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.**

Actividades realizadas en el Proyecto de Arquitectura de la ATN SAM

(Nota presentada por el Coordinador del Proyecto Arquitectura de la ATN SAM)

RESUMEN

Esta nota de estudio tiene por objeto presentar a los participantes la situación de los entregables previstos para el Proyecto de Arquitectura de la ATN SAM.

REFERENCIAS:

- Proyecto de Arquitectura ATN CAR/SAM (D1);
- Decimosexta Reunión del Grupo de Planificación y Ejecución CAR/SAM - GREPECAS/16 (Punta Cana, República Dominicana, del 28 Marzo al 1^0 de Abril de 2011;
- Décimo Taller/Reunión del Grupo de Implantación SAM (SAM/IG/10) Proyecto RLA/06/901 (Lima, Perú, 01-05 de Octubre de 2012);
- Estudio para la Implantación de una Nueva Red Digital Sudamericana (REDDIG);
- Especificaciones Técnicas para la REDDIG II; y
- Licitación para la Modernización de la REDDIG.

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

1. Introducción

1.1 Dentro del Programa de Infraestructura de Comunicaciones Tierra-Tierra y Aire-Tierra de la Región SAM se encuentran dos proyectos que son:

a) Arquitectura de la ATN CAR/SAM (D1); y
b) Aplicaciones tierra-tierra y tierra-aire de la ATN (D2).

1.2 Se resalta que al principio el Proyecto de Arquitectura de la ATN SAM se cerraba con la elección de la plataforma óptima basada en IP para las Regiones SAM. El proyecto no trataba de la implantación de la nueva red (REDDIG II) que remplazará la estructura actual.

1.3 En base a lo descrito en el párrafo anterior, el Coordinador de Programa y el del Proyecto D1 hicieron una revisión de todos los entregables involucrados y llegaron a la conclusión de que se debería extender el proyecto para incluir las tareas de monitoreo de la implantación de la REDDIG II, estimada a implantarse inicialmente para el primer trimestre del 2015.

1.4 Al respecto, en esta nota de estudio se describe, todos los documentos involucrados, los cambios y ajustes en los documentos originales para el Proyecto de la Infraestructura SAM (D1) y las actividades que fueron desarrolladas a la fecha.

2. **Análisis**

2.1 En la reunión SAM/IG/7, han sido nombrados los Coordinadores de Proyecto para la Región SAM. Para el Proyecto de Arquitectura SAM fue elegido el Sr. Athayde Licério Vieira Frauche (Brasil), experto que ya estaba trabajando en las tareas para las Regiones CAR/SAM.

2.2 Con eso, fueron hechas adaptaciones en todos los documentos originales para contemplar tareas que involucran solamente la Región SAM, conforme se describe en el cuerpo de esta nota de estudio.

2.3 **Documentos del Proyecto**

2.3.1 Los documentos que componen el Proyecto de Arquitectura de la ATN SAM son:

a) Programa de Trabajo;
b) Descripción del Proyecto (DP);
c) Archivo en Project; y
d) Estructura Detallada de Trabajo (EDT).

2.3.2 A los entregables originales asignados al Proyecto de Arquitectura de la ATN SAM, se agregó el monitoreo para la implantación de la REDDIG II, que está descrito en el entregable D, 1.8. La Tabla del **Apéndice A** contiene el Programa de Trabajo actual**.**

2.3.3 Como resultado de todo el análisis hecho para el proyecto se presentan, en el documento de Descripción de Proyecto, reflejado en el **Apéndice B,** los entregables del Proyecto de Arquitectura de la ATN SAM. Adicionalmente, el documento contiene un resumen de todas las principales fases del proyecto, desde su creación hasta el cierre de todas las actividades. La fecha para la implantación de la REDDIG II fue actualizada para Marzo de 2015, teniéndose en cuenta los retrasos para la firma del contrato con la empresa vencedora del proceso licitatorio.

2.4 **Avance de las Actividades**

2.4.1 El Quinto Taller del Grupo de Implantación de la Región SAM (SAM/IG/5) consideró llevar a cabo estudios sobre la implantación de una nueva red digital regional satelital, terrestre o mixta (satelital y terrestre), que oficie de *backbone* de la Red de Telecomunicaciones Aeronáuticas de la Región SAM (ATN SAM), la que deberá soportar los actuales requerimientos fijos aeronáuticos de voz y datos, el intercambio de datos radar y planes de vuelo, así como las nuevas aplicaciones ATN tierra – tierra entre los Estados / Territorios de la Región SAM, previstas a implantarse, a corto y mediano plazo.

2.4.2 Los estudios para la elección de la estructura medular *(backbone)* IP de la Región SAM fueron finalizados y presentados para evaluación de los Estados de la Región en la Reunión SAM/IG/6.

2.4.3 La evolución natural de todo lo que se presenta en los entregables fue contemplado en agosto de 2011 con la elaboración de las especificaciones técnicas para la modernización de la REDDIG.

2.4.4 Se enfatiza que los documentos de especificaciones elaborados fueron presentados y aprobados en la Duodécima Reunión de Autoridades de Aviación Civil, que sucedió en la Oficina Regional de la OACI de Lima – Perú, del 03 al 06 de Octubre de 2012.

2.4.5 La REDDIG II será formada por los “backbone” satelital (principal) y terrestre que deberán trabajar en paralelo para aumentar la disponibilidad y la flexibilidad para la carga de nuevas aplicaciones en la red. La Figura 1, muestra la futura arquitectura de la REDDIG II.

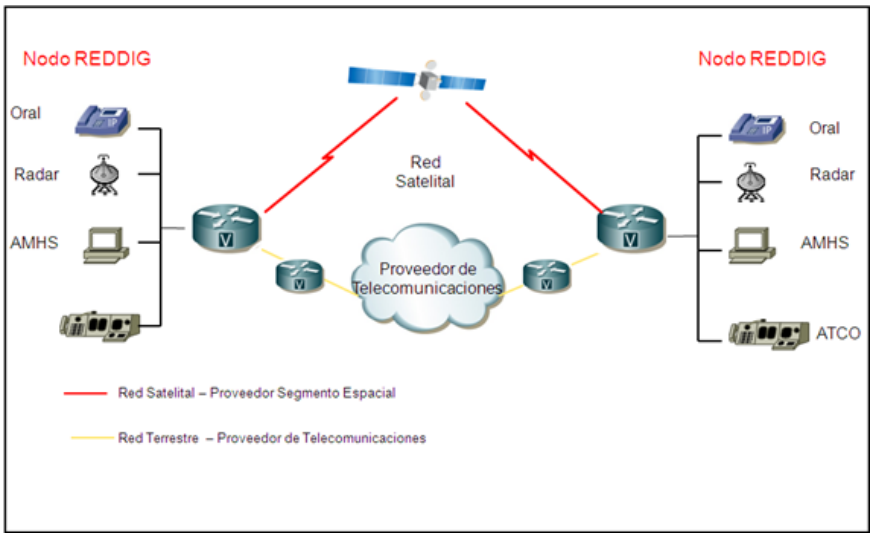


Figura 1: Arquitectura de la REDDIG II

2.4.6 Con el apoyo del Proyecto de Cooperación Técnica RLA/03/901, fueron contratados dos expertos, por un periodo de una semana cada uno, para el desarrollo de la Guía de Seguridad y para la Política de Enrutamiento para la Región SAM, lo que se presenta, respectivamente, en los **Apéndices C** y **D**.

2.4.7 Como consecuencia, se llega a la conclusión de que solamente queda faltando la tarea de acompañamiento de las actividades para la implantación de la REDDIG II, que depende, principalmente, de la firma del contrato por parte del TCB de la OACI, en nombre de los Estados miembros de la REDDIG con la empresa INEO, vencedora del proceso licitatorio. A ese respecto, la Secretaría está presentando una nota de estudio con todos los detalles de la evolución del proceso para la implantación de la REDDIG II.

3. Acción sugerida

3.1 Se invita a la Reunión a:

a) tomar nota de la información presentada;
b) revisar las actividades del Proyecto de la Infraestructura ATN SAM, descrito en la sección 2 de esta nota de estudio, incluyendo los apéndices A ,B,C,D, en base a los ajustes hechos en los documentos originales del Proyecto D1 SAM en lo que concierne la implantación de la REDDIG II; y
c) analizar los avances de los entregables de las actividades del proyecto D1.

- - - - - -

APPENDIX A / APENDICE A

PROJECT WORK PROGRAMME / PROGRAMA DE TRABAJO DEL PROYECTO

PROGRAMME/PROGRAMA: GROUND-GROUND AND AIR-GROUND TELECOMMUNICATIONS INFRASTRUCTURE/ INFRAESTUCTURA DE COMUNICACIONES TIERRA-TIERRA Y TIERRA-AIRE

PROJECT/PROYECTO: D1. CAR/SAM ATN ARCHITECTURE / ARQUITECTURA DE LA ATN CAR/SAM

PROJECT COORDINATOR/ COORDINADOR DEL PROYECTO: Athayde Frauche

No.	Tarea/Task	Inicio Fin / Start End	Responsable / Responsible	Estado/Status	Deliverable/Entregable
1	2	3	4	5	6
D 1.1	Guide the interconnection/integration of Communications digital networks Guiar la interconexión/ integración de redes digitales de comunicaciones	Mar-Dec 2010 / Mar-Dic 2010	ICAO REDDIG Administration MEVA TMG Group OACI Administración REDDIG Grupo MEVA TMG	Valid/Válida	Evaluation of the performance of the interconnection of MEVA II/REDDIG Evaluación del desempeño de la interconexión MEVA II/REDDIG
D 1.2	Technical revision of Regional Telecommunication Network for ATN implementation Revisión técnica de redes regionales de telecomunicaciones para la implantación de la ATN	Jun 2009- Jul 2011	ICAO REDDIG Administration OACI Administración REDDIG	Valid/Válida	Technical study of MEVA II and REDDIG networks for ATN implementation Estudio técnico de las redes MEVA II y REDDIG para la implementación de la ATN
D 1.3	Trial implementation to determine ATN bandwidth to support ground application Implantación de pruebas para determinar el ancho de banda de la ATN para soportar las aplicaciones terrestre	2009-Sep 2010	SAM Project / Proyecto SAM	Valid/Válida	Evaluation of the preliminary trials results on the definition of the CAR/SAM ATN bandwidth requirement Evaluación de los resultados de las pruebas preliminares para determinar ancho banda requerido para la red ATN en las Regiones CAR y SAM
D 1.4	Study for an IP ATN CAR/SAM backbone network configuration Estudio para la configuración de una red medular IP para las Regiones CAR/SAM	2009-Dec 2011 / 2009-Dic 2011	SAM Project / Proyecto SAM	Valid/Válida	Study for the configuration of an IP backbone network Estudio para la configuración de una red medular IP

No.	Tarea/Task	Inicio Fin / Start End	Responsable / Responsible	Estado/Status	Deliverable/Entregable
1	2	3	4	5	6
D 1.5	Update of CAR/SAM Router Plan Actualización del plan regional CAR/SAM de encaminadores	Jan 2012 / Ene 2012	ICAO/OACI	Valid/Válida	Update to CAR/SAM Regional Plan on ATN Routers Actualización al Plan regional CAR/SAM de encaminadores del ATN
D 1.6	Analyze proposals for data Communications infrastructure in support of ATFM implementation This activity supports the activity *Support PBN and ATFM implementation, optimization of ATM routes and guidance for ATM service automation* covered in the communication area. Analizar las propuestas de infraestructura de comunicaciones de datos en apoyo de la implantación de la ATFM Esta actividad apoya la actividad *Soporte a la implantación del PBN el ATFM, optimización de las rutas ATM y guías para el servicio de automatización ATM* cubierta en el área de comunicaciones.	2009 - Dec 2011 / 2009 - Dic 2011	SAM Project / Proyecto SAM **Note**: Coordination needed with Programmes A (PBN), B (ATFM) and C (Situational Awareness) **Nota**: Coordinación requerida con Programas A (PBN), B (ATFM) y C (Comprensión Situacional)	Valid/Válida	Study of communication requirements to support ATFM implantation Estudio de requerimientos de las comunicaciones para soportar la implantación de la ATFM
D 1.7	Elaborate a CAR/SAM plan for the establishment of the communications system needed for the migration towards aeronautical MET messages exchange (METAR/SPECI and TAF) in the new format to be defined Elaborar un plan CAR/SAM para establecer el sistema de comunicaciones necesario para la migración hacia el intercambio de mensajes aeronáuticos MET (METAR/SPECI y TAF) en el nuevo formato a definirse	Jun 2011- Jun 2012	ICAO/OACI **Note**: Coordination needed with AERMET/SG **Nota**: Coordinación requerida con AERMET/SG	Valid/Válida	Study of communication requirement to support the migration to new OPMET format Estudio de requerimientos de comunicaciones para soportar la migración al nuevo formato OPMET
D 1.8	Install the new REDDIG network, called REDDIG II Instalar la nueva red REDDIG, llamada REDDIG II	Nov 2013 – Mar 2015	ICAO/OACI	Valid/Válida	Accompany the bid and the installatioin of REDDIG II Acompañar la licitación y la instalación de la REDDIG II

