ORGANIZACIÓN DE AVIACION 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.

Abril 2013

ÍNDICE

1. INTRODUCCIÓN 3
1.1 Antecedentes 3
1.2 Organización del Documento 3

2. SEGURIDAD DE LA INFORMACIÓN 5
2.1 Introducción 5
2.2 Conceptos Básicos 6
2.3 Principios de Seguridad de la Información 7
2.4 Escenario Actual 9
2.5 Amenazas, Ataques y Vulnerabilidades 9

3. LA ATN SAM 16
3.1 Introducción 16
3.2 Servicios de la ATN 18
3.3 Características Técnicas del Sistema de Ruteo (SR) 18
3.4 Tolerancia a fallos y recuperación 20
3.5 Red de Acceso 21

4. PRÁCTICAS DE SEGURIDAD PARA LA ATN SAM 22
4.1 Objetivos de Seguridad 22
4.2 Estrategia de Seguridad 23
4.3 Controles de Seguridad 25
4.4 Seguridad en las Redes 26

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 Tierr0- 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 Subgrupo (órganos contributorios del GREPECAS) transformándolo en Programa 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 seguridad IP fueron incluidas en el Proyecto D1 Arquitectura ATN SAM cuyo principal entregable es la implantación de la nueva arquitectura de red digital para la Región SAM que reemplazará la actual REDDIG.

1.1.4 El seguimiento de la implantación de las actividades del proyecto D1 se está 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 Ciudad de México del 25 al 27 de abril de 2012.

1.1.5 En 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 completarlas la guías de orientación de seguridad para la implantación de redes IP y de presentar la misma 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

1.2.1 Este documento posee 4 capítulos, que comprenden 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 la seguridad como un proceso, que requiere la existencia de un sistema de gestión.

Capítulo 3 hace un amplio abordaje 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 intentan 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 a la humanidad puede ser caracterizada como la Era de la Información, en que los sistemas están altamente conectados en red, creando, procesando y distribuyendo la información en gran cantidad y velocidad.

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, haciendo uso la información como 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, se utilizan para diversos fines, generando nuevas informaciones que, a su vez, incrementan nuevos negocios, en un ciclo de crecimiento económico y social. Hubo 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 y está disponible en cualquier momento en diferentes dispositivos conectados a la Internet, surge la necesidad de contar con mecanismos protectores que garanticen su disponibilidad, integridad, autenticidad y confidencialidad, entre otros requisitos de seguridad de la información.

2.1.4 Se puede así decir que 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 los negocios de una Organización y como tal debe ser protegida de forma adecuada, especialmente en los ambientes de negocio de hoy en día, los cuales son 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 electrónico, por ejemplo, y almacenada en discos magnéticos o otros dispositivos de almacenamiento. Lo que importa es la necesidad de protección de todos los tipos de información para garantizar los negocios de la Organización.

2.1.7 Por lo tanto, se puede caracterizar 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 los investimentos (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 Como es una actividad dinámica, con nuevas amenazas que aparecen cada día, es adecuado 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.

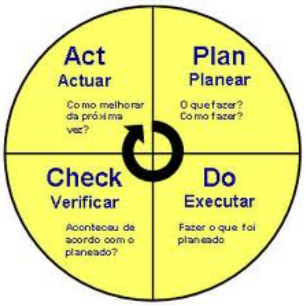


Fig. 1 – El Ciclo PDCA

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

a) La protección de los datos y la privacidad de las informaciones personales;

b) La protección de registros organizacionales; y

c) Derechos de propiedad intelectual

2.1.11 Los controles asociados a las mejores 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 a 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 pude definir como la causa potencial de un incidente no deseado que pueda causar daño en un sistema o 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 pela posibilidad de una amenaza explorar alguna vulnerabilidad y comprometer uno o más principios de la seguridad.

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

f) **Criticidad del Riesgo:** Consiste en la evaluación combinada de la probabilidad del riesgo 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.

