por medio de la ejecución de un software legítimo pero infectado. Por lo tanto, un virus depende de otro software para infectar la máquina y ser difundido.

- ***Worm***

2.5.22 Es un programa que se propaga automáticamente en las redes y que no necesita de ejecución explícita por un usuario o por un software. Así, no hay dependencia de otro software para infectar la máquina. Una característica de los *worms* es que consumen muchos recursos de la red y de los sistemas.

- ***Spyware***

2.5.23 Son códigos maliciosos que poseen el objetivo de recolectar informaciones digitadas en formularios *web*, sitios visitados en la Internet, etc. O sea, son técnicas de recolección de datos pero necesitan de infección hecha anteriormente por un *malware*.

- ***Loggers***

2.5.24 Básicamente son software que capturan informaciones en computadoras. Existe los *keyloogers*, que capturan las teclas digitadas en una computadora, y los *screenloggers*, que capturan la imagen de la pantalla (screen).

- ***Trojans***

2.5.25 Son programas que se presentan como algo de útil para el usuario, pero contienen códigos maliciosos.

- ***Exploits***

2.5.26 Programas (o *kits* de programas) que tornan fácil la exploración de vulnerabilidades conocidas de sistemas operativos y aplicaciones. No requieren de muchos conocimientos de redes o de sistemas de información.

2.5.27 Seguidamente, serán descritos algunos ataques de denegación del servicio:

- ***IP spoofing***

2.5.28 El ataque de *spoofing* está basado en una situación en que una entidad logra pasar con éxito por otra. En el caso de IP *spoofing*, el atacante puede falsificar una dirección IP de origen con el envío de paquetes IP de origen diferente de su propia dirección IP, haciéndose pasar por otra máquina. La falsificación de direcciones IP se utiliza principalmente en los ataques de denegación de servicio, donde el atacante necesita que muchas de las respuestas se envíen a la máquina que desea atacar y no a él.

- ***DNS spoofing***

2.5.29 En este ataque, el servidor DNS es invadido por el host blanco del ataque utilizado y su información cambiada a asignaciones incorrectas entre nombres y direcciones. Así, cada vez que una aplicación de usuario utiliza un nombre particular que ha sido cambiado, este comunicará con una entidad falsa. Por ejemplo, si la dirección IP de una página ha cambiado en el DNS, el navegador redirige al usuario a
la página falsa sin informar que dirección está en uso (para eso sirven DNS, navegadores, etc.) El servidor que hospeda esta página falsa está preparado por el atacante para robar información del usuario sin que él se de cuenta.

- ***ARP spoofing***

2.5.30 El ARP spoofing, también conocido como ARP Poisoning o ARP Poison Routing, es un técnica usada para infiltrarse en una red Ethernet conmutada(basada en switches y no en hubs), que puede permitir al atacante leer paquetes de datos en la LAN (red de área local), modificar el tráfico o incluso detenerlo.

2.5.31 EL principio del ARP Spoofing es enviar mensajes ARP falsos (falsificados o spoofed) a la Ethernet. Normalmente, la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro nodo (del nodo atacado), como, por ejemplo, la puerta de enlace predeterminada (Gateway). Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo). El atacante puede incluso lanzar un ataque tipo DoS (Denegación de Servicio) contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

2.5.32 El ataque ARP Spoofing puede ser ejecutado desde una máquina controlada (el atacante ha conseguido previamente hacerse con el control de la misma: intrusión), o bien la máquina del atacante está conectada directamente a la LAN Ethernet.

- ***DoS***

2.5.33 DoS (*Denial of Service*) es un ataque que tiene el objetivo de interrumpir la disponibilidad de un determinado servicio, sistema o red. Muchas de las técnicas utilizadas son conocidas como *flooding (*inundación*)* y sus blancos son los servidores utilizados por varios usuarios, como DNS y de páginas *web*.

2.5.34 Una ampliación del poder de este tipo de ataque es el DDoS (*Distributed Denial of Service*), donde el atacante hace uso de varias máquinas (miles) para atacar un determinado servicio, servidor o sistema.

3. LA ATN SAM

3.1 Introducción

3.1.1 El concepto CNS/ATM de la OACI considera que los nuevos servicios serán soportados por la ATN (*Aeronautical Telecommunications Network*), que engloba las Redes Regionales. En el caso de la Región SAM, la ATN SAM está compuesta por una red digital regional, la REDDIG II, y las redes de cada Estado.