- - - - - - - - -

APENDICE B

PROYECTO ARQUITECTURA DE LA ATN EN LA REGION SAM

Región SAM	**DESCRIPCION DEL PROYECTO (DP)**	**DP N° D1**	
Programa	**Título del Proyecto**	**Fecha Inicio**	**Fecha Término**
Infraestructura de Comunicaciones Tierra-Tierra / Aire-Tierra (*Coordinador del Programa: Onofrio Smarrelli)*	Arquitectura de la ATN en la Región SAM *Coordinador del Proyecto: Athayde Licério Vieira Frauche (Brasil)* *Expertos contribuyentes al proyecto: Omar Gouarnalusse (Argentina), Michel Areno (Francia), Jose Luis Paredes (Peru), Jesús Bolívar (Venezuela), Hernando Lara (Bolivia) y Cristian Amaris De León (Colombia)*	Marzo 2010	Marzo 2015
Objetivo	Estudio e implantación de arquitectura óptima para una red medular basada en el protocolo IP (REDDIG II) para la Región SAM		
Alcance	Estudio e implantación de una red medular IP para la Región SAM, que incluya una configuración óptima y contemple, entre otros entregables, lo siguiente: • Revisión técnica de las redes regionales de telecomunicaciones (terrestres, satelitales o mixtas) para la implantación de la ATN bajo un análisis de costo-beneficio • Implantación de pruebas para determinar el ancho de banda de la ATN para soportar las aplicaciones terrestres • Esquema de direccionamiento IP (IPv4 e IPv6) y análisis de la infraestructura de comunicaciones de datos en apoyo a los requerimientos operacionales ATS a corto, mediano y largo plazo • Soporte al proceso licitatorio, por parte de TCB (Montreal) y de la implantación de la red medular IP para la Región SAM • Implantación de la REDDIG II		
Métricas	• Porcentaje concluido del estudio de una red medular IP para la Región SAM • Elaboración de las especificaciones técnicas para la REDDIG II • Porcentaje de la implantación de la REDDIG II		
Estrategia	• Todos los trabajos serán ejecutados por expertos nominados por los Estados de la Región SAM miembros del proyecto *Arquitectura de la ATN en la Región SAM*, bajo la gestión del coordinador del proyecto, en coordinación con el coordinador del programa. Las comunicaciones entre miembros del proyecto, así como entre el coordinador del proyecto y el coordinador del programa, deberán efectuarse por medio de teleconferencias y de la Internet. Asimismo, el coordinador del programa, junto con el coordinador del proyecto y los expertos contribuyentes, podrán reunirse en las reuniones de implantación SAM/IG • Una vez completado el estudio e implantada la REDDIG II, los resultados serán remitidos al coordinador del programa de la OACI en forma de documento final de consolidación para su análisis, revisión y aprobación al CRPP del GREPECAS		

Metas	•
Justificación	• Un estudio sobre una red medular ATN IP para la Región SAM permitirá definir la estructura óptima de la arquitectura de la red de comunicaciones en dicha región, que actualmente está basada principalmente en la REDDIG (red de telecomunicación digital por satélite). • Para llegar a la conclusión de la mejor infraestructura de red, se considera muy importante que se determine la demanda de las aplicaciones actuales en términos de ancho de banda. A este respecto, los Estados ya están realizando pruebas, principalmente de AMHS, para la determinación del segmento espacial asociado. La acción es considerada como el inicio de toda la investigación de la relación costo-beneficio de las redes. • Adicionalmente, los requerimientos crecientes de ancho de banda para nuevos servicios tales como automatización, vigilancia, ATFM y meteorología. Asimismo, es necesaria una estrecha relación con otros programas y sus respectivos proyectos con el fin de recolectar los requisitos operacionales demandados por las aplicaciones mencionadas y sus respectivas fechas tentativas de implantación. • Después de elaborar todas las tareas necesarias para la determinación de la mejor infraestructura de red, serán elaboradas especificaciones técnicas para la adquisición e implantación de la red medular SAM (REDDIG II) • Este proyecto se cierra una vez implantada la red medular IP SAM (REDDIG II) • Este proyecto contribuye a la implantación de los PFF SAM CNS 01, CNS04, ATM 05, ATM 06, MET 04 y AIM 02 del *Plan de Implantación del Sistema de Navegación Basado en el Rendimiento para la Región SAM (SAM PBIP)*
Proyectos Relacionados	• Sistemas de Navegación Aérea en Apoyo a la PBN • Automatización • Mejora de la Comprensión Situacional ATM • Implementación del Nuevo Formato de Plan de Vuelo de la OACI • Aplicaciones Tierra-Tierra y Aire-Tierra de la ATN

Entregables del Proyecto	Relación con el Plan Regional basado en el Rendimiento (PFF)	Responsable	Estado de Implantación[1]	Fecha Entrega	Comentarios
Análisis de la situación actual de la red de comunicaciones SAM (REDDIG)	PFF SAM CNS01	Administración de la REDDIG, Coordinador Proyecto y Omar Gouarnalusse (Argentina)		Agosto 2010	Finalizada
Análisis de la situación actual de la interconexión MEVA II/ REDDIG	PFF SAM CNS01	Administración REDDIG		Junio 2011	Finalizada
Análisis del impacto del ancho de banda de AMHS en la infraestructura actual satelital REDDIG	PFF SAM CNS01	Coordinador Proyecto y Omar Gouarnalusse (Argentina)		Septiembre 2010	Finalizada
Requerimientos de aplicaciones a lo largo del tiempo en la Región SAM	PFF SAM CNS01 PFF SAM CNS 04 PFF SAM MET 04 PFFs SAM ATM 05 y 06 PFF SAM AIM 02	OACI		Septiembre 2010	Finalizada

[1] ***Gris*** *- Tarea no iniciada*
Verde *- Actividad en progreso de acuerdo con el cronograma*
Amarillo *- Actividad iniciada con cierto retardo, pero estaría llegando a tiempo en su implantación*
Rojo *- No se ha logrado la implantación de la actividad en el lapso de tiempo estimado y se requieren adoptar medidas mitigatorias*

Entregables del Proyecto	Relación con el Plan Regional basado en el Rendimiento (PFF)	Responsable	Estado de Implantación[1]	Fecha Entrega	Comentarios
Estudio comparativo de los modelos de red satelital, terrestre y mixta (satelital y terrestre) basados en IP para la Región SAM	PFF SAM CNS 01	Coordinador Proyecto, Omar Gouarnalusse (Argentina) y Administración de la REDDIG		Octubre 2010	Finalizada Aprobado por los Estados miembros de la REDDIG
Definición del modelo de infraestructura de red ATN IP para la Región SAM	PFF SAM CNS 01	Coordinador Proyecto, Omar Gouarnalusse (Argentina) y Administración de la REDDIG		Octubre 2010	Finalizada Aprobado por los Estados miembros de la REDDIG
Completar el plan de direccionamiento IPv4 para la Región SAM	PFF SAM CNS 01	Coordinador Proyecto y Omar Gouarnalusse (Argentina)		Agosto 2010	Finalizada El esquema de direccionamiento fue aprobado a través de la Conclusión GREPECAS 16/37
Elaborar las especificaciones técnicas para la REDDIG II	PFF SAM CNS01 PFF SAM CNS 04 PFF SAM MET 04 PFFs SAM ATM 05 y 06 PFF SAM AIM 02	Coordinador Proyecto, Omar Gouarnalusse (Argentina) y Administración de la REDDIG		Agosto 2011	Finalizada y aprobada por los Estados miembros de la REDDIG
Elaborar guía de seguridad para la REDDIG	PFF SAM CNS 01	Administración REDDIG		Mayo 2012	Finalizada para presentación en la reunión SAM/IG/11
Elaborar el documento IP Routing Policy	PFF SAM CNS 01	Coordinador Proyecto		Octubre 2013	Finalizada para presentación en la reunión SAM/IG/11

Entregables del Proyecto	Relación con el Plan Regional basado en el Rendimiento (PFF)	Responsable	Estado de Implantación[1]	Fecha Entrega	Comentarios
Soporte en el proceso de licitación y de la evaluación de las ofertas		Coordinador del Proyecto, Omar Gouarnalusse (Argentina), Michel Areno (Francia), José Luis Paredes (Peru), Jesús Bolívar (Venezuela), Hernando Lara (Bolivia), Christian Amaris (Colombia) y Administración de la REDDIG		Abril 2012	Finalizada. La licitación fue efectuada por TCB bajo la coordinación de la Oficina Regional de la OACI. El proceso de evaluación contará con la Administración de la REDDIG y con expertos CNS seleccionados por los Estados miembros de la REDDIG
Soportar la implantación de la REDDIG II		Administración de la REDDIG Coordinador Proyecto y Omar Gouarnalusse (Argentina) Puntos focales REDDIG II		Noviembre 2013-Marzo 2015	Esta actividad está prevista iniciarse a finales del 2013
Monitorear las actividades del proyecto de arquitectura de la ATN en la Región SAM		OACI		Marzo 2010-Marzo 2015	
Recursos necesarios	Contribución económica necesaria para la implantación de la REDDIG II				

APENDICE C

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.

BORRADOR

Abril 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 Decimo 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 (Organos 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 del 1 al 5 de octubre) 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.(13 al 17 de mayo de 2013) .A este respecto la Sexta Reunión del Comité de Coordinación del Proyecto RLA/06/901 (Lima Perú xxxx) 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 :

Capitulo 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 ceuales 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.

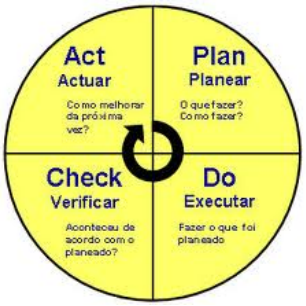


Fig. 1 – El Ciclo PDCA

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:

- La protección de los datos y la privacidad de las informaciones personales;
- La protección de registros organizacionales; y
- Derechos de propiedad intelectual

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

- El documento conteniente la política de seguridad de la información;
- La atribución de responsabilidades;
- La educación, concientización y entrenamiento en seguridad da información;
- El procesamiento correcto en las aplicaciones;
- La gestión de las vulnerabilidades técnicas;
- La gestión de la continuidad del negocio; y
- 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 continuacion algunos conceptos básicos, basados en las Normas ISO/IEC 27000:2007.

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

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

- **Probabilidad del Riesgo:** Se caracteriza pela posibilidad de una amenaza explorar alguna vulnerabilidad y comprometer uno o más principios de la seguridad.

- **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.

- **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.

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

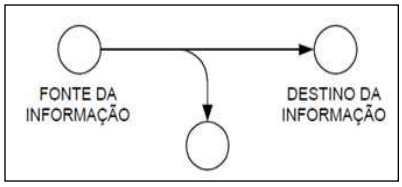
- **Incidente:** una o más serie de eventos de seguridad de la información no deseados o no esperados, que tengan una gran probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **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:

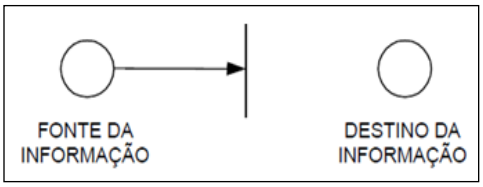
- **Confidencialidad:** capacidad de un sistema de impedir que usuarios no autorizados tengan acceso a determinada información que fue delegada a solamente usuarios autorizados. La pérdida de la confidencialidad puede ser obtenida por medio de la interceptación. La figura siguiente ilustra dicha situación:



Fuente: SANTOS (2011)

Fig. 2– Pérdida de la Confidencialidad

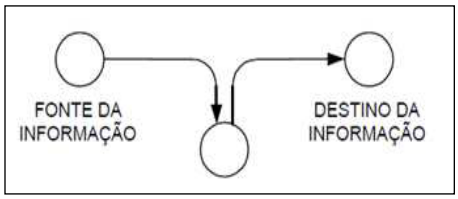
- **Disponibilidad:** indica la cantidad de veces que el sistema cumplió una tarea solicitada sin fallas internas, para un número de veces en que fue solicitado a hacer la tarea. La pérdida de la disponibilidad pode ocurrir por media de una interrupción.



Fuente: SANTOS (2011)

Fig. 3 – Pérdida de la Disponibilidad

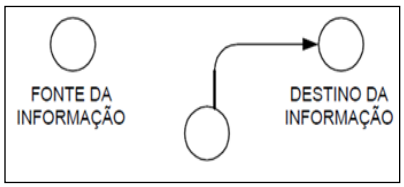
- **Integridad:** atributo de seguridad que indica si una información puede ser alterada solamente de forma autorizada. La pérdida de la integridad puede ocurrir por modificación.



Fuente: SANTOS (2011)

Fig. 4 – Pérdida de la Integridad

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



Fuente: SANTOS (2011)

Fig. 5 – Pérdida de la Autenticidad

- **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:

- **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.

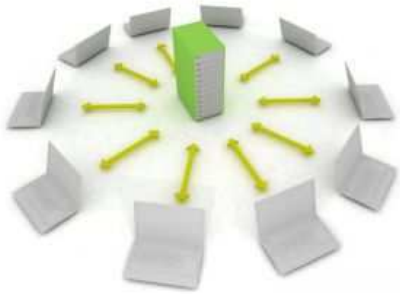


Fig 6 – La automatización multiplica el poder del atacante

- **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.

- **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.

- **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:

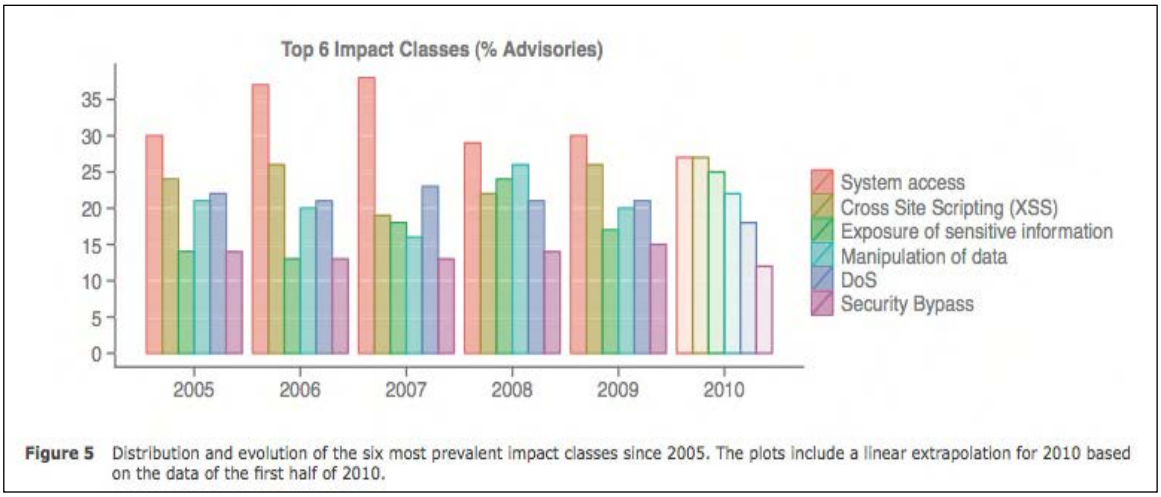


Figure 5 Distribution and evolution of the six most prevalent impact classes since 2005. The plots include a linear extrapolation for 2010 based on the data of the first half of 2010.