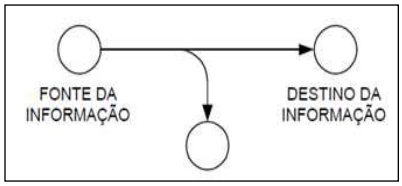
h) **Incidente:** una o más serie de eventos de seguridad de la información no deseados o no esperados, que tengan una gran probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.

i) **Evento:** es una 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 de que un evento de seguridad de la información es cualquier cosa que merezca investigación por parte de los responsables de 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 más importantes propiedades de la información, también llamados de principios de seguridad de la información, qué necesitan de preservación son:

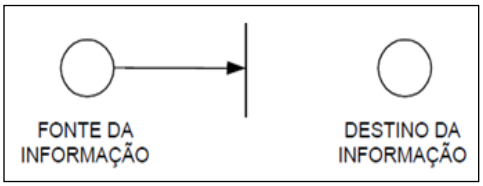
a) **Confidencialidad:** capacidad de un sistema de impedir que usuarios no autorizados tengan acceso a determinada información que fue delegada a solamente usuarios autorizados. La pérdida de la confidencialidad puede ser obtenida por medio de la interceptación. La figura siguiente ilustra dicha situación:



Fuente: SANTOS (2011)

Fig. 2– Pérdida de la Confidencialidad

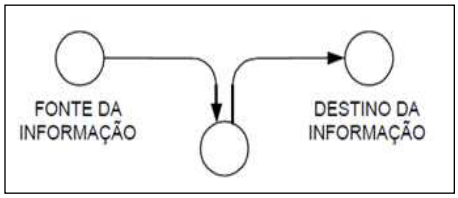
b) **Disponibilidad:** indica la cantidad de veces que el sistema cumplió una tarea solicitada sin fallas internas, para un número de veces en que fue solicitado a hacer la tarea. La pérdida de la disponibilidad pode ocurrir por media de una interrupción.



Fuente: SANTOS (2011)

Fig. 3 – Pérdida de la Disponibilidad

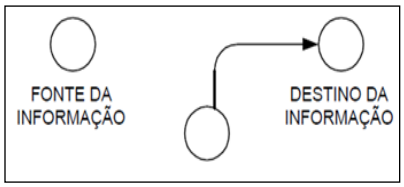
c) **Integridad:** atributo de seguridad que indica si una información puede ser alterada solamente de forma autorizada. La pérdida de la integridad puede ocurrir por modificación.



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 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 aplique los controles para mitigar dichas vulnerabilidades.

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

a) **Automatización:** las redes de hoy son altamente interconectadas lo que cambió la forma de actuación de los ataques, lo 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, o que dificulta la identificación e la toma de acciones punitivas, por involucrar aspectos jurídicos de diferentes Estados.

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

d) **Colaboración:** Hoy día es mucho 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, alguna persona desarrollar una aplicación que explora una determinada vulnerabilidad (un *exploit*) y difundirla para todos.

2.5 Amenazas, Ataques y Vulnerabilidades

2.5.1 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. Ya la empresa Secunia publicó un reporte conteniendo las 6 más importantes clases de impactos ocurridas en la mitad del 2010, presentadas a seguir:

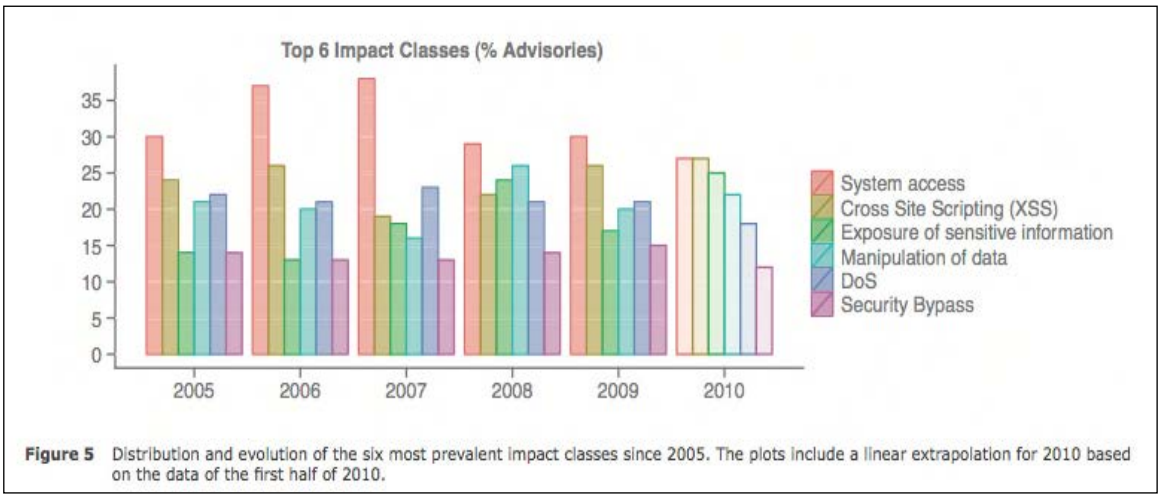


Figure 5 Distribution and evolution of the six most prevalent impact classes since 2005. The plots include a linear extrapolation for 2010 based on the data of the first half of 2010.

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 controle 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 a 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 un o varios dos principios de seguridad de la información, sea para interrumpir su operación, sea para obtener información estratégica o para modificar un documento financiero. A seguir 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 y integridad;

c) *Hardware*: ataques al hardware afectan principalmente el principio da disponibilidad; y

d) *Software*: ataques al software 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 Aquecimiento	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 apagadas o destruidas	Mensajes modificadas	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. Ya 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 informaciones cerca de la infraestructura de las redes e 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 informaciones que pueden ser importantes para la violación de la seguridad de un sistema. El foco de la 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 mensaje no solicitada por la víctima, intentando de 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 para 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:

2.5.16 Es una técnica utilizada por los atacantes para la búsqueda de informaciones cerca de los servicios disponibles en una red o sistema, por medio de las puertas de comunicación utilizadas por los protocolos de comunicación, a ejemplo del TCP/IP.

2.5.17 Conociendo una puerta abierta, el atacante pude invadir la red y obtener la información o interrumpir la operación de una red o sistema. No hay como impedir la identificación de las puertas abiertas, pues la técnica consiste en el envío de solicitaciones de conexión, similar a una solicitación de un usuario legítimo de la red.

- ***Scanning* de Vulnerabilidades**

2.5.18 La búsqueda pro vulnerabilidades es hecha por herramientas de *software* que identifican las características de las aplicaciones y sistemas más utilizados en las organizaciones. La técnica consiste e 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) Puertas de comunicación abiertas;

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 consecuente comprometimiento de la red o sistema.

2.5.20 Algunos *malwares* son presentados a seguir:

- **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 difundir.

- ***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. Existem 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 requiere muchos conocimientos de redes o de sistemas de información.

2.5.27 En secuencia, serón descritos algunos ataques de denegación del servicio:

- ***IP spoofing***

2.5.28 El ataque de *spoofing* es basado en una situación en que una entidad loga 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 envían no a él sino a la máquina que desea atacar.

- ***DNS spoofing***

2.5.29 En este ataque el servidor DNS utilizado por el host blanco del ataque es invadido 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, él se comunicará con una entidad falsa. Por ejemplo, si la dirección IP de una página ha cambiado en DNS, el navegador redirige al usuario a la página falsa sin reporte de 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 diera cuenta.