3.1.2 Para cumplir con los requerimientos operacionales, la REDDIG II fue concebida con dos *backbones*, uno satelital y otro terrestre y debe asegurar:

a) Disponer de dispositivos de ruteo, equipos y enlaces satelitales, asimismo servicios terrestres, con todas las interfaces de canal con que hoy cuenta la red actual (REDDIG), adicionando las necesarias para el soporte de los futuros servicios basados en el concepto CNS/ATM;

b) La aplicación generalizada del protocolo IP en la red de transporte para las comunicaciones aeronáuticas de voz y datos;

c) El establecimiento de parámetros de calidad de servicio adecuados;

d) Mantener los servicios analógicos en aquellos casos que aun sean necesarios (AFTN, datos radar de equipos antiguos, etc.);

e) Mantener la conexión a la red MEVA II;

f) Mantener una administración centralizada y común para la red;

g) Mantener el alto grado de disponibilidad alcanzado por la actual REDDIG;

h) Ser el medio de integración regional de los sistemas de redes nacionales desarrolladas por los Estados de la Región; y

i) Dar soporte a las comunicaciones regionales de una manera costo-eficiente, con alta confiabilidad, disponibilidad y mínimo retardo.

3.1.3 Las características mínimas de la REDDIG II son:

a) Accesos satelitales y terrestres;

b) Topología mallada, flexible, multiprotocolo, multiservicio y de área externa;

c) Ser escalable y de fácil expansión;

d) Redundancia y encaminamientos satelitales y terrestres;

e) Ser de arquitectura abierta, basada en protocolo IP;

f) Permitir la migración a otras tecnologías de redes;

3.1.4 Se observa la definición del protocolo IP para la implantación de la nueva REDDIG, así como la existencia de dos *backbones*, uno terrestre y otro satelital, con redundancia de equipamientos garantizando alta confiabilidad, disponibilidad y mínimo retardo.

3.1.5 Otra característica importante es la compatibilidad con protocolos y servicios existentes en la actual REDDIG, incluyendo los servicios analógicos, a ejemplo de la AFTN.

3.1.6 La red satelital está proyectada para operar con el protocolo TCP/IP bajo la administración de los Estados da Región SAM y operada por la OACI, mientras que la red terrestre está proyectada para uso del MPLS y es un servicio prestado por una empresa privada.

3.1.7 Estudios realizados por los expertos apuntan para una disponibilidad de 99,999985002% de la red mixta (satelital y terrestre), correspondiendo a una indisponibilidad mensual de 0,02 min/mes.

3.1.8 Las figuras siguientes presentan de forma esquemática la topología proyectada para la REDDIG II:

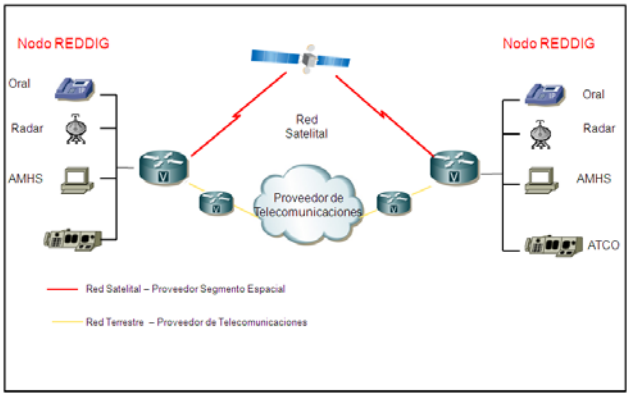


Fig 8 – La REDDIG II – Topología

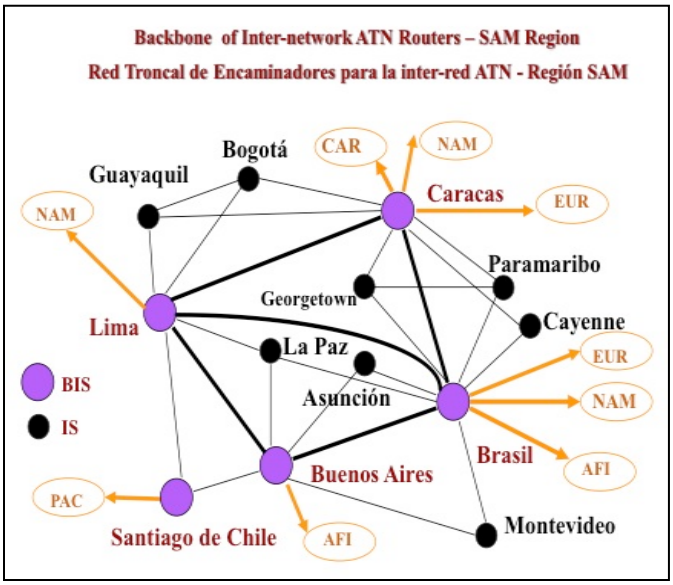


Fig 9 – La REDDIG II – Puntos de Interconexión

3.2 **Servicios de la ATN**

3.2.1 La lista de requerimientos de servicios para el apoyo a la navegación aérea en la Región SAM, incluyendo los previstos a corto, mediano y largo plazo, a ser transportados por la REDDIG II se compone de los siguientes:

Servicios actuales

3.2.2 Los que surgen de los requisitos contenidos en el Plan de Navegación Aérea de las Regiones del Caribe y de Sudamérica y que a la fecha se encuentran operativos casi en su totalidad, a saber:

a) Tabla CNS1A (Plan AFTN); y

b) Tabla CNS1C (Plan de circuitos orales directos ATS). Servicios futuros

c) Los que surgieron de la interconexión MEVA II – REDDIG;

d) El Servicio de Teleconferencia para las unidades de gestión de flujo (FMU) o puestos de gestión de flujo (FMP), a realizarse en forma diaria entre todas las unidades de la Región, inicialmente para veinte usuarios;

e) El Intercambio de planes de vuelo y/o información radar, por los métodos convencionales, de acuerdo a los respectivos MoU (Memorandos de Entendimientos) suscriptos o a subscribirse;

f) Los requerimientos de interconexión AMHS, reemplazando progresivamente el servicio AFTN, de acuerdo a los respectivos MoU (Memorandos de Entendimientos) suscriptos o a subscribirse;

g) Los requerimientos de interconexión AIDC, reemplazando progresivamente el servicio Oral ATS;

h) El Intercambio de datos ADS-B y multilateración, entre todos los ACCs de FIRs colindantes;

i) La Interconexión de sistemas automatizados utilizando Asterix 62 y 63, entre todos los ACCs de FIRs colindantes.

j) Los requerimientos AIM: respecto a este particular, a la fecha no se dispone de un requerimiento concreto;

3.3 **Características Técnicas del Sistema de Ruteo (SR)**

3.3.1 Desde el punto de vista de la seguridad de la información, uno de los activos más importantes de la REDDIG II son los enrutadores, los cuales poseen las siguientes características técnicas:

a) La cantidad mínima necesaria de memoria que atienda a todas las funcionalidades exigidas, en conformidad a las recomendaciones del fabricante.

b) Protocolo de gerenciamiento SNMP y MIB-II implementados en conformidad con la RFC 1157 y con RFC 1213, respectivamente.

c) Compatibilidad del Gateway para voz sobre IP que atienda a todas las funcionalidades requeridas.

d) Las características necesarias para la implementación de los protocolos RTP/RTCP y RTP "header compression" en conformidad con la RFC 2508.

3.3.2 Los enrutadores permiten:

a) Priorización de tráfico por tipo de protocolo y por servicios de la pila de protocolos TCP/IP.

b) La utilización de protocolo que viabilice el establecimiento de clases de servicio, con reserva de banda, para garantía de priorización de aplicaciones críticas, en conformidad con estándares IP definidos (RFCs).

c) La compatibilidad, inclusive para VoIP, con enrutadores Cisco de los más variados tipos, ya existentes en los nodos de la REDDIG.

d) Disponer de funcionalidad de acceso remoto, que permita como mínimo cinco (5) conexiones simultáneas, con la utilización de claves de diferentes niveles, que posibiliten restricciones a la configuración de los equipos y a comandos que alteren su funcionamiento.

e) Estar interconectado con el sistema de enrutamiento del proveedor de servicio terrestre.

f) Poseer manejo del enrutamiento alterno para el backbone MPLS terrestre automático en caso de falla.

g) Tener capacidad de técnicas de compresión de encabezamiento, aceleración TCP y balance de carga.

h) Disponer todos los puertos necesarios para satisfacer los requerimientos actuales y futuros.

i) Establecer comunicaciones permanentes y conmutadas para voz y datos. Las comunicaciones conmutadas se establecerán a solicitud del usuario.

j) Establecer grupos cerrados de usuarios para tráfico telefónico y de datos.

k) Incluir una métrica que permita establecer de manera automática los caminos que proporcionen el mínimo retardo a las comunicaciones dentro del ancho de banda disponible en la red.

l) Incluir las facilidades para la definición de los circuitos, direccionamientos, velocidades de transmisión y priorización del tráfico con la aplicación de calidad de servicio (QoS).

m) Establecer redes privadas IP (VPN), e interconectarse con las redes públicas.

n) Incluir los elementos necesarios para sincronizar la red.

o) Estar integrada al sistema de gestión de red (NMS).

3.3.3 Implementan los protocolos de enrutamiento:

a) RIPv1 (RFC 1058).

b) RIPv2 (RFCs 2453, 1723 e 1724).

c) EIGRP.

d) OSPF versión 2 de acuerdo con las siguientes RFCs (RFC 2328, RFC 1793, RFC 1587 e RFC 2370).

f) BGPv4 conforme RFCs 4271, 4272 4360, 4374, 4451, 4456, 1966, 1997, 2796, 2439, 2858, 2918.