Fuente: Secunia - Half Year Report, 2010.

2.5.3 Las vulnerabilidades pueden ser clasificadas en los siguientes tipos:

- Física: son aquellas asociadas a las instalaciones, como controle de acceso, energía, climatización, incendios, inundación, etc.
- Hardware y Software: están relacionadas a fallas en los equipamientos y en las aplicaciones.
- Comunicación: involucran las fragilidades relacionadas a los sistemas de comunicación de datos; y
- 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:

- Acceso no autorizado a la red;
- Exposición de información confidencial;
- Daño o distorsión de la información;
- Proveer de datos para el hurto o secuestro de identidad;
- Exponer secretos organizacionales;
- Desencadenar fraudes;
- Paralizar las operaciones del negocio; y

- 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*.

- Datos: ataques a los datos afectan los siguientes principios de seguridad: confidencialidad, integridad, autenticidad y no repudio;
- Redes: ataques a las redes afectan los siguientes principios de seguridad: disponibilidad, confidencialidad y integridad;
- *Hardware*: ataques al hardware afectan principalmente el principio da disponibilidad; y
- *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:

- Búsqueda por vulnerabilidades; y
- 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.

1. 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 las mensajes tramitadas 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 e 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:

- Tipo y versión de sistema operativo;
- Fabricante de la interfaz de red;
- Dirección de red (IP) o de enlace (MAC);
- Puertas de comunicación abiertas;
- Versiones de software; y
- *Passwords defaults* en los activos de red y de seguridad.

2. *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 esta 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:

- Accesos satelitales y terrestres;
- Topología mallada, flexible, multiprotocolo, multiservicio y de área externa;
- Ser escalable y de fácil expansión;
- Redundancia y encaminamientos satelitales y terrestres;
- Ser de arquitectura abierta, basada en protocolo IP;
- 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:

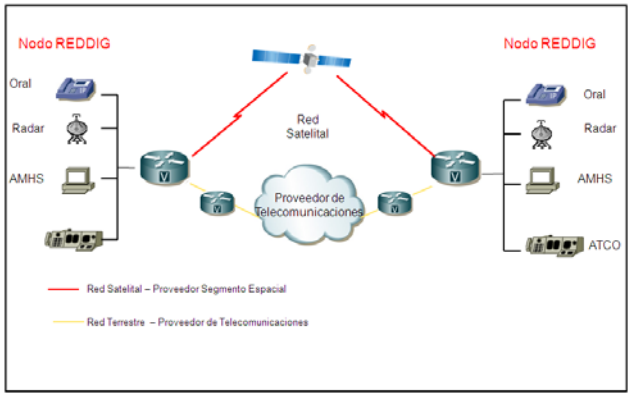


Fig 8 – La REDDIG II – Topología

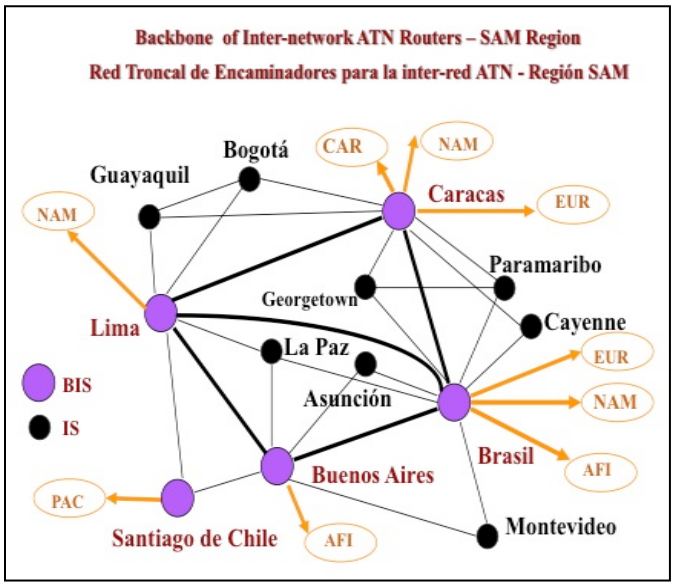


Fig 9 – La REDDIG II – Puntos de Interconexión

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:

a. 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:

- Tabla CNS1A (Plan AFTN); y

- Tabla CNS1C (Plan de circuitos orales directos ATS).

b. Servicios futuros:

- Los que surgieron de la interconexión MEVA II – REDDIG;
- 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;
- 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;
- Los requerimientos de interconexión AMHS, reemplazando progresivamente el servicio AFTN, de acuerdo a los respectivos MoU (Memorandos de Entendimientos) suscriptos o a subscribirse;
- Los requerimientos de interconexión AIDC, reemplazando progresivamente el servicio Oral ATS;
- El Intercambio de datos ADS-B y multilateración, entre todos los ACCs de FIRs colindantes;
- La Interconexión de sistemas automatizados utilizando Asterix 62 y 63, entre todos los ACCs de FIRs colindantes.
- 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:

- La cantidad mínima necesaria de memoria que atienda a todas las funcionalidades exigidas,en conformidad a las recomendaciones del fabricante.
- Protocolo de gerenciamiento SNMP y MIB-II implementados en conformidad con la RFC 1157 y con RFC 1213, respectivamente.
- Funcionalidad de Gateway para voz sobre IP que atienda a todas las funcionalidades requeridas.
- 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:

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

- 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).

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

- 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.

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

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

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

- Disponer todos los ports necesarios para satisfacer los requerimientos actuales y futuros.

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

- Establecer grupos cerrados de usuarios para tráfico telefónico y datos.

- 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.

- 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).

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

- Incluir los elementos necesarios para sincronizar la red.

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

3.3.3 Implementan los protocolos de enrutamiento:

- RIPv1 (RFC 1058).

- RIPv2 (RFCs 2453, 1723 e 1724).

- EIGRP.

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

- 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:

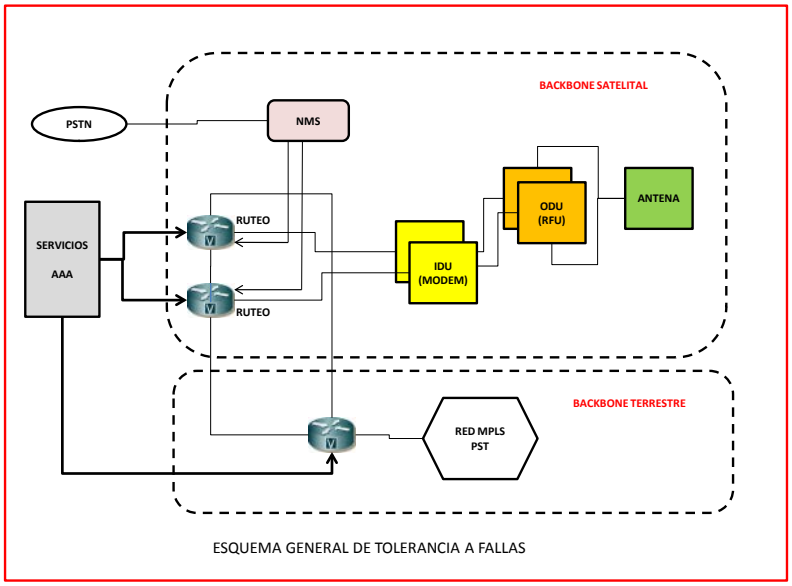


Fig 10 – Tolerancia a Fallas

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:

1. Protección de los datos de la ATN en contra acceso no autorizado, modificación o apagado;

2. 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:

- Integridad;
- Disponibilidad;
- Confidencialidad;
- Autenticidad;
- No repudio; y
- 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:

- Controles Gerenciales;
- Controles Operacionales; y
- 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:

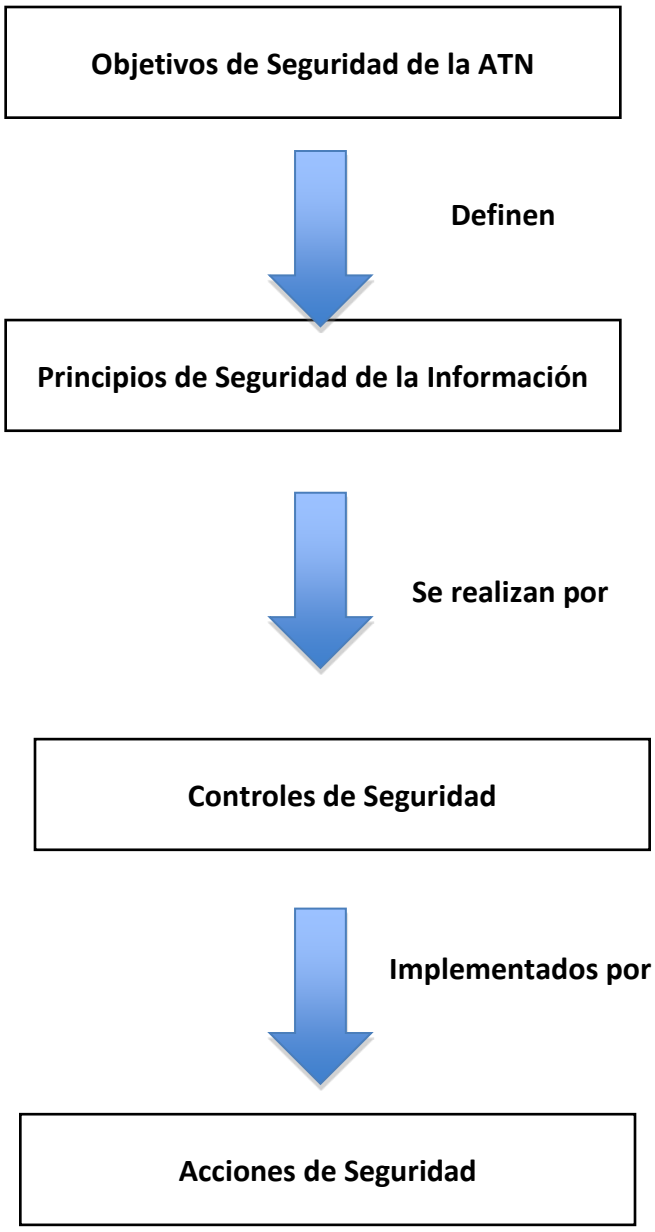


Fig 11– Objetivos de Seguridad

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:

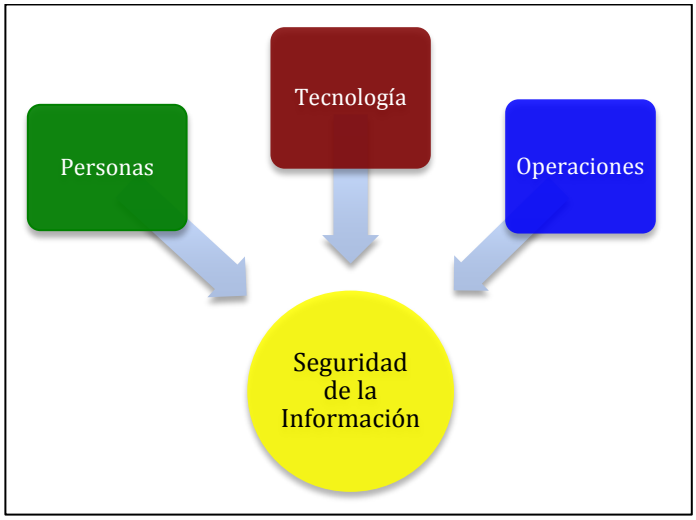


Fig 12– Elementos de la Seguridad

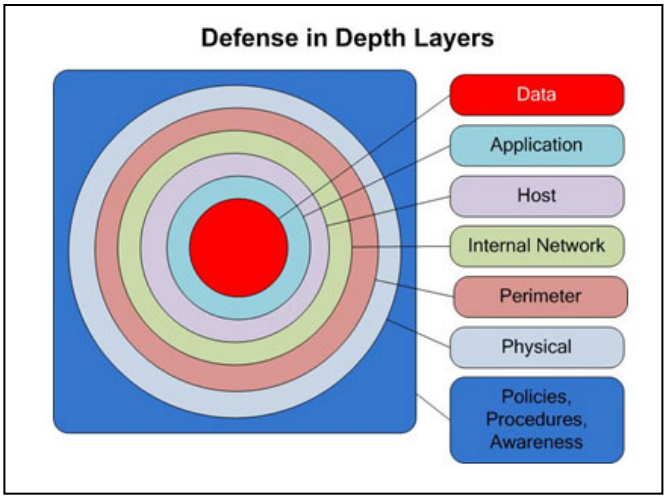
a) **Personas:** Involucra los aspectos relacionados al establecimiento de políticas y procedimientos para la definición de reglas y responsabilidades; la realización de entrenamientos para la creación de una mentalidad de seguridad tanto del personal técnico cuanto de los operadores, así como medidas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

1) Controles Gerenciales:

1.1) 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.

1.2) Planeamiento: garantiza la administración de la Organización desarrolla y implementa un plan de seguridad.

1.3) 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.

1.4) 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.

1.5) Adquisición de Sistemas y Servicios: garantiza que la administración de la Organización aloca los recursos necesarios a la adecuada protección de la información.

2) Controles Técnicos

2.1) 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.

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

2.3) Protección de las Comunicaciones: es la capacidad de monitoreo, control y protección de las comunicaciones.

3) Controles Operacionales

3.1) Gestión de la Configuración: garantiza que el control de los componentes del sistema, incluyendo hardware, software y los parámetros de adaptación del sistema.

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

3.3) 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.

3.4) Protección de Datos: garantiza la protección los datos y de las midias de almacenamiento del sistema.

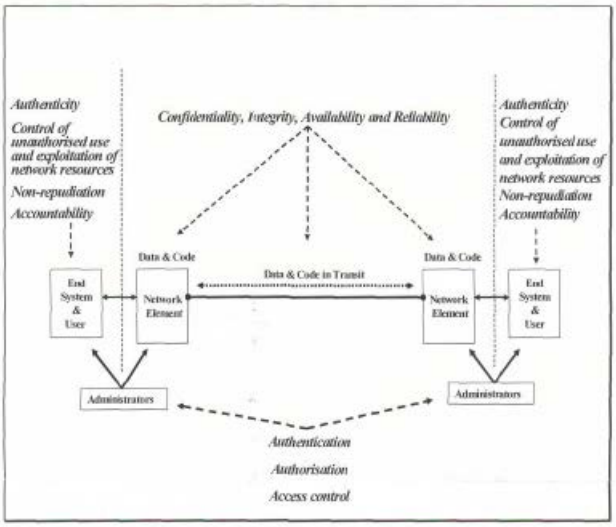
3.5) Protección de las Instalaciones: garantiza que los ambientes poseen acceso controlado.