- ***ARP spoofing***

2.5.30 El ARP *spoofing* es una técnica de suplantación de identidad en el que un atacante intenta suplantar a un destinatario legítimo de la comunicación en respuesta a consultas ARP enviadas por la fuente de tráfico. La respuesta del atacante se envía dentro del dominio de *broadcast* antes de que el destinatario tiene una legítima oportunidad de hacerlo. Así, tanto el equipo de origen como el *swicth* aprenden un mapeo falso entre la dirección MAC (el atacante) y la dirección IP (el destino legítimo). De esto, todos los *frames* están encapsulados por el origen con la dirección MAC del atacante y se conmutan mediante el *switch* en la puerta donde el atacante está basado en el MAC.

- ***Dos***

2.5.31 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*.

2.5.32 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 es 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, como 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, y 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 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 rede 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:

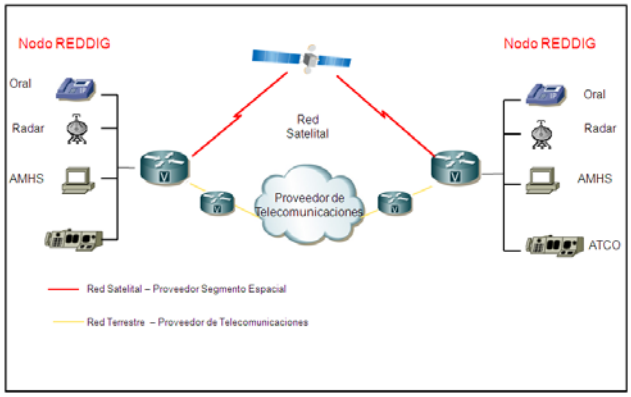


Fig 8 – La REDDIG II – Topología

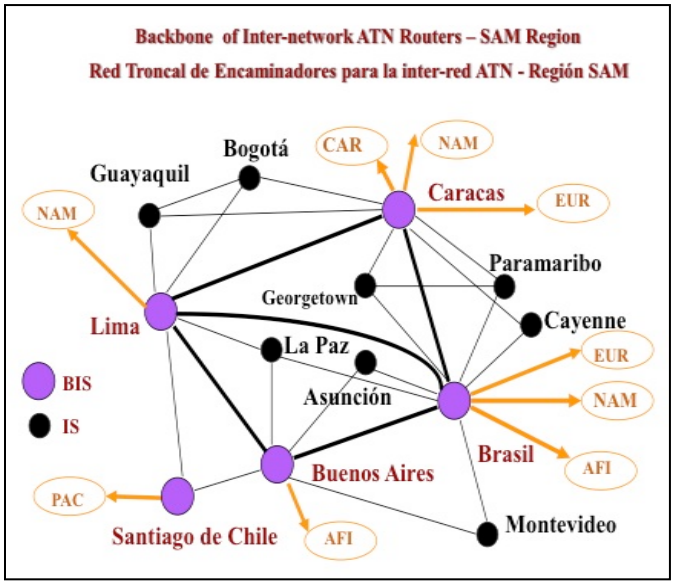


Fig 9 – La REDDIG II – Puntos de Interconexión

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:

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 en su casi 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) Funcionalidad de Gateway para voz sobre IP que atienda a todas las funcionalidades requeridas.

d) Las características necesarias para la implementación de los protocolos RTP/RTCP e RTP "header compresión" 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 interoperabilidad, 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 ports 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 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).

e) 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 figura a seguir presenta el esquema general de tolerancia a fallas:

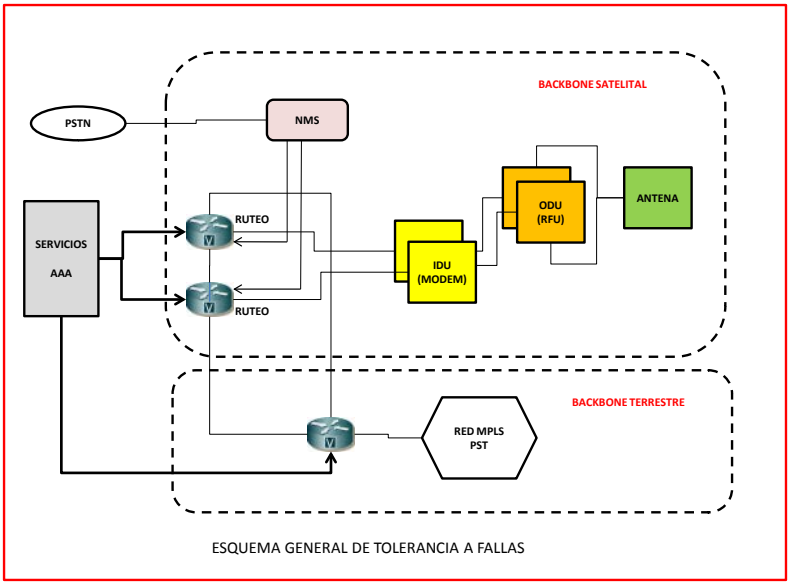


Fig 10 – Tolerancia a Fallas

3.5 **Red de Acceso**

3.5.1 El backbone terrestre será próvido 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 ser provisto por 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 requiere el atendimiento de 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 en contra uso no autorizado y negación de servicio.

4.1.2 Tales objetivos requieren el atendimiento de 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 como ejemplo la característica intrínseca de la aviación civil, en que es mui importante el acceso por todos los involucrados a las informaciones de un vuelo, la confidencialidad nos es tan crítica cuanto 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, cuando de la analice 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, sus probabilidades, las vulnerabilidades y los respectivos impactos.

4.1.4 La implementación de los principios de seguridad se hace por medio de una serie de controles de seguridad de la información, como preconizado pelas 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:

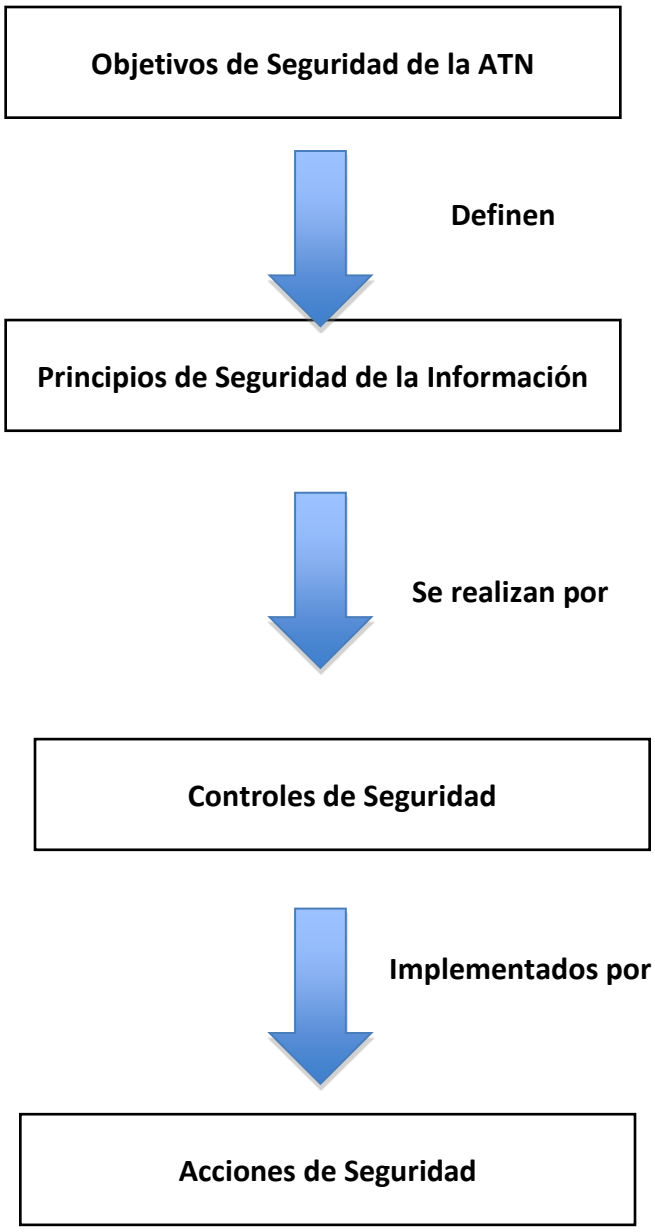


Fig 11– Objetivos de Seguridad

4.2 Estrategia de Seguridad

4.2.1 La estrategia de seguridad adoptada es 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 los ataques. Su concepción está fuertemente apoyada en el uso intensivo de las técnicas y tecnologías existentes hoy 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:

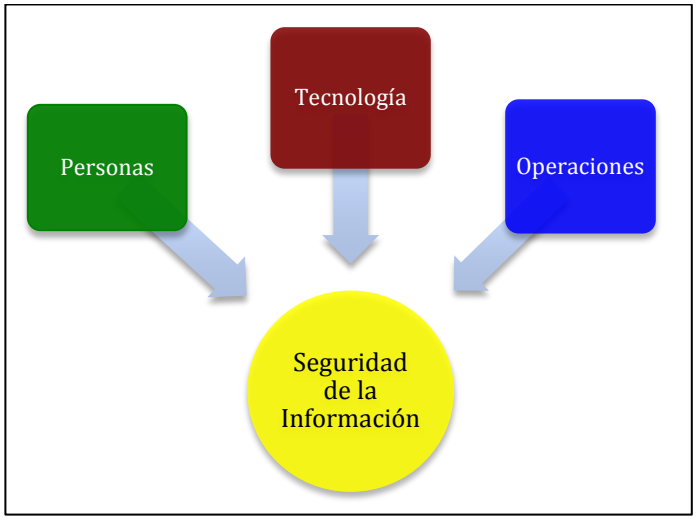


Fig 12– Elementos de la Seguridad

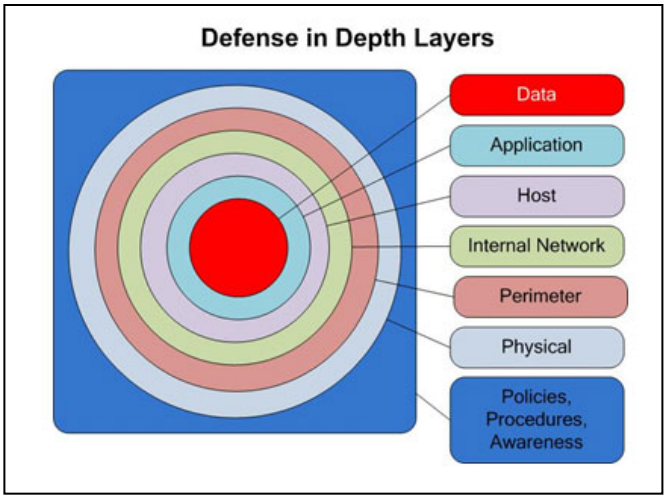
a) **Personas:** Involucra los aspectos relacionados al establecimiento de políticas y procedimientos para la definición de reglas y responsabilidades; la realización de entrenamientos para la creación de una mentalidad de seguridad tanto del personal técnico cuanto de los operadores, así como medidas 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 cualidad, así como la adopción de los siguientes principios:

- Defensa en múltiples áreas, con foco en la defensa de la red y de la infraestructura; defensa de las bordas y defensa del ambiente computacional;

- Incluir tanto medidas de detección cuanto de protección, con infraestructuras para detectar intrusiones y para analizar y correlacionar los resultados y reaccionar en consecuencia.