3.4 Tolerancia a fallos y recuperación

3.4.1 La arquitectura del backbone satelital de la REDDIG II y los sistemas que componen el suministro fue proyectada para ser tolerante a fallas, no existiendo ningún elemento común cuya falla provoque el cese de los servicios que presta la red. Una eventual falla solo puede producir una degradación gradual de los servicios que presta la red. La siguiente figura presenta el esquema general de tolerancia a fallas:

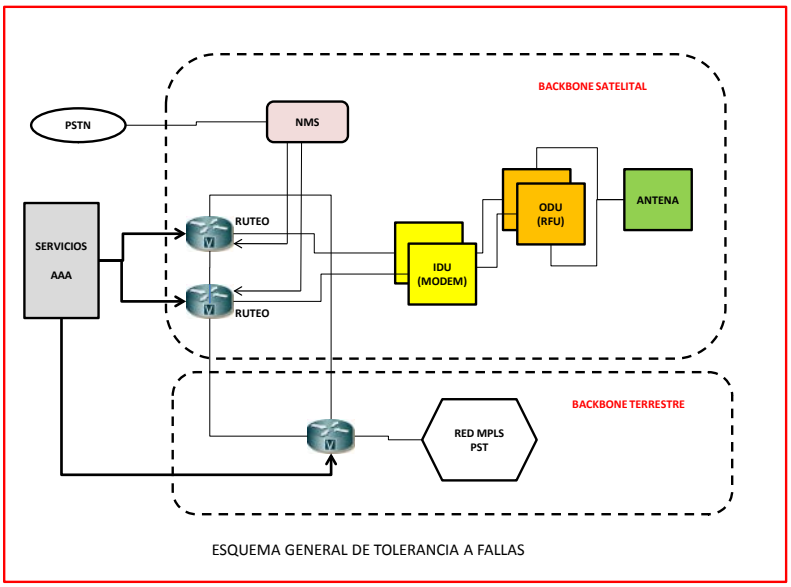


Fig 10 – Tolerancia a Fallas

3.5 **Red de Acceso**

3.5.1 El backbone terrestre será proporcionado por una empresa privada y poseerá una disponibilidad mensual mínima de 99,5%, con un retardo inferior a 60 ms y una tasa de error inferior a 10^{-7} para el 99,5% del tiempo. Actuará como una infraestructura multiservicios y deberá estar provisto de una Plataforma IP Multiservicios, lógicamente independiente y aislada de cualquier otra red y, en especial, del ambiente público de la Internet. Esta red permitirá la creación de VPN y la implementación de QoS.

4. PRÁCTICAS DE SEGURIDAD PARA LA ATN SAM

4.1 Objetivos de Seguridad

4.1.1 Para atender los requerimientos operacionales de los servicios ATM, la ATN se requiere cumplir con los siguientes objetivos fundamentales de seguridad:

a) Protección de los datos de la ATN en contra acceso no autorizado, modificación o apagado; y

b) Protección de los activos de la ATN contra el uso no autorizado y negación de servicio.

4.1.2 Tales objetivos requieren cumplir con los siguientes principios de seguridad de la información, anteriormente descritos, pero con distintos grados de relevancia:

a) Integridad;

b) Disponibilidad;

c) Confidencialidad;

d) Autenticidad;

e) No repudio; y

f) Responsabilidad.

4.1.3 Tomando en cuenta la característica intrínseca de la aviación civil, en la que es muy importante el acceso de todos los involucrados a la información de un vuelo, la confidencialidad nos es tan crítica como la integridad y la disponibilidad. Por lo tanto, las medidas de seguridad o controles, deben recomendar la implantación de acciones tales que garanticen prioritariamente dichos principios, analizando costo/beneficio de cada acción. O sea, el esfuerzo de protección debe ser proporcional y adecuado a las necesidades de protección. Para esto, es importante tener en cuenta la criticidad de los riesgos asociados a la actividad, conociendo las amenazas, probabilidades, vulnerabilidades y sus respectivos impactos.

4.1.4 La implementación de los principios de seguridad se hace por medio de una serie de controles de la seguridad de la información, como las adoptadas por las Normas ISO/IEC 27000, los cuales pueden ser organizados en:

a) Controles Gerenciales;

b) Controles Operacionales; y

c) Controles Técnicos

4.1.5 La figura siguiente, describe las relaciones entre objetivos de seguridad de la ATN, principios de seguridad, controles de seguridad y acciones de seguridad:

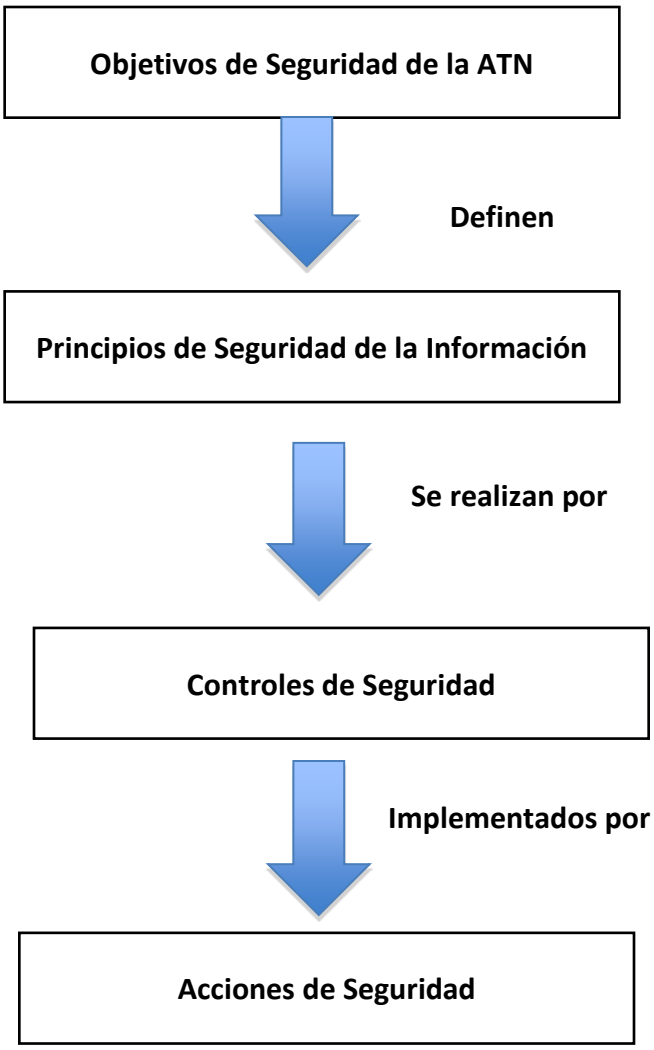


Fig 11– Objetivos de Seguridad

4.2 Estrategia de Seguridad

4.2.1 La estrategia de seguridad adoptada está basada en el concepto de "*Defense in Depth*", donde se implementan múltiples capas de seguridad, formando una estructura de defensa amplia que protege la información en contra de los ataques. Su concepción, está fuertemente apoyada en el uso intensivo de las técnicas y tecnologías existentes hoy en día, con un equilibrio entre los costos, capacidad de protección, performance y aspectos operacionales.

4.2.2 Un punto importante de este concepto es el equilibrio entre los tres principales elementos de la seguridad de la información: Personas, Tecnología y Operaciones:

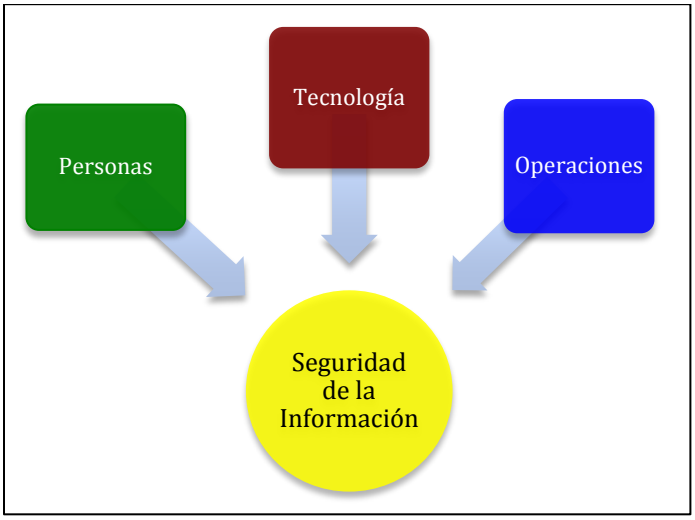


Fig 12– Elementos de la Seguridad

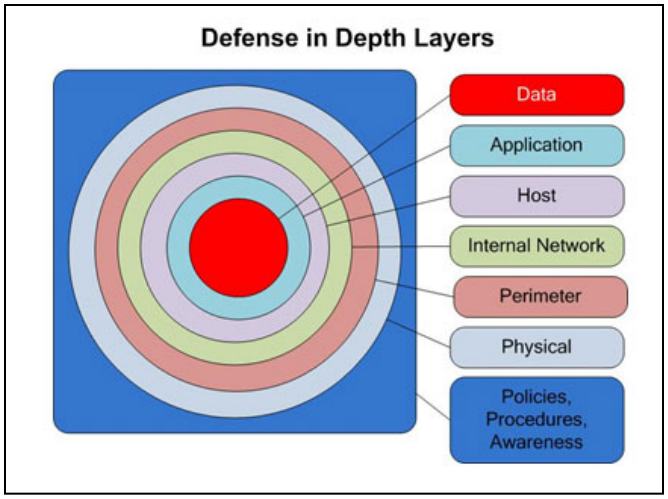
a) **Personas:** Involucra los aspectos relacionados al establecimiento de políticas y procedimientos para la definición de reglas y responsabilidades; la realización de entrenamientos para la creación de una mentalidad de seguridad tanto del personal técnico como de los operadores, así como las medidas de control de acceso físico a las instalaciones críticas.