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.

1- 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;

2- 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

3- 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

4- 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).

5- 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

6- Los equipamientos y sistemas deben poseer certificación de seguridad.

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

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

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

c) 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.

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

e) Los enrutadores deben estar constantemente actualizados, con *passwords* y *login* distintos de los de fabrica.

f) 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 y integridad de las informaciones, así como el desempeño de la red según sus especificaciones;

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

h) 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

i) Los links de gerenciamiento deben ser encriptados;

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

9- 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;

10- 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 fabrica;

11- Los equipamientos y sistemas críticos para la operación, supervisión y monitoreo de las redes deben poseer fornecimiento continuo de energía y climatización adecuada;

12- 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;

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

14- 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.

15- Es recomendable el uso de VPN para proveer comunicaciones que requieran confidencialidad y 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.

16- 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.

17- 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;
- Auditoria permanente

18- 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.

APENDICE D

RED DE TELECOMUNICACIONES AERONAUTICAS REGION SAM (REDDIG II)

POLITICA DE ENRUTAMIENTO PARA LA REGIÓN SAM

INDICE

REFERENCIAS

- Doc 9855 - Orientación sobre la Utilización de la Internet pública para Aplicaciones Aeronáuticas
- Doc 9896 – Manual para la Red de Telecomunicaciones Aeronáuticas (ATN) con el uso de los Protocolos y Estándares IPS
- Guía de Orientación para la Implementación de Redes Nacionales Digitales en Protocolo IP para Apoyar Actuales y Futuras Aplicaciones Aeronáuticas (Región SAM)
- Plan de navegación Aérea para las Regiones Caribe y Sudamérica – FASID – Tablas CNS1A y CNS1C
- Plan Regional SAM de Direccionamiento IP
- RFC 4271 –BGP-4 *Specifications*
- RFC 4360 – BGP *Extended Communities Attribute*
- Tabla CNS 1Ba – Plan Regional de Encaminadores / Región SAM.

GLOSARIO DE ACRONIMOS

- AMHS ATS *Message Handling System*
- ANSP Proveedor de Servicio de Navegación Aérea *(Air Navigation Service Provider)*
- ARIN *American Registry for Internet Numbers*
- ATN Red de Telecomunicaciones Aeronáuticas *(Aeronautical Telecommunication Network*)
- BER Tasa de Error de Bit *(Bit Error Rate)*
- BGP *Border Gateway Protocol*
- EGP *Exterior Gateway Protocol*
- ES Sistema Terminal *(End System)*
- EUR/NAT *European and North Atlantic Region*
- FASID *Facilities and Services Implementation Document*
- GREPECAS Grupo Regional de Planificación e Ejecución del Caribe y Sudamérica
- IANA *Internet Assigned Numbers Authority*
- IGP *Interior Gateway Protocol*
- IPS Conjunto de Protocolos de la Internet *(Internet Protocol Suite)*
- ISO *International Organization for Standardization*
- MPLS *Multiprotocol Label Switching*
- OSI *Open System Interconnection*
- OSPF *Open Shortest Path First*
- PBR enrutamiento basado en política *(Policy-Based Routing)*
- PST Proveedor de Servicios de Telecomunicaciones
- QoS Calidad de Servicio *(Quality of Service)*
- REDDIG Red Digital Sudamericana
- RFC *Request for Comments*
- RIP *Routing Information Protocol*
- RIR *Regional Internet Registry*
- SAM *South American Region*
- SLA *Service Level Agreement*
- SICAS *Secondary Surveillance Radar Improvements and Collision Avoidance Systems*
- SICASP SICAS *Panel* (ICAO)
- TCP *Transmision Control Protocol*
- VoIP Voz sobre IP *(Voice Over IP)*
- VPN *Virtual Private Network*
- UDP *User Datagram Protocol*
- WACAF *Western and Central African Region*
- WAN *Wide Area Network*

DEFINICIONES

Para fines de este documento, se aplican las siguientes definiciones:

Ancho de Banda: velocidad máxima de paquetes de una puerta de conexión dedicada expresa en kbit/s o Mbit/s.

Aplicaciones de la REDDIG II: servicios a ser prestados por la REDDIG II que se definen en el cuerpo del documento.

Capa Física (Nivel1): La capa física define las características técnicas de los dispositivos eléctricos y ópticos (físicos) del sistema. Ella contiene los equipamientos de cableado u otros canales de comunicación que se comunican directamente con el controlador de interfaz de red. Se ocupa, por tanto, en permitir una comunicación simple y confiable, en la mayoría de los casos con control de errores básicos:

Funciones de la Capa:

- Mueve bits (o bytes, conforme a la unidad de transmisión) a través de un medio de transmisión;
- Define las características eléctricas y mecánicas del medio, la tasa de transferencia de los bits, tensiones, etc.
- Ejecuta o controla la cantidad y velocidad de transmisión de las informaciones de la red.

No es función del nivel físico tratar problemas como los errores de transmisión, ya que ellos son tratados por las otras capas del modelo OSI.

Capa de Red (Nivel 3): La capa de Rede responsable del direccionamiento de los paquetes en la red, también conocidos como datagrama, asociando direcciones lógicas (IP) a direcciones físicas, de forma que los paquetes de red consigan llegar correctamente a destino. Esta capa también determina la ruta que los paquetes irán a seguir para arribar a destino, basada en factores como condiciones de tráfico de red y prioridades.

La referida capa es usada cuando la red posee mas de un segmento y, por ello, habrá mas de un camino para un paquete de datos para corre del origen al destino.

Funciones de la Capa:

- Mueve paquetes a partir de su fuente original hasta su destino a través de uno o más enlaces.
- Define como los dispositivos de red se descubren unos a otros y como los paquetes son ruteados hasta su destino final.

Disponibilidad: parámetro de medición del desempeño que consiste en el porcentaje de tiempo en el cual el PP/nodo (según corresponda) está operacional, en un periodo determinado de prestación del servicio.

Enrutador: equipo dotado de capacidad de procesamiento IP, con la función de determinar las rutas a través de las cuales los paquetes deben ser encaminados.

Enrutadores Inter-Regionales: son los equipos que proveen la interconexión que enrutadores de otras regiones de la OACI. En términos prácticos son enrutadores que pertenecen al AS de un Estado y que se ligan a la Región a las regiones EUR/NAT y WACAF por medio de la red CAFSAT, a la Región CAR por la interconexión de la interconexión de las redes MEVA II y REDDIG y a la Región APAC con la contratación de Proveedores de Servicios de Telecomunicaciones (PST).

Enrutadores Intra-Regionales: para el propósito de este documento, son los enrutadores utilizados para la comunicación dentro de la Región SAM.

Enrutamiento Inter-Domínio *(Inter-domain routing):* Enrutamiento de paquetes de datos por AS con diferentes autoridades administrativas.

Enrutamiento Intra-Domínio *(Intra-domain routing):* Enrutamiento de paquetes de datos por un único AS.

Path Vector Protocol: protocolo utilizado para el cambio de informaciones de enrutamiento entre diferentes Sistemas Autónomos (AS), como se da con el BGP-4. El término *path vector* lleva en cuenta el hecho de que la información de enrutamiento del BGP-4 tiene una secuencia de números de AS, indicando el camino el camino que una determinada ruta atravesó.

Protocolo de Enrutamiento: son aquellos utilizados entre enrutadores para el intercambio de informaciones sobre la topología de la red. Permiten la actualización de la tabla de enrutamiento, que es usada pelos enrutadores para elegir el mejor camino para enviar un paquete entre los segmentos de la red.

Protocolo de Enrutamiento Interno (IGP): protocolo de enrutamiento que intercambia información dentro de un Sistema Autónomo (AS), tales como: RIP (*Routing Information Protocol*) y OSPF (*Open Shortest Path First*).

Protocolo de Enrutamiento Externo (EGP): protocolo de enrutamiento que conecta diferentes Sistemas Autónomos (AS). El BGP es un tipo de EGP.

Red de los Estados Miembros de la REDDIG II: conjunto de equipos, cables y *softwares* interconectados y pertenecientes a los representados por la Contratante.

Retardo (o latencia): parámetro de medida del desempeño del servicio, que consiste en el tiempo medio de tránsito de un paquete de 64 *bytes* entre dos PP de la Contratante.

Retardo (*delay*): en este pliego, se entiende como la característica inherente a las redes estadísticas y determinísticas que consiste en el tiempo de propagación fin-a-fin (origen-destino, end–to-end) de las aplicaciones.

Seguridad física de los datos: a efectos de esta licitación, se entiende como seguridad física la protección contra el acceso no autorizado en los circuitos de comunicación y dispositivos del Adjudicatario. No forma parte del presente proceso la inclusión de criptografía en los circuitos de comunicación, por parte del Adjudicatario.

Sistema Autónomo (*Autonomous System)*: conjunto de sistemas que son administrados por una única autoridad administrativa, siguiendo una política interna establecida por la autoridad. En la Región SAM, puede ser un Estado o un Proveedor de Servicio de Navegación Aérea (ANSP). Los Sistemas Autónomo también pueden ser llamados de Dominio de Enrutamiento *(Routing Domain).*

1. INTRODUCCION

1.1 Antecedentes

1.1.1 Cuando se hace referencia a la Red de Telecomunicaciones Aeronáuticas (ATN), es necesario volver al año de 1989 cuando el Panel de Mejoras de los Radares Secundarios de Vigilancia (SICASP), encargado por el Comité Especial sobre los Futuros Sistemas de Navegación Aérea (FANS), empezó a desarrollar documentos para el intercambio de aplicaciones de voz y datos a través de variadas plataformas digitales de comunicaciones.

1.1.2 Para llevar a buen término los trabajos del SICASP, el Comité FANS recomendó la adopción de los principios de protocolos abiertos - *Open Systems Interconnection* (OSI) de la *International Organization for Standardization* (ISO) con fines de proveer la interoperabilidad entre las plataformas de red existentes.

1.1.3 Es importante enfatizar que muchas provisiones de la OACI fueron desarrolladas, en lo que concierne a las aplicaciones aire-tierra y tierra-tierra, sobre la plataforma OSI. Aunque tenga recibido apoyo considerable de los Estados miembros de la OACI para el uso de la topología OSI, sin embargo la industria impulsó los equipos basados en la plataforma *Internet Protocol Suite* (IPS).

1.1.4 En el año de 2003, fue creado el Panel de Comunicaciones Aeronáuticas (ACP) por la Comisión de Navegación Aérea (ANC) de la Organización de Aviación Civil Internacional (OACI). El ACP tiene su origen a partir de la junción del Panel de Comunicaciones Móviles Aeronáuticas (AMCP) y del Panel de Redes de Telecomunicaciones Aeronáuticas (ATNP).

1.1.5 Una de las recomendaciones principales, desde el inicio de los trabajos del panel, fue que la OACI se preocuparía en el desarrollo de documentación para la ATN en base a los protocolos TCP/IP.

1.1.6 Para efectivamente apoyar el desarrollo de las nuevas provisiones, fue creado el Grupo de Trabajo I (IP) del ACP (WG-I). Entre las funciones del WG-I están las cuestiones de seguridad, la convergencia y adaptación de las provisiones del ATN/OSI para el ATN/IP. Además de eso, trata del desarrollo de documentos para nuevas aplicaciones basadas, directamente, en el ATN/IP.

1.1.7 En términos regionales CAR/SAM, el Grupo Regional de Planificación e Ejecución del Caribe y Sudamérica (GREPECAS), por intermedio del antiguo Subgrupo CNS/ATM, ya tenía el Grupo de Tarea ATN (ATN/TF) activo para el desenvolvimiento de materiales guía a los Estados de las dos regiones con base a los protocolos TCP/IP.

1.1.8 Uno de los entregables del ATN/TF fue la elaboración de un esquema de direccionamiento basado en la versión 4 del protocolo IP (IPv4) para todos los Estados CAR/SAM, lo que está en franca implantación en dichas regiones, y que se refleja en el **Apéndice A** de este documento en lo que respeta a los Estados SAM.

1.1.9 Durante la Primera Reunión del *Working Group of the Whole* del ACP, realizada en Setiembre de 2008, el Plan CAR/SAM de direccionamiento fue presentado con la énfasis de que la intención final sería la implantación del IPv6, pero como forma de impulsar la implantación de las aplicaciones ATN en las Regiones CAR y SAM, en especial del *ATS Message Handling System* (AMHS), se haría la utilización del IPv4.

1.1.10 Se enfatiza que todas las actuales provisiones en elaboración por parte de la Oficina Central de la OACI de Montreal están calcadas en el IPv6. Sin embargo, la propia OACI está buscando formas de viabilizar la adquisición de bloques de direcciones para el uso en todas las regiones.

1.1.11 Además de eso, se resalta que los enrutadores implantados en los Estados de la Región SAM, que tengan que intercambiar datos con otras regiones, son *dual stack*, lo que representa que tienen condiciones de manejar paquetes IPv4 o IPv6.

1.1.12 Cuando la OACI logre obtener los bloques de direccionamiento IP junto a la autoridad encargada de proveer las direcciones mundialmente, que es la *Internet Assigned Numbers Authority* (IANA), y sus oficinas regionales, llamadas de *Regional Internet Registry* (RIR), se tendrá condiciones de implantar el nuevo esquema de direccionamiento IP para la Región SAM por medio de un plan de transición a ser desarrollado oportunamente.

1.2 Organización del Documento

1.2.1 La parte inicial de este documento es compuesta de las Referencias, del Glosario de Acrónimos y de las Definiciones que funcionan como un guía para todo el documento, teniéndose en cuenta la gran cantidad de informaciones presentes en el contenido de esta política. Completando esta parte, se introduce, en la Sección 1.1 de Antecedentes del Capítulo 1, un histórico de todas las actividades de la OACI para impulsar el uso del ATN/IPS en las redes de comunicaciones.