- Defensa en capas: consiste en implementar varios mecanismos de defensa o controles entre el enemigo y su objetivo. Cada uno de estos mecanismos debe presentar obstáculos únicos. La figura a seguir 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:

- Manutención de la política de seguridad;
- Gestión de la actitud de seguridad;
- Evaluaciones de seguridad;
- Monitoreo;
- Detección, alarme 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: personas, consideradas en el contexto de la gestión; 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 avalia los controles de seguridad en sus sistemas y autoriza la operación.

4.3.2.2 **Planeamiento:** garantiza la administración de la Organización desarrolla y implementa un plan de seguridad.

4.3.2.3 **Gestión de Riesgos y Vulnerabilidades:** garantiza que la administración de la Organización avalia 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 conozcan las políticas de seguridad aplicables a sus áreas de actuación y están 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 aloca 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 que el control de los componentes del sistema, incluyendo hardware, software y los parámetros de adaptación 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 poseen un plan que garanta la continuidad de la operación para los usuarios y servicios más críticos y situaciones de emergencia.

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

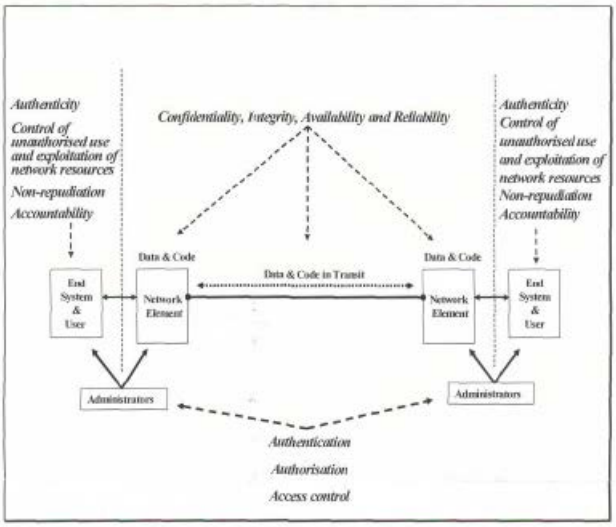
4.3.4.5 **Protección de las Instalaciones:** garantiza que los ambientes poseen acceso controlado.

4.4 **Seguridad en las Redes**

4.4.1 Considerando las capas de red interna y de borda 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 hay que 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 de adecuada de los recursos necesarios a la protección de la información, incluyendo los activos de red (enrutadores, switches, etc) y de seguridad (firewalls, IDS, IPS, etc).

e) Las equipes de mantenimiento y de operación deben estar concientizadas e entrenadas con respectos 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 ser 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 garantan la disponibilidad E integridad de las informaciones, así como el desempeño de la red según sus especificaciones.

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

- La gerencia 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 con el uso de autenticación segura.

- Los links de gerenciamiento 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) Hay que se tener un proceso de gestión de la configuración de las redes, con procedimientos para la actualización de versiones de software, de cambios de hardware y de puntos de conectividad, así como para la guarda de copias *backup* do *softwares* de instalación;

j) Es necesario se tener procedimientos específicos para el control de acceso físico y lógico a los equipamientos y sistemas de las redes, con el uso de claves seguras, equipos de identificación de identidad como tarjetas magnéticas, biometría, etc. Los enrutadores y otros activos de rede 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 fornecimiento continuo de energía y climatización adecuada;

l) Los sistemas, aplicaciones y activos de red y seguridad deben ser configurados para ejecución solamente de los servicios realmente necesarios (*hardening*), se desactivando servicios desnecesarios a la operación como, por ejemplo, FTP, DNS, etc.;

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

n) Es necesario que se tenga una equipe de específica 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 las informaciones. En estos casos, deben ser considerados los siguientes aspectos:

- Seguridad en el *endpoint* y en el *termination point* ;
- Protección en 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 ser configurados con protección en contra software maliciosos;

- 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 rede protegida por firewalls y 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;

- Autentificación fuerte;

- 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 de periferia;

- 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.