b) **Tecnología:** Engloba el establecimiento de políticas y procesos para la adquisición de herramientas y productos de calidad, así como la adopción de los siguientes principios:

- Defensa en múltiples áreas, orientadas a la seguridad de la red y de la infraestructura; defensa de las bordas y defensa del ambiente computacional;

- Incluir medidas tanto de detección como de protección mediante infraestructura para detectar intrusiones, analizar y correlacionar resultados y reaccionar seguidamente.

- Defensa en capas: consiste en implementar varios mecanismos de defensa o controles contra el enemigo y su objetivo. Cada uno de estos mecanismos debe presentar obstáculos únicos. La figura a continuación presenta este principio, con la visualización de las capas de datos, aplicación, equipamiento o *host*, red interna, red perimetral, ambiente físico y, involucrando todos, las políticas y procedimientos.



Fuente: www.personal.psu.edu

Fig 12 – Defensa en Capas

c) **Operaciones:** Se centra en todas las actividades necesarias para mantener una postura de seguridad de la organización en el día a día. Incluye:

- Mantenimiento las políticas de seguridad;
- Gestión del comportamiento de la seguridad;
- Evaluaciones de seguridad;
- Monitoreo;
- Detección, alarma y respuesta a ataques;
- Recuperación y reconstitución.

4.3 Controles de Seguridad

4.3.1 La implementación de la estrategia se hace por medio de los controles de seguridad, que se aplican a los tres elementos: consideradas en el contexto de la gestión; personas, tecnología y operaciones.

4.3.2 Controles Gerenciales

4.3.2.1 **Certificación, Acreditación y Evaluación de la Seguridad:** garantiza que la administración de la Organización evalúa los controles de seguridad en sus sistemas y autoriza la operación.

4.3.2.2 **Planificación:** garantiza que la administración de la Organización desarrolla e implementa un plan de seguridad.

4.3.2.3 **Gestión de Riesgos y Vulnerabilidades:** garantiza que la administración de la Organización evalua los riesgos y la criticidad de los daños causados por un ataque.

4.3.2.4 **Concientización y Entrenamiento:** garantiza que los técnicos y operadores tengan conciencia de los riesgos de seguridad asociados a sus respectivas actividades, así como que también conozcan las políticas de seguridad aplicables a sus áreas de actuación y esten debidamente entrenados para la ejecución responsable y correcta de sus actividades.

4.3.2.5 **Adquisición de Sistemas y Servicios:** garantiza que la administración de la Organización asigne los recursos necesarios a la adecuada protección de la información.

4.3.3 **Controles Técnicos**

4.3.3.1 **Control de Acceso:** es la capacidad de limitar el acceso a servicios y recursos solamente a las personas autorizadas, considerando, también lo que cada persona puede utilizar en un determinado recurso o sistema.

4.3.3.2 **Identificación y Autenticación:** es la capacidad de identificar y autenticar usuarios de un sistema u otros recursos.

4.3.3.3 **Protección de las Comunicaciones:** es la capacidad de monitoreo, control y protección de las comunicaciones.

4.3.4 **Controles Operacionales**

4.3.4.1 **Gestión de la Configuración:** garantiza el control de los componentes del sistema, incluyendo hardware, software y los parámetros de configuración del sistema.

4.3.4.2 **Respuesta a Incidentes:** garantiza el tratamiento adecuado a los incidentes de seguridad y los comunica a las respectivas autoridades.

4.3.4.3 **Plan de Contingencia:** garantiza que los operadores posean un plan que garantiza la continuidad de la operación para los usuarios y servicios más críticos en situaciones de emergencia.

4.3.4.4 **Protección de Datos:** garantiza la protección de los datos y de las medidas de almacenamiento del sistema.