1.2.2 En el Capítulo 2, están descriptos, en líneas generales, los aspectos del Plan Regional SAM para direccionamiento IPv4, desarrollado como una transición para la futura implementación del esquema de direccionamiento IPv6.

1.2.3 Tomándose en cuenta que la estructura medular IP liga una serie de Sistemas Autónomos (AS) de Estados diferentes y otras regiones, el Capítulo 3 presenta los conceptos principales del protocolo *Border Gateway Protocol* (BGP) en su versión de utilización actual (BGP-4).

1.2.4 Por fin, el Capítulo 4 hace un abordaje de la utilización del enrutamiento BGP-4 con la aplicación a la situación específica a la Región Sudamericana y su interconexión con otras regiones de la OACI.

2. LA ATN SAM

2.1 Plan de Direccionamiento IPv4 SAM

2.1.1 Para la adopción del plan de direccionamiento IP, se hizo un estudio, por medio del ATN/TF del extinto CNS/ATM, llevando en cuenta que el IPv4 pudiera ser aplicado a todas las regiones de la OACI. Así, se analizó la cantidad de Estados/Territorios por Región, la cantidad de direcciones que cada Estado/Territorio podría utilizar y la cantidad de direcciones reservadas para la interconexión entre Estados/Territorios.

2.1.2 En primera instancia cabe destacar que a efectos de que las redes que se asignen a cada Estado / Territorio sean Redes Privadas (RFC 1918) el primero de los cuatro Bytes que componen las direcciones asignadas se mantendrá siempre con un valor decimal igual a 10. Mientras que los otros tres Bytes serán utilizados para repartir en forma jerárquica los bloques de direcciones correspondientes a cada Estado.

2.1.3 Del referido estudio se concluyó que:

a) Los primeros cuatro bits del segundo Byte (4 bits) serían utilizados para identificar las Regiones en torno de las cuales se encuentran agrupados los Estados/Territorios del mundo:
   - SAM: South American Office.
   - NACC: North American, Central American and Caribbean Office.
   - APAC: Asia and Pacific Office.
   - MID: Middle East Office.
   - WACAF: Western and Central African Office.
   - ESAF: Eastern and Southern African Office.
   - EUR/NAT: European and North Atlantic Office.

b) Se utilizaría 7 bits a nivel Estado/Territorio. Esto significa la posibilidad de tenerse 128 Estados por Región. Para dar un ejemplo real, la región EUR/NAT, que es la más numerosa, tiene 53 Estados/Territorios, o sea que hay muchos números vacantes.

c) Se reservaría los últimos cinco bits del tercer Byte y los ocho bits que componen el cuarto Byte (13 bits) para los *hosts*. Eso permite direccionar 8190 *hosts* por Estado/Territorio. Se resalta que se consideró debido requerimientos actuales y posibles aplicaciones futuras que se implementarían, principalmente en los Estados más desarrollados.

2.1.4 Teniendo en cuenta lo expresado anteriormente, el esquema adoptado tiene el siguiente formato de la Tabla 1:

Dirección IPv4																			
10								Región				Estado/Territorio							
0	0	0	0	1	0	1	0	.	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	1
1er. Byte								.	2do. Byte							.	3er. Byte								.	4to. Byte							

Tabla 1: Esquema de Direccionamiento IPv4

2.1.5 En resumen, esta forma con el esquema de asignación planteado se podrán abarcar:

a) 16 Regiones.
b) 128 Estados/Territorios por cada Región.
c) 8190 *hosts* para cada Estado/Territorio.

2.1.6 Teniendo en cuenta lo establecido anteriormente en la tabla adjunta como Apéndice A, se ha realizado la asignación de direcciones correspondientes para cada Estado/Territorio para la Región SAM. En esta tabla podrá observarse como la última red disponible ha sido marcada como "RESERVADA" a efectos de que la misma sea utilizada para los enlaces inter e intra-regionales.

2.1.7 Aunque tenga sido planeada para posible aplicación en todas las regiones, sin embargo el plan de direccionamiento IP solamente fue adoptado, y está siendo masivamente utilizado por la Región SAM mientras la OACI hace los esfuerzos para obtener bloques de direccionamiento IPv6 junto a la IANA para todas las regiones.

2.1.8 En Sudamérica, la plataforma de comunicaciones usada en la REDDIG, que liga los enrutadores de los Estados para la transmisión de aplicaciones IP ya con la adopción del plan de direccionamiento desarrollado. Las características de la REDDIG actual y los datos para la modernización de su infraestructura son presentados en el **Apéndice B**.

.

3. FUNDAMENTOS DE ENRUTAMIENTO POR DOMINIOS

3.1 El Protocolo BGP

3.1.1 El protocolo BGP, en su más reciente versión 4, es un protocolo *path vector* utilizado para el intercambio de informaciones de enrutamiento entre diferentes sistemas autónomos.

3.1.2 Los principales atributos del BGP-4 son:

a) *Origin*: informa la origen de la ruta BGP-4. Si fue generada por medio de un protocolo de enrutamiento interno (IGP), la métrica es así anunciada en la ruta BGP (el enrutador siempre elige el camino de menor métrica generada por el IGP).
b) AS-*Path*: indica por cuales AS la ruta pasó. El BGP-4 mantiene en su banco de datos todas las alternativas de camino, pero selecciona aquel que transita por menor número de AS.
c) *Next-hope*: indica la interface del enrutador de origen donde fue anunciada la ruta BGP-4. Todos los enrutadores BGP-4 encaminarán los datos para la ruta, caso tengan conectividad con la dirección IP descripta en el atributo NEXT-HOPE.
d) *Local-preference*: el atributo tiene un significado local y sirve para que el BGP-4 seleccione el mejor camino de salida en base a los enlaces WAN disponibles.
e) *Multi-exit-discriminator:* define el camino que los enrutadores vecinos BGP-4 enviarán los paquetes destinado a sus redes internas.

3.1.3 Diferentemente de otros protocolos internos de enrutamiento que utilizan *User Datagram Protocol* (UDP), BGP-4 utiliza el *Transmision Control Protocol* (TCP) como su protocolo de transporte, lo que representa que el circuito es orientado a la conexión y tiene garantía de entrega de los paquetes de forma confiable. Con eso, el BGP-4 no tiene que implementar mecanismos de retransmisión ya que eso es suministrado por el TCP.

3.1.4 Para que el BGP-4 establezca una adyacencia que los enrutadores, es necesario que se configure explícitamente el vecindario. Con eso, se forma un relacionamiento entre los enrutadores configurados como vecinos que proporciona que se sepa las condiciones de cada uno por medio del intercambio de mensajes *keepalive* a intervalos regulares de tiempo.

3.1.5 Después de establecidas las adyacencias, los enrutadores envían las rutas BGP-4 en sus tablas de enrutamiento para los vecinos que lograran éxito en el establecimiento de las referidas adyacencias. Todas las rutas aprendidas de los vecinos son puestas en la base de datos de topología del BGP-4 de cada enrutador.

3.1.6 El protocolo BGP es, originalmente, usado para el enrutamiento entre AS diferentes. Sin embargo, puede ser utilizado en enrutadores pertenecientes a un mismo AS y en ese caso es llamado de IBGP. La Figura 4 trae el concepto en que los enrutadores B, C y D, del AS 65000 son considerados vecinos IBGP.

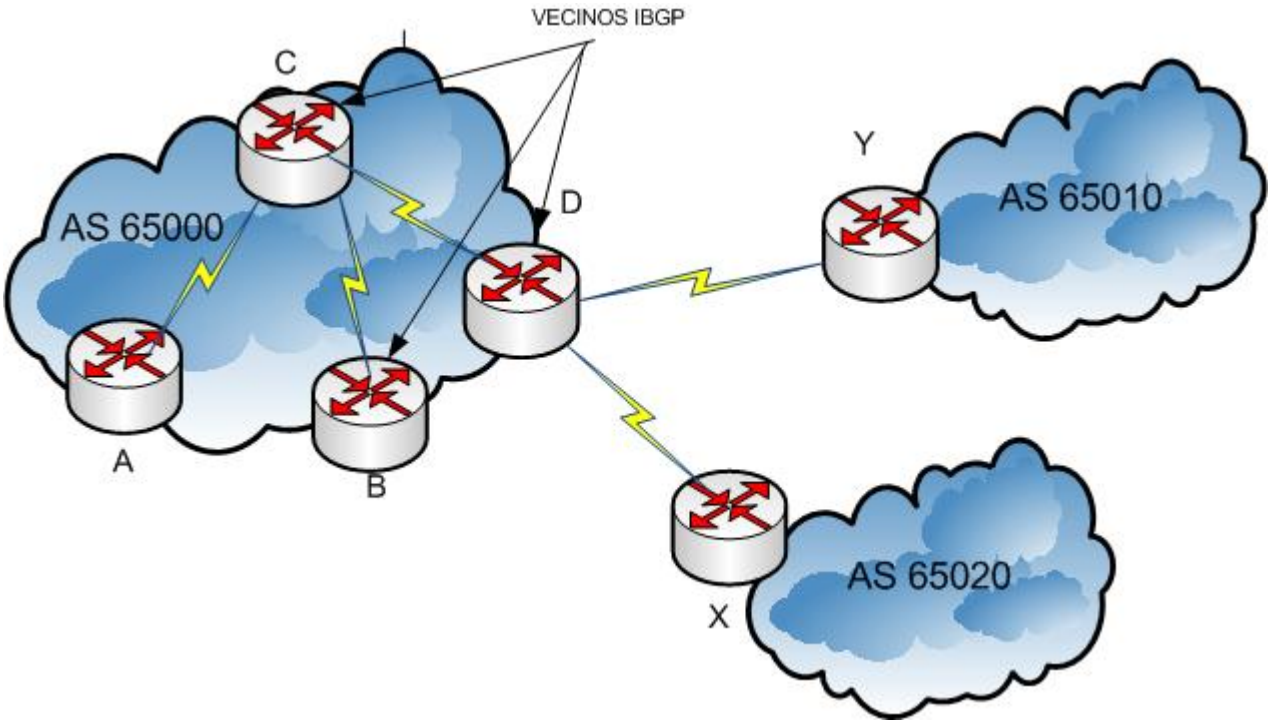


Figura 4: Enrutadores Vecinos Internos BGP

3.1.7 En la Figura 5 es mostrado el vecindario entre enrutadores que pertenecen a AS con dominios administrativos diferentes. Con eso, D y Y son vecinos externos y lo mismo sucede con los enrutadores B y X.

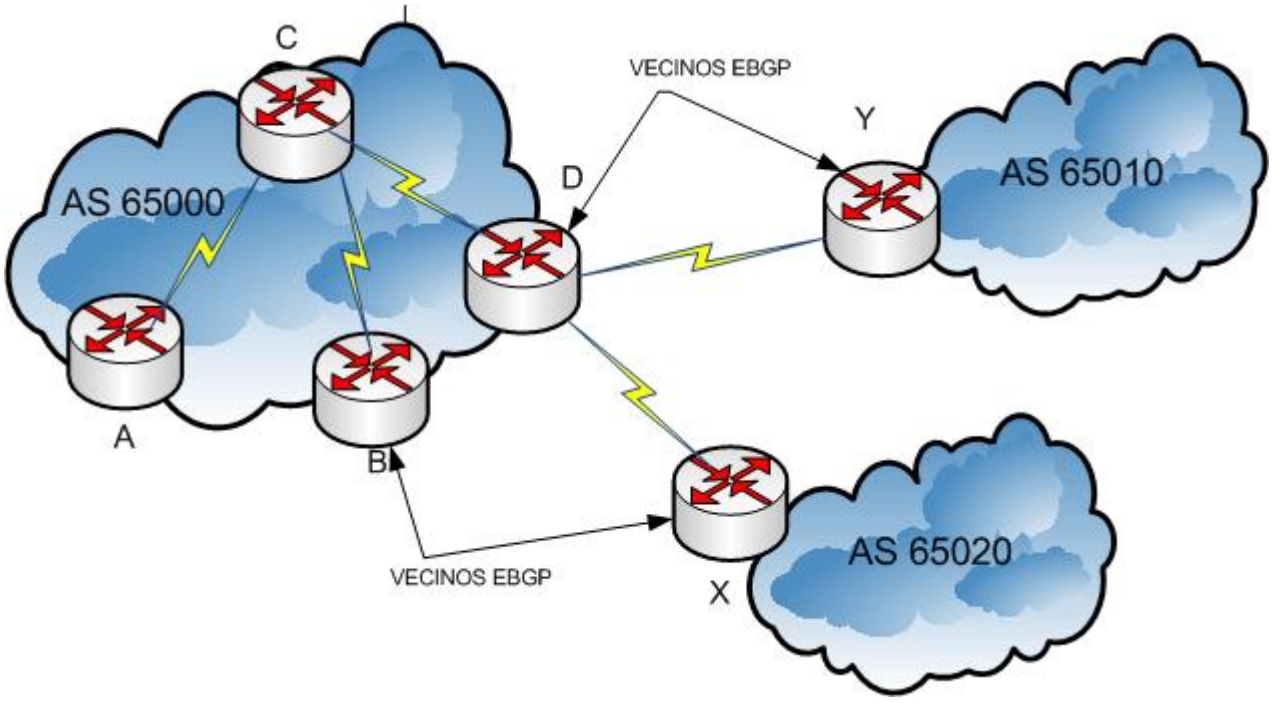


Figura 5: Enrutadores Vecinos Externos BGP

3.2 Los Sistemas Autónomos BGP

3.2.1 Como se ha definido anteriormente, un Sistema Autónomo representa una colección de redes, con sus enrutadores, bajo una única administración. Con eso, el principal objetivo del BGP-4 es garantizar el intercambio de informaciones de enrutamiento entre AS diferentes.

3.2.2 Los sistemas autónomos pueden utilizar más de un IGP y, con eso, aparece un conjunto de métricas diferentes asociadas a cada uno de los protocolos internos en el enrutador BGP-4 de salida del AS. Sin embargo, la más importante característica del AS es que para los otros enrutadores BGP-4 parece que hay solamente un IGP dentro del referido AS y los enrutadores externos sabrán, fácilmente, como alcanzar los destinos internos conectados.