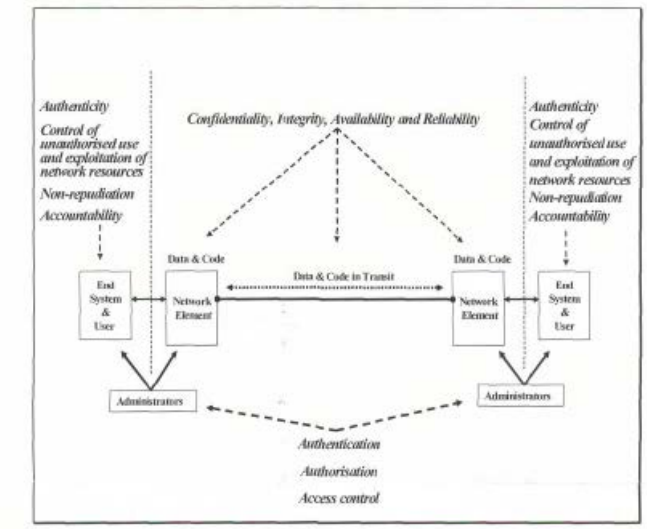
4.3.4.5 **Protección de las Instalaciones:** garantiza que los ambientes poseen acceso controlado.

4.4 **Seguridad en las Redes**

4.4.1 Considerando las capas de red interna y externa de una Organización, así como de la REDDIG II, bajo la estrategia de defensa en capas, se describe a seguir algunos aspectos que toda Organización debe tener en cuenta.

a) Toda organización debe planear, implementar y actualizar un plan de seguridad para las redes de su responsabilidad, teniendo en cuenta los objetivos de seguridad anteriormente descritos por esta guía;

b) Hay que tener implementado un proceso de gestión de riesgos para las redes, considerando el siguiente escenario, conforme la ISO/IEC 120-28-1:2006:



Fuente: ISO/IEC 18028-1:2006

Fig 13 – Áreas de Riesgo en Redes

c) Por lo tanto, hay que considerar las vulnerabilidades involucradas a las redes, con base en las siguientes posibilidades:

Network Facet	Types of Potential Network Security Vulnerability				
	Interruption	Interception	Modification	Intrusion	Deception
Network Users	Users may suffer loss or interruption of service.	User transactions and/or network activity may be monitored.	User details and user data may be modified or destroyed.	Users may be impersonated to gain unauthorized access to facilities.	Users may be impersonated to conduct fraudulent transactions.
Network End-Systems	End-systems may become temporarily or permanently unavailable.	Unauthorized persons may read data or code on end-systems.	Data or code may be modified or destroyed.	End systems may be impersonated to gain unauthorized access to facilities. Unauthorized persons might gain access to system accounts and use them to launch further attacks.	End systems may be impersonated to conduct fraudulent transactions, or to launch further attacks.
Networked Applications	Applications may become temporarily or permanently unavailable.	Data or code may be intercepted in transit, or read on servers, by unauthorized persons.	Data or code may be modified or destroyed.	Unauthorized persons might gain access to system accounts and use them to launch further attacks.	Unauthorized persons might gain access to system accounts and use them to launch further attacks.
Network Services	Services may become temporarily or permanently unavailable.	Data or code may be intercepted in transit, or read on servers, by unauthorized persons	Data or code may be modified or destroyed.	Unauthorized persons might gain access to system accounts and use them to launch further attacks.	Network servers and devices may be impersonated to gain unauthorized access, to intercept network traffic, or to disrupt network services.
Network Infrastructure	Facilities may become temporarily or permanently unavailable			Unauthorized persons may infiltrate facilities.	

Fuente: ISO/IEC 18028-1:2006

Tabla 2 –Vulnerabilidades en Redes

d) La administración debe garantizar la adquisición adecuada de los recursos necesarios para la protección de la información, incluyendo los activos de red (enrutadores, switches, etc) y de seguridad (firewalls, IDS, IPS, etc).

e) Las equipos de mantenimiento y de operación deben estar concientizados y entrenados con respecto a las medidas de seguridad requeridas por el plan de seguridad

f) Los equipamientos y sistemas deben poseer certificación de seguridad.

g) Cada red debe poseer una topología que tenga en cuenta los aspectos de seguridad, considerando por lo menos lo siguiente:

- Los puntos de interconexión con otras redes deben poseer activos de seguridad, como firewalls y IDS/IPS, instalados y adecuadamente configurados y monitoreados.

- Las direcciones IP deben ser proyectadas para que non sean conocidas en la Internet.

- Los firewall deben ser configurados, por lo menos, con las siguientes reglas:

- Política de negación (*deny all*) como default;

- Protocolos *web* (http, https, por ejemplo) solamente *outgoing;*

- Protocolos de e-mail en las dos direcciones.

- Los enrutadores deben ser configurados considerando el uso de ACLs y NAT, así como ocultar las direcciones IP.

- Los enrutadores deben estar constantemente actualizados, con *passwords* y *login* distintos de los de fábrica.

- Las interconexiones de las redes con la REDDIG II deben ser hechas con redundancia de activos, incluyendo los de seguridad, y otras providencias que garanticen la disponibilidad e integridad de la información, así como el desempeño de la red según sus especificaciones.

- Las conexiones con las redes públicas (internet) deben poseer topología que garanticen la seguridad en múltiples capas.