3.2.3 La *Internet Assigned Numbers Authority* (IANA) es la organización encargada por alocar los números de AS. Específicamente para la región de las Américas, la *American Registry for Internet Numbers* (ARIN), que es la Oficina Regional – (RIR *Regional Internet Registry*) de IANA, es responsable por dicha tarea. Los números AS varían de 1 a 65535 y para el uso privado está reservado el rango de 64512 hasta 65535.

3.3 Enrutamiento con BGP-4

3.3.1 Un protocolo de enrutamiento interno busca el camino más rápido entre un punto de un sistema corporativo para otro, basado en métricas.

3.3.2 El BGP-4, que es un protocolo de enrutamiento externo, utiliza otro mecanismo diferente de aquel usado por los IGP. El BGP es un protocolo de enrutamiento basado en política (PBR) que permite el control de flujo de tráfico por la red con el uso de atributos definidos en 3.1 además de otros. Eso permite la manipulación de caminos preferenciales por parte de la administración de la red.

3.3.3 Así, el BGP-4 es conocido como *path vector*, pues lleva en cuenta que la información de enrutamiento del BGP-4 tiene una secuencia de números de AS, indicando el camino que una determinada ruta atravesó y los enrutadores anuncian el camino salto a salto *(hop-by-hop)* hasta el AS de destino. La Figura 6 describe un ejemplo simple del enrutamiento BGP.

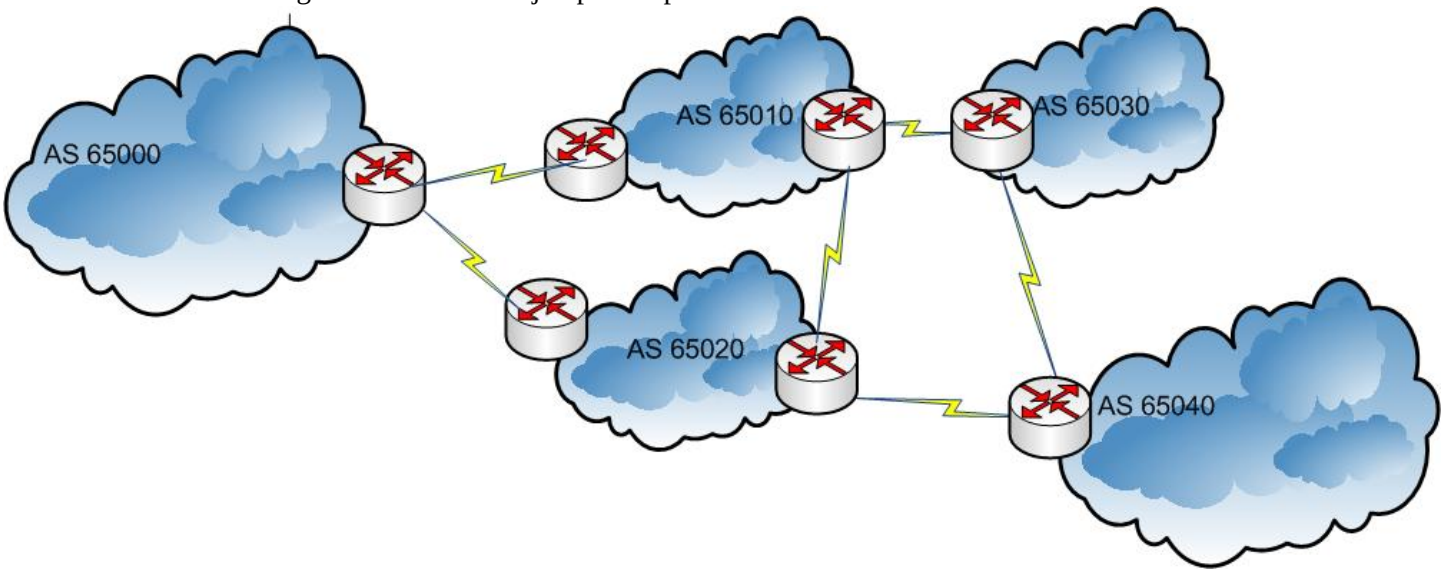


Figura 6: Enrutamiento entre AS Diferentes

3.3.4 Por la Figura 6 es posible llegarse a la conclusión de que los siguientes caminos son posibles para que el AS 65000 alcance las redes del AS 65040:

a) 65020-65040;
b) 65010-65030-65040;
c) 65010-65020-65040;
d) 65020-65010-65030-65040.

3.3.5 Los enrutadores BGP-4 de un eligen por cual camino los vecinos deben enviar sus paquetes. Con eso, el máximo que el AS 65000, que es la origen, puede hacer es decidir por cual AS quiere pasar en su salida.

3.3.6 Como ejemplo, si el enrutador de salida del AS 65000 elige el AS 65020 para llegar hacia 65040, el camino a partir del AS 65020 es decidido internamente por este AS. Así, en el ejemplo dado AS 65020 anuncia para el AS 65000 que el camino para llegar al AS 65040 es 65020-65040 aunque haya otro camino que, sin embargo, no es divulgado por AS 65020 para el AS 65000, a no ser que haya un problema en el camino principal..

4. ENRUTAMIENTOS POR DOMINIOS SAM

4.1 Dominios de Enrutamiento

4.1.1 Como forma de utilizar el protocolo de enrutamiento BGP-4, y garantizar de modo seguro el aislamiento de los sistemas autónomos, los números de AS privados, definidos en el Doc 9896 y que están descriptos en el **Apéndice E**, son recomendados para utilización en la Región SAM.

Nota: El protocolo BGP-4 permite la adopción de una serie de parámetros opcionales y de extensión. Así se recomienda que la utilización de los referidos atributos sea definida futuramente para mejor aprovechamiento de los recursos del protocolo. Sin embargo, como el BGP-4 fue desarrollado, originalmente, para la utilización del IPv4, su aplicación inicial no traerá grandes problemas.

4.1.2 Bajo un punto de vista administrativo, la red ATN/IPS de la Región SAM es un conjunto de dominios administrativos que pueden ser representados, en la Región SAM, por un Estado o por un Proveedor de Servicio de Navegación Aérea (ANSP) de un Estado.

4.1.3 En términos de los conceptos técnicos de enrutamiento, la interconexión de dominios administrativos corresponde al intercambio de informaciones entre sistemas autónomos distintos, cada uno con un conjunto de direcciones IP. El medio de interconexión de los AS en la Región SAM es conseguido por la plataforma de la REDDIG y, futuramente, de la REDDIG II.

4.1.4 El Apéndice B muestra las características básicas de la plataforma actual de la REDDIG, además de la futura (REDDIG II). La referida arquitectura soporta los servicios actuales e futuros que están o serán implantados en la Región SAM. El **Apéndice C** describe las aplicaciones que deben ser transmitidas por la referida red de comunicaciones.

4.2 Enrutamiento por Dominio en la Región SAM

4.2.1 El Apéndice A muestra la asignación de rangos de direcciones IP que serán seguidos por las Autoridades Aeronáuticas de cada Estado de la Región en los enrutadores nacionales que se ligan a la REDDIG. Representa el plan vigente de direccionamiento IP de la Región SAM.

4.2.2 Como mencionado anteriormente, que cuando la OACI, actuando en favor de los Estados, adquiera los bloques de direcciones IPv6 junto a la IANA, será necesario el preparo de un nuevo plan de direccionamiento IP SAM. Además de eso, los enrutadores utilizados en la Región SAM son *dual stack* en lo que concierne a la posibilidad de encaminar paquetes inter-regionales en que el destino ya esté utilizando el IPv6. La Figura 7 ilustra esa posibilidad para la aplicación de AMHS.

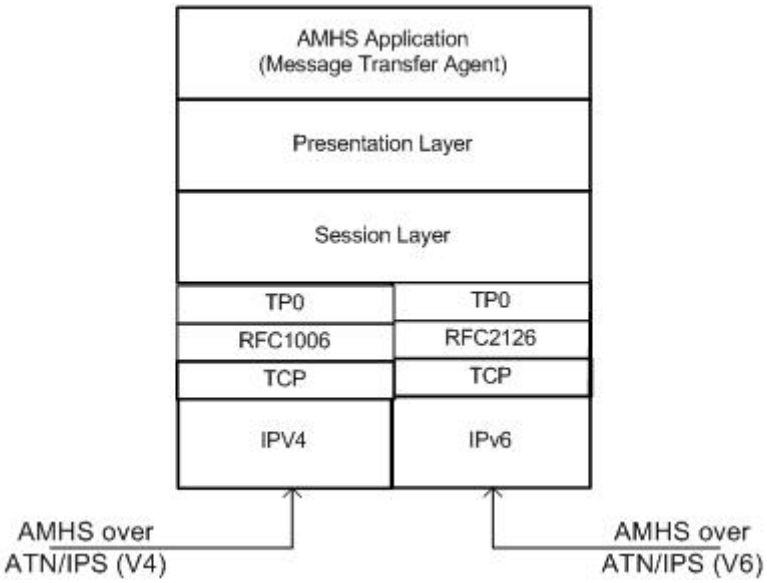


Figura 7: Traducción de Direcciones IPV4/IPv6

4.2.3 Como se sabe, la REDDIG es utilizada para ligar AS de Estados distintos de modo que un sistema terminal (ES) pueda alcanzar otro en un Estado diferente. Con eso son utilizados enrutadores intra-regionales, como se muestra en la Figura 8.

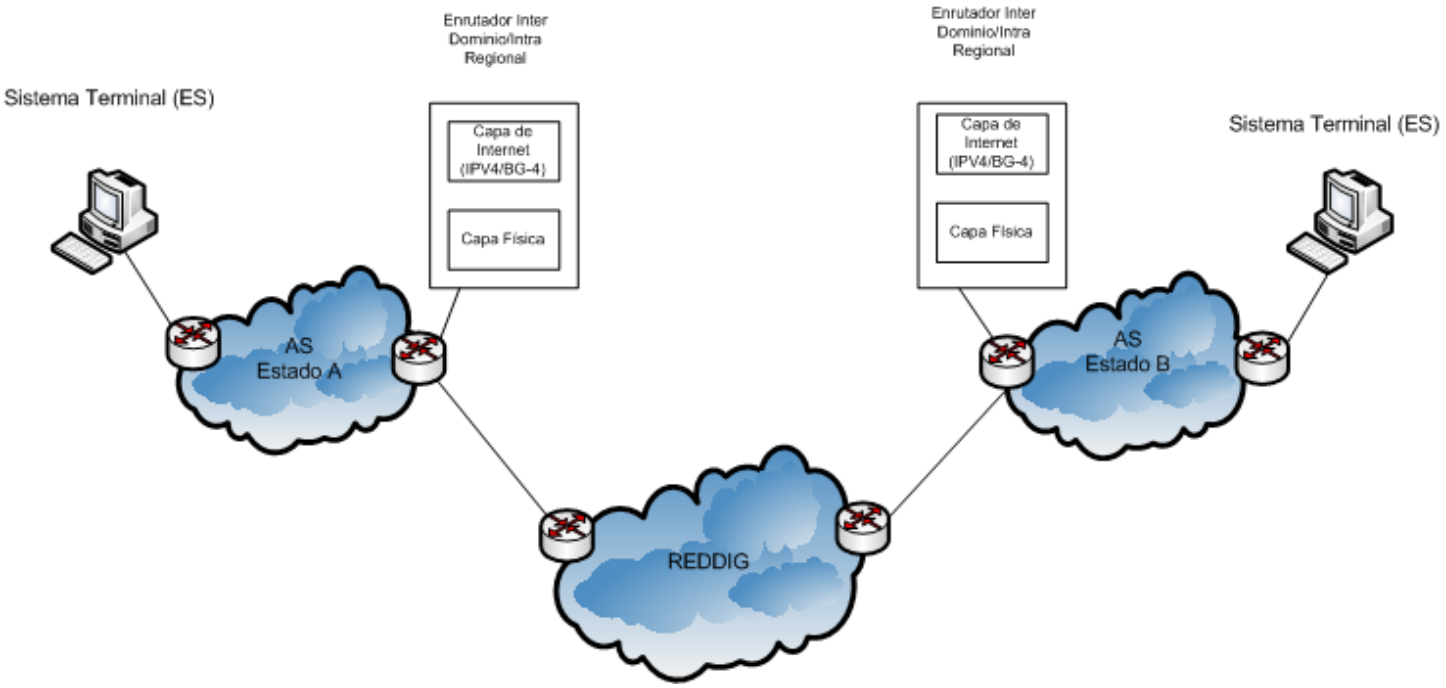


Figura 8: Enrutamiento Intra-Regional SAM

4.2.4 La Figura 9 presenta la topología básica de enrutamiento para la Región SAM, en base a los requerimientos que están presentes en el FASID y en la Tabla además de los futuros que están presentes en el Apéndice C. Como la REDDIG II se trata de una red medular IP, los servicios serán transmitidos del origen al destino, de forma transparente, con el uso de las direcciones IP de los sistemas terminales (ES) y de los números de AS involucrados.

4.2.5 Lógicamente, con el uso de BGP-4, hay que considerarse los conceptos presentados en la Sección 3.3 Enrutamiento con BGP-4, ya que el enrutador de origen no elige el camino hasta el destino, lo que es hecho por el enrutador (*Next-hope*).

4.2.6 Con eso, en la Figura 9 se reflejan los siguientes enrutamientos en la Región SAM, llevándose en cuenta la origen y el destino de las aplicaciones, representados con colores diferentes, además de la Tabla CNS 1Ba (Plan Regional de Encaminadores), que aparece en el **Apéndice D**.

a) En púrpura: enlaces intra-regionales, con el uso de los enrutadores inter-dominio (AS) de los Estados ligados por la REDDIG;
b) En rojo: enlaces inter-regionales con la utilización de la interconexión MEVA II/REDDIG; y
c) En negro: enlaces inter-regionales, donde los enrutadores que pertenecen a un AS de la Región SAM alcanzan su destino por medio de un PST o por la interconexión con la red CAFSAT.

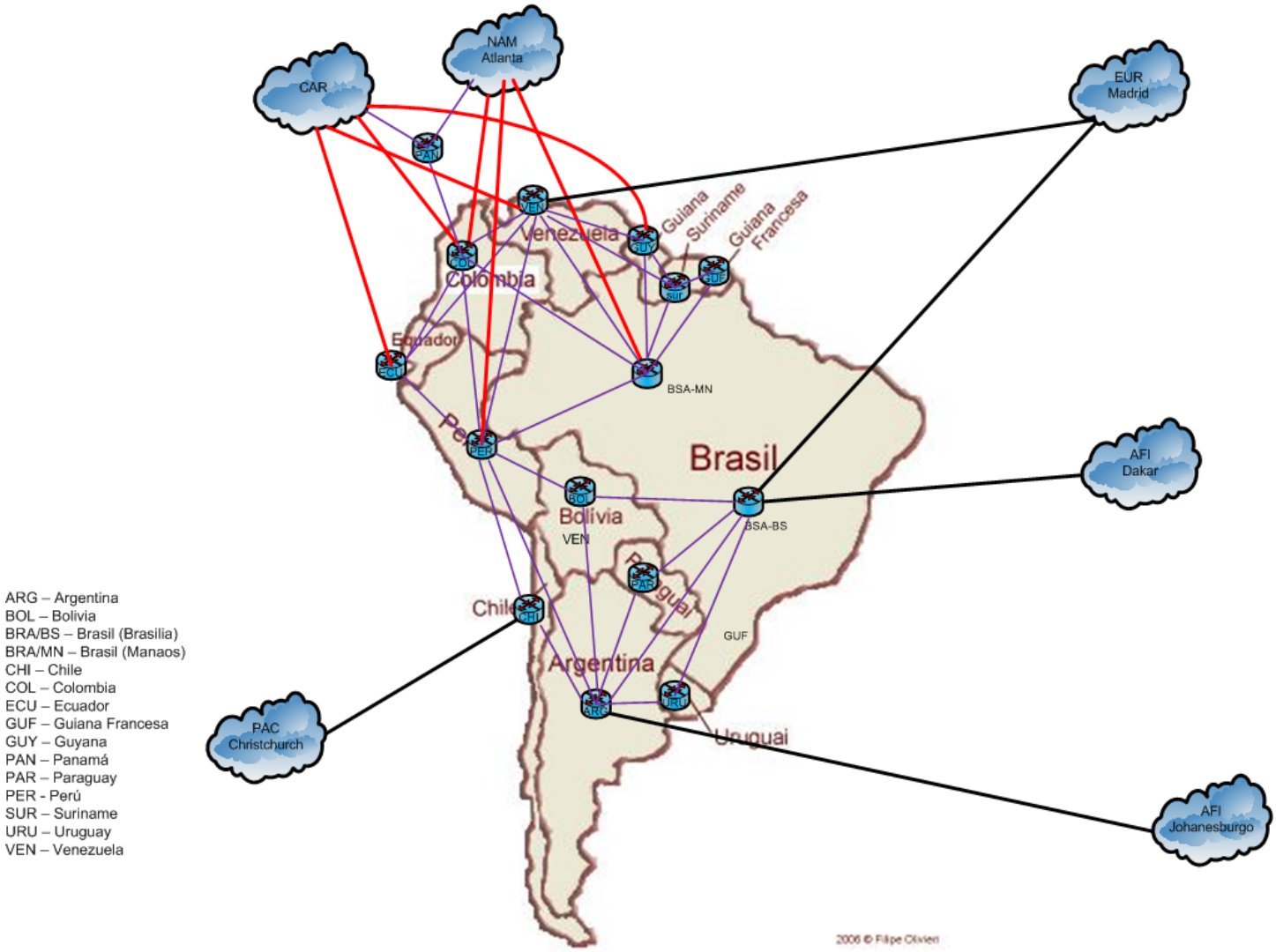


Figura 9: Topología Básica de Enrutamiento SAM

4.2.7 Las siguientes políticas de enrutamiento BGP-4 deberán observadas en la Región SAM:

a) Si en enrutador tiene varios caminos para llegar hasta el destino, deberá ser elegido aquel que pasa por un menor número de AS.

Nota: La REDDIG utiliza la red satelital que funciona como una red determinística con un único salto. Futuramente, la REDDIG II también tendrá la red satelital como principal, sin embargo la red terrestre, que es suministrada por un PST, contará con una infraestructura que podrá involucrar varios AS distintos.

b) Todos los enrutadores que estén configurados con el protocolo BGP-4 en la Región SAM (REDDIG y Estados), deberán hacer la autenticación con los vecinos configurados.
c) Con el objetivo de disminuir el tamaño de las tablas de enrutamiento, los enrutadores BGP-4 de la Región SAM deberán ser configurados para aceptar agregación de rutas.
d) BGP-4 enrutadores que pertenezcan a un dominio administrativo deberán ser configurados para recibir la agregación de rutas de todas las redes internas del AS.
e) El atributo *Local-Preference* debe estar configurado de forma que el enrutador BGP-4 elija el mejor camino de salida cuando al referido enrutador estén conectadas más de una WAN.

4.2.8 Además de las políticas mencionadas, cada Estado o ANSP tiene sus propias políticas que serán complementarias al contenido de este documento.

APENDICE A

Asignación de Redes por Estado/Territorio.

Región	Nro	Estado / Territorio	Red	Direcciones utilizables	Notacion Decimal	Notacion Binaria		
						Región	Estado / Territorio	Host's
SAM	1	Argentina	10.0.0.0 / 19	Primera	10 . 0 . 0 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 0 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 31 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 0 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	2	Chile	10.0.32.0 / 19	Primera	10 . 0 . 32 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 0 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 63 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 0 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	3	Brasil	10.0.64.0 / 19	Primera	10 . 0 . 64 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 1 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 95 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 1 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	4	Uruguay	10.0.96.0 / 19	Primera	10 . 0 . 96 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 1 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 127 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 0 1 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	5	Paraguay	10.0.128.0 / 19	Primera	10 . 0 . 128 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 0 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 159 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 0 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	6	Bolivia	10.0.160.0 / 19	Primera	10 . 0 . 160 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 0 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 191 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 0 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	7	Peru	10.0.192.0 / 19	Primera	10 . 0 . 192 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 1 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 223 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 1 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	8	Ecuador	10.0.224.0 / 19	Primera	10 . 0 . 224 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 1 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 0 . 255 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 0 . 1 1 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	9	Colombia	10.1.0.0 / 19	Primera	10 . 1 . 0 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 1 . 0 0 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 1 . 31 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 1 . 0 0 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	10	Venezuela	10.1.32.0 / 19	Primera	10 . 1 . 32 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 1 . 0 0 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 1 . 63 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 1 . 0 0 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	11	Guyana	10.1.64.0 / 19	Primera	10 . 1 . 64 . 1	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 1 . 0 1 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-	-	-	
				-	-	-	-	
				Ultima	10 . 1 . 95 . 254	0 0 0 0 1 0 1 0 . 0 0 0 0	0 0 0 1 . 0 1 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0

Asignación de Redes por Estado/Territorio.

Región	Nro	Estado / Territorio	Red	Direcciones utilizables	Notacion Decimal	Notacion Binaria		
						Región	Estado / Territorio	Host's
SAM	12	Surinam	10.1.96.0 / 19	Primera	10 . 1 . 96 . 1	00001010.0000	0001.011	00000.00000001
				-	-		-	
				-	-		-	
				Ultima	10 . 1 . 127 . 254	00001010.0000	0001.011	11111.11111110
	13	Guyana Francesa (France)	10.1.128.0 / 19	Primera	10 . 1 . 128 . 1	00001010.0000	0001.100	00000.00000001
				-	-		-	
				-	-		-	
				Ultima	10 . 1 . 159 . 254	00001010.0000	0001.100	11111.11111110
	-	VACANTE	10.1.160.0 / 19	Primera	10 . 1 . 160 . 1	00001010.0000	0001.101	00000.00000001
				-	-		-	
				-	-		-	
				Ultima	10 . 1 . 191 . 254	00001010.0000	0001.101	11111.11111110
	-	VACANTE	10.1.192.0 / 19	Primera	10 . 1 . 192 . 1	00001010.0000	0001.110	00000.00000001
				-	-		-	
				-	-		-	
				Ultima	10 . 1 . 223 . 254	00001010.0000	0001.110	11111.11111110
	-	VACANTE	10.1.224.0 / 19	Primera	10 . 1 . 224 . 1	00001010.0000	0001.111	00000.00000001
				-	-		-	
				-	-		-	
				Ultima	10 . 1 . 255 . 254	00001010.0000	0001.111	11111.11111110
	-	VACANTE	10.2.0.0 / 19	Primera	10 . 2 . 0 . 1	00001010.0000	0010.000	00000.00000001
				-	-		-	
				-	-		-	
				Ultima	10 . 2 . 31 . 254	00001010.0000	0010.000	11111.11111110
	-	-	-	-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
	-	-	-	-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
	-		-	-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
	-	-	-	-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
				-	-		-	
	126 (ULTIMA)	RESERVADA	10.15.224.0 / 19	Primera	10 . 15 . 224 . 1	00001010.0000	1111.111	00000.00000001
				-	-		-	
				-	-		-	
				Ultima	10 . 15 . 255 . 254	00001010.0000	1111.111	11111.11111110

APENDICE B

ENLACES IP INTER/INTRA REGIONALES

Red	Enlace				
	Nro.	Subred	Extremos	Direcciones a utilizar	
10.15.224.0 / 19	1	10.15.224.0 / 30	Argentina-Bolivia	-	10 . 15 . 224 . 0 / 30
				Argentina	10 . 15 . 224 . 1 / 30
				Bolivia	10 . 15 . 224 . 2 / 30
				-	10 . 15 . 224 . 3 / 30
	2	10.15.224.4 / 30	Argentina-Chile	-	10 . 15 . 224 . 4 / 30
				Argentina	10 . 15 . 224 . 5 / 30
				Chile	10 . 15 . 224 . 6 / 30
				-	10 . 15 . 224 . 7 / 30
	3	10.15.224.8 / 30	Argentina-Paraguay	-	10 . 15 . 224 . 8 / 30
				Argentina	10 . 15 . 224 . 9 / 30
				Paraguay	10 . 15 . 224 . 10 / 30
				-	10 . 15 . 224 . 11 / 30
	4	10.15.224.12 / 30	Argentina-Peru	-	10 . 15 . 224 . 12 / 30
				Argentina	10 . 15 . 224 . 13 / 30
				Peru	10 . 15 . 224 . 14 / 30
				-	10 . 15 . 224 . 15 / 30
	5	10.15.224.16 / 30	Argentina-Uruguay	-	10 . 15 . 224 . 16 / 30
				Argentina	10 . 15 . 224 . 17 / 30
				Uruguay	10 . 15 . 224 . 18 / 30
				-	10 . 15 . 224 . 19 / 30
	6	10.15.224.20 / 30	Argentina-AFI	-	10 . 15 . 224 . 20 / 30
				Argentina	10 . 15 . 224 . 21 / 30
				AFI (Johannesburgo)	10 . 15 . 224 . 22 / 30
				-	10 . 15 . 224 . 23 / 30
	7	10.15.224.24 / 30	Brasil-Colombia	-	10 . 15 . 224 . 24 / 30
				Brasil	10 . 15 . 224 . 25 / 30
				Colombia	10 . 15 . 224 . 26 / 30
				-	10 . 15 . 224 . 27 / 30
	8	10.15.224.28 / 30	Brasil-Guyana	-	10 . 15 . 224 . 28 / 30
				Brasil	10 . 15 . 224 . 29 / 30
				Guyana	10 . 15 . 224 . 30 / 30
				-	10 . 15 . 224 . 31 / 30
	9	10.15.224.32 / 30	Brasil-Guyana Francesa	-	10 . 15 . 224 . 32 / 30
				Brasil	10 . 15 . 224 . 33 / 30
				Guyana Francesa	10 . 15 . 224 . 34 / 30
				-	10 . 15 . 224 . 35 / 30

Enlaces Inter/Intra Regionales correspondientes a la Región SAM

Red	Enlace				
	Nro.	Subred	Extremos	Direcciones a utilizar	
10.15.224.0 / 19	10	10.15.224.36 / 30	Brasil-Peru	-	10 . 15 . 224 . 36 / 30
				Brasil	10 . 15 . 224 . 37 / 30
				Peru	10 . 15 . 224 . 38 / 30
				-	10 . 15 . 224 . 39 / 30
	11	10.15.224.40 / 30	Brasil-Surinam	-	10 . 15 . 224 . 40 / 30
				Brasil	10 . 15 . 224 . 41 / 30
				Surinam	10 . 15 . 224 . 42 / 30
				-	10 . 15 . 224 . 43 / 30
	12	10.15.224.44 / 30	Brasil-Venezuela	-	10 . 15 . 224 . 44 / 30
				Brasil	10 . 15 . 224 . 45 / 30
				Venezuela	10 . 15 . 224 . 46 / 30
				-	10 . 15 . 224 . 47 / 30
	13	10.15.224.48 / 30	Brasil-AFI (tentativo)	-	10 . 15 . 224 . 48 / 30
				Brasil	10 . 15 . 224 . 49 / 30
				AFI (Dakar)	10 . 15 . 224 . 50 / 30
				-	10 . 15 . 224 . 51 / 30
	14	10.15.224.52 / 30	Brasil-EUR (tentativo)	-	10 . 15 . 224 . 52 / 30
				Brasil	10 . 15 . 224 . 53 / 30
				EUR (Madrid)	10 . 15 . 224 . 54 / 30
				-	10 . 15 . 224 . 55 / 30
	15	10.15.224.56 / 30	Brasil-NAM	-	10 . 15 . 224 . 56 / 30
				Brasil	10 . 15 . 224 . 57 / 30
				NAM(Atlanta)	10 . 15 . 224 . 58 / 30
				-	10 . 15 . 224 . 59 / 30
	16	10.15.224.60 / 30	Brasil-Argentina	-	10 . 15 . 224 . 60 / 30
				Brasil	10 . 15 . 224 . 61 / 30
				Argentina	10 . 15 . 224 . 62 / 30
				-	10 . 15 . 224 . 63 / 30
	17	10.15.224.64 / 30	Brasil-Bolivia	-	10 . 15 . 224 . 64 / 30
				Brasil	10 . 15 . 224 . 65 / 30
				Bolivia	10 . 15 . 224 . 66 / 30
				-	10 . 15 . 224 . 67 / 30
	18	10.15.224.68 / 30	Brasil-Paraguay	-	10 . 15 . 224 . 68 / 30
				Brasil	10 . 15 . 224 . 69 / 30
				Paraguay	10 . 15 . 224 . 70 / 30
				-	10 . 15 . 224 . 71 / 30