- La administración de la red debe ser hecha por medio del protocolo SNMP versión 3, con la activación de alertas y de SNMP *traps*. El acceso a los dispositivos deben ser hechos mediante el uso de autenticación segura.

- Los links de administración deben ser encriptados.

h) Las líneas de comunicación críticas para la interconexión de las redes de los Estados con la REDDIG II deben ser constantemente monitoreadas;

i) Se debe contar con un proceso de gestión de la configuración de las redes, con procedimientos para la actualización de versiones de software, cambios de hardware y de puntos de conectividad, así como el resguardo de copias *backup y* de *software* de instalación;

j) Es necesario tener procedimientos específicos para el control de acceso físico y lógico a los equipamientos y sistemas de las redes, mediante el uso de claves seguras, equipos de certificación de identidad como tarjetas magnéticas, biometría, etc. Los enrutadores, dispositivos de red y de seguridad deben tener desactivados sus *logins* y *passwords* de fábrica;

k) Los equipamientos y sistemas críticos para la operación, supervisión y monitoreo de las redes deben poseer suministro continuo de energía y climatización adecuada;

l) Los sistemas, aplicaciones y activos de red y seguridad deben estar configurados para ejecutar solamente los servicios realmente necesarios (*hardening*), desactivandose servicios innecesarios a la operación como, por ejemplo, FTP, DNS, etc.;

m) Es necesario que se tenga un equipo de respuesta a incidentes de seguridad debidamente preparado para garantizar la ejecución de las medidas de protección necesarias;

n) Es necesario que se tenga un equipo específico para el monitoreo del estado de los equipamientos y activos de seguridad, tales como firewalls, IDS/IPS, etc.;

o) Es recomendable el uso de VPN para proveer comunicaciones que requieran confidencialidad e integridad de la información. En estos casos, deben ser considerados los siguientes aspectos:

- Seguridad en el *endpoint* y en el *termination point* ;
- Protección contra *software* maliciosos;
- Autenticación;
- Detección de intrusos con IDS/IPS;
- El uso de firewalls; y
- El uso de la técnica de split tunneling.

p) Las redes que soportan convergencia en IP, con el tráfico de voz y datos, deben considerar, por lo menos:

- Uso de QoS para la definición de las prioridades de transmisión de los datos;
- Todos los servidores VOIP deben estar configurados con protección contra software malicioso;

- Los dispositivos VOIP, como computadoras portando softphones, deben poseer firewalls personales activados, así como programas antivirus constantemente actualizados;
- Los servidores VOIP deben estar en una red protegida por firewalls e IDS/IPS;
- Solamente deben estar disponibles las puertas de comunicación estrictamente necesarias para el soporte a VOIP;
- Todos los accesos a los servidores deben ser autenticados.

q) Los accesos remotos (RAS) deben ser implementados considerando, por lo menos:

- Uso de firewalls;
- Enrutadores con ACL;
- Encriptación de los links externos, especialmente los conectados a la internet;
- Alta Autentificación;
- Antivirus actualizado; y
- Auditoria permanente.

r) Las redes inalámbricas WLAN (*wireless*) deben ser implementadas considerando, por lo menos:

- Las interconexiones con la infraestructura de la red principal, deben ser protegidas por firewalls;
- Implementar VPN para la conexión entre un cliente y un firewall periférico;
- Los clientes (computadoras, laptops, smartphones, etc.) deben tener firewalls personales y antivirus;
- El protocolo SNMP debe estar configurado para acceso solamente de lectura;
- Uso de SSH para gerencia de los links; y
- Los dispositivos de acceso a la red deben estar en locales físicamente seguros.

REFERENCIAS

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 - Tecnologia da Informação-Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação. Brasil, 2005.

ANDERSON, Ross. Security Engineering. 2 Edition. John Wiley & Sons. New Jersey, USA, 2008.

CANAVAN, John E. Fundamental of Network Security. Artech House. Boston, USA, 2001.

ICAO. International Civil Aviation Organization - Asia and Pacific Office. ASIA/PAC Aeronautical Telecommunication Network Security Guidance Document. 2nd Edition, 2010.

ICAO. International Civil Aviation Organization. SAM. Guía de Orientación para la Mejora de los Sistemas de Comunicación, Navegación y Vigilancia para Satisfacer los Requisitos Operacionales a Corto y Mediano Plazo para las Operaciones en Ruta y Área Terminal. Versión Final. Lima. Perú, 2008.

ISO/IEC. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 18028-1:2006 - Information technology — Security techniques — IT network security – Part I – Network Security Management, 2006.

SANTOS. Luis E. Curso de Segurança em Redes de Computadores. CEDERJ. Rio de Janeiro. Brasil, 2011.
STALLINGS, William. Network Security Essencials - Application & Standards. 4 Edition. Prentice Hall. USA, 2011.