Enlaces Inter/Intra Regionales correspondientes a la Región SAM

Red	Enlace				
	Nro.	Subred	Extremos	Direcciones a utilizar	
10.15.224.0 / 19	19	10.15.224.72 / 30	Brasil-Uruguay	-	10 . 15 . 224 . 72 / 30
				Brasil	10 . 15 . 224 . 73 / 30
				Uruguay	10 . 15 . 224 . 74 / 30
				-	10 . 15 . 224 . 75 / 30
	20	10.15.224.76 / 30	Chile-PAC	-	10 . 15 . 224 . 76 / 30
				Chile	10 . 15 . 224 . 77 / 30
				PAC(Christchurch)	10 . 15 . 224 . 78 / 30
				-	10 . 15 . 224 . 79 / 30
	21	10.15.224.80 / 30	Chile-Peru	-	10 . 15 . 224 . 80 / 30
				Chile	10 . 15 . 224 . 81 / 30
				Peru	10 . 15 . 224 . 82 / 30
				-	10 . 15 . 224 . 83 / 30
	22	10.15.224.84 / 30	Colombia-NAM	-	10 . 15 . 224 . 84 / 30
				Colombia	10 . 15 . 224 . 85 / 30
				NAM (Atlanta)	10 . 15 . 224 . 86 / 30
				-	10 . 15 . 224 . 87 / 30
	23	10.15.224.88 / 30	Colombia-Ecuador	-	10 . 15 . 224 . 88 / 30
				Colombia	10 . 15 . 224 . 89 / 30
				Ecuador	10 . 15 . 224 . 90 / 30
				-	10 . 15 . 224 . 91 / 30
	24	10.15.224.92 / 30	Colombia-Peru	-	10 . 15 . 224 . 92 / 30
				Colombia	10 . 15 . 224 . 93 / 30
				Peru	10 . 15 . 224 . 94 / 30
				-	10 . 15 . 224 . 95 / 30
	25	10.15.224.96 / 30	Colombia-Venezuela	-	10 . 15 . 224 . 96 / 30
				Colombia	10 . 15 . 224 . 97 / 30
				Venezuela	10 . 15 . 224 . 98 / 30
				-	10 . 15 . 224 . 99 / 30
	26	10.15.224.100 / 30	Ecuador-Peru	-	10 . 15 . 224 . 100 / 30
				Ecuador	10 . 15 . 224 . 101 / 30
				Peru	10 . 15 . 224 . 102 / 30
				-	10 . 15 . 224 . 103 / 30
	27	10.15.224.104 / 30	Ecuador-Venezuela	-	10 . 15 . 224 . 104 / 30
				Ecuador	10 . 15 . 224 . 105 / 30
				Venezuela	10 . 15 . 224 . 106 / 30
				-	10 . 15 . 224 . 107 / 30

Enlaces Inter/Intra Regionales correspondientes a la Región SAM

Red	Enlace				
	Nro.	Subred	Extremos	Direcciones a utilizar	
10.15.224.0 / 19	28	10.15.224.108 / 30	Guyana Francesa-Surinam	-	10 . 15 . 224 . 108 / 30
				Guyana Francesa	10 . 15 . 224 . 109 / 30
				Surinam	10 . 15 . 224 . 110 / 30
				-	10 . 15 . 224 . 111 / 30
	29	10.15.224.112 / 30	Guyana-C-CAR	-	10 . 15 . 224 . 112 / 30
				Guyana	10 . 15 . 224 . 113 / 30
				C-CAR (Piarco)	10 . 15 . 224 . 114 / 30
				-	10 . 15 . 224 . 115 / 30
	30	10.15.224.116 / 30	Guyana-Surinam	-	10 . 15 . 224 . 116 / 30
				Guyana	10 . 15 . 224 . 117 / 30
				Surinam	10 . 15 . 224 . 118 / 30
				-	10 . 15 . 224 . 119 / 30
	31	10.15.224.120 /30	Guyana-Venezuela	-	10 . 15 . 224 . 120 / 30
				Guyana	10 . 15 . 224 . 121 / 30
				Venezuela	10 . 15 . 224 . 122 / 30
				-	10 . 15 . 224 . 123 / 30
	32	10.15.224.124 / 30	Peru-NAM	-	10 . 15 . 224 . 124 / 30
				Peru	10 . 15 . 224 . 125 / 30
				NAM (Atlanta)	10 . 15 . 224 . 126 / 30
				-	10 . 15 . 224 . 127 / 30
	33	10.15.224.128 / 30	Peru-Bolivia	-	10 . 15 . 224 . 128 / 30
				Peru	10 . 15 . 224 . 129 / 30
				Bolivia	10 . 15 . 224 . 130 / 30
				-	10 . 15 . 224 . 131 / 30
	34	10.15.224.132 / 30	Peru-Colombia	-	10 . 15 . 224 . 132 / 30
				Peru	10 . 15 . 224 . 133 / 30
				Colombia	10 . 15 . 224 . 134 / 30
				-	10 . 15 . 224 . 135 / 30
	35	10.15.224.136 / 30	Peru-Venezuela	-	10 . 15 . 224 . 136 / 30
				Peru	10 . 15 . 224 . 137 / 30
				Venezuela	10 . 15 . 224 . 138 / 30
				-	10 . 15 . 224 . 139 / 30
	36	10.15.224.140 / 30	Surinam-Venezuela	-	10 . 15 . 224 . 140 / 30
				Surinam	10 . 15 . 224 . 141 / 30
				Venezuela	10 . 15 . 224 . 142 / 30
				-	10 . 15 . 224 . 143 / 30

Enlaces Inter/Intra Regionales correspondientes a la Región SAM

Red	Enlace				
	Nro.	Subred	Extremos	Direcciones a utilizar	
10.15.224.0 / 19	37	10.15.224.144 / 30	Venezuela-CAM	-	10 . 15 . 224 . 144 / 30
				Venezuela	10 . 15 . 224 . 145 / 30
				CAM (San Juan)	10 . 15 . 224 . 146 / 30
				-	10 . 15 . 224 . 147 / 30
	38	10.15.224.148 / 30	Venezuela-EUR	-	10 . 15 . 224 . 148 / 30
				Venezuela	10 . 15 . 224 . 149 / 30
				EUR (Madrid)	10 . 15 . 224 . 150 / 30
				-	10 . 15 . 224 . 151 / 30
	39	10.15.224.152 / 30	Venezuela-Trinidad y Tobago	-	10 . 15 . 224 . 152 / 30
				Venezuela	10 . 15 . 224 . 153 / 30
				Trinidad y Tobago	10 . 15 . 224 . 154 / 30
				-	10 . 15 . 224 . 155 / 30
	40	10.15.224.156 / 30	VACANTE	-	10 . 15 . 224 . 156 / 30
					10 . 15 . 224 . 157 / 30
					10 . 15 . 224 . 158 / 30
				-	10 . 15 . 224 . 159 / 30
	41	10.15.224.160 / 30	VACANTE	-	10 . 15 . 224 . 160 / 30
					10 . 15 . 224 . 161 / 30
					10 . 15 . 224 . 162 / 30
				-	10 . 15 . 224 . 163 / 30
	42	10.15.224.164 / 30	VACANTE	-	10 . 15 . 224 . 164 / 30
					10 . 15 . 224 . 165 / 30
					10 . 15 . 224 . 166 / 30
				-	10 . 15 . 224 . 167 / 30
	-	-	-	-	-
					-
					-
				-	-
	-	-	-	-	-
					-
					-
				-	
	2048 (última)	10.15.31.252 / 30	VACANTE	-	10 . 15 . 31 . 252 / 30
					10 . 15 . 31 . 253 / 30
					10 . 15 . 31 . 254 / 30
				-	10 . 15 . 31 . 255 / 30

APENDICE C

1. B1 - Arquitectura Actual de Red de la Región SAM

1.1 La OACI, Contratante en nombre de los Estados Miembros, a través del Proyecto de Cooperación Técnica RLA03/901, es el Organismo encargado de la coordinación, licitación y dirección de de la Red Digital de Comunicaciones SAM (REDDIG).

1.2 Los países y nodos, con sus coordenadas geográficas básicas, que son parte de esta licitación, son los detallados en la Tabla 2.

País	Nodo	Indicativo	Latitud	Longitud
Argentina	Ezeiza	SAEZ	34° 49’ 25” S	58° 31’ 43” W
Bolivia	La Paz	SLLP	16° 30’ 29” S	68° 11’ 24” W
Brasil	Manaos	SBMN	03° 02’ 19” S	60° 02’ 59” W
	Recife	SBRE	08° 07’ 36” S	34° 55’ 23” W
	Curitiba	SBCT	25° 31’ 43” S	49° 10’ 33” W
Chile	Santiago	SCEL	33° 23’ 26” S	70° 47’ 09” W
Colombia	Bogotá	SKED	04° 42’ 05” N	74° 08’ 48” W
Ecuador	Guayaquil	SEGU	02° 09’ 29” S	79° 53’ 02” W
Guyana	Georgetown	SYGC	06° 29’ 56” N	58° 15’ 16” W
French Guyana	Cayenne	SOCA	04° 49’ 11” N	52° 21’ 38” W
Paraguay	Asunción	SGAS	25° 14’ 24” S	57° 31’ 09” W
Perú	Lima	SPIM	12° 01’ 19” S	77° 06’ 52” W
Surinam	Paramaribo	SMPM	05° 27’ 10” N	55° 11’ 16” W
Trinidad y Tobago	Piarco	TTZP	10° 35’ 44” N	61° 20’ 36” W
Uruguay	Montevideo	SUMU	34° 50’ 15” S	56° 01’ 49” W
Venezuela	Maiquetía	SVMI	10° 36’ 12” N	66° 59’ 26” W

Tabla 2: Ubicación de los Nodos de la REDDIG

1.3 La topología básica de la actual REDDIG, con sus dieciséis nodos, está representada en la Figura 1.

Figura 1: Topología Actual de la REDDIG

1.4 Además de lo esquematizado en la Figura 1, la REDDIG está interconectada a la red MEVAII, que atiende a los países de Centro-América, Caribe y los Estados Unidos. Para dicha interconexión, la REDDIG utiliza los nodos de Bogotá (Colombia) y Maiquetía (Venezuela), conforme a lo descrito en la Figura 2.

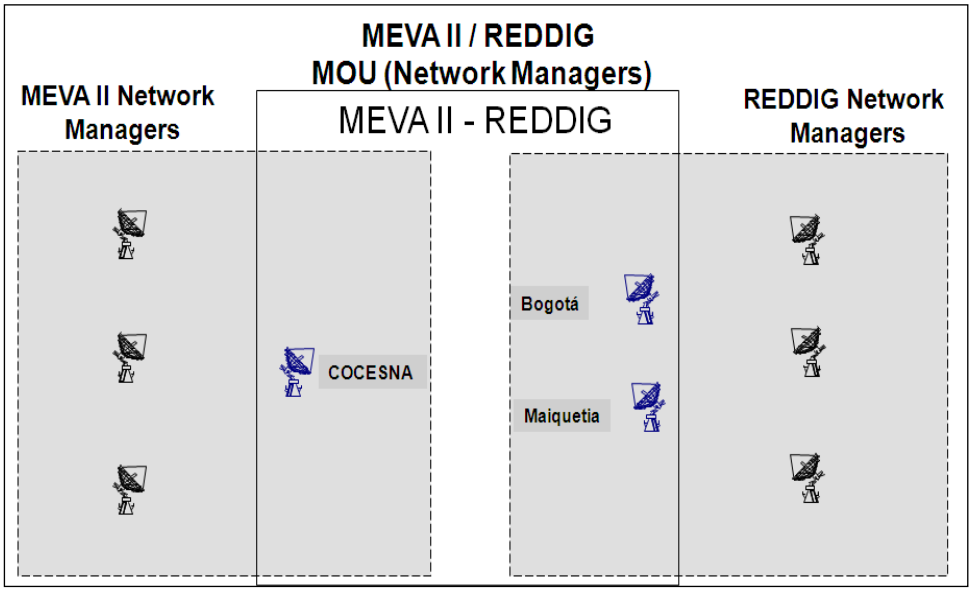


Figura 2. Interconexión MEVA II - REDDIG

1.5 Las características básicas de la red actual son las siguientes:

a) La REDDIG es una red mallada que utiliza la tecnología VSAT (*Very Small Aperture Terminal*) con antenas de 3,7m, Banda C (4-6 GHz), utilizando el satélite INTELSAT IS-14, que está localizado a 315°E. Actualmente la capacidad rentada para satisfacer las necesidades de las aplicaciones de la REDDIG es de 4,4 MHz.
b) La REDDIG dispone de un total de 1.328 Kbps para cursar tráfico entre todos los terminales de la red, que equivalen a 83 bursts de 16 Kbits/s.
c) El proveedor satelital actual es INTELSAT, ya que la Organización de Aviación Civil Internacional (OACI) como Agencia de la Organización de las Naciones Unidas (ONU), es signatario de pleno derecho ante la misma, por lo que se encarga de reservar y abonar el ancho de banda requerido.
d) La red REDDIG utiliza la banda C (4-6 GHz), debido a que algunos de sus nodos se encuentran en zonas cuyas condiciones climatológicas así lo requieren.
e) Los principales equipos (*indoor* y *outdoor*), así como el software utilizado, se encuentran descriptos en el Apéndice A, mientras que los principales servicios de voz y datos, están descriptos en Apéndice B.
f) La red también soporta RC&M (*Remote Control & Monitoring)* para el manejo eficiente de los recursos. Hay dos centros de control de la red (NCC), estando el principal está ubicado en Manaos (Brasil) y el alterno en Ezeiza (Argentina).
g) La interconexión entre las redes MEVA II y REDDIG mantiene las características básicas individuales de las dos redes en términos de gestión y control. Sin embargo, agrega un modem de la MEVA II en los nodos REDDIG de Bogotá (Colombia) y Maiquetía (Venezuela), y un modem de la REDDIG al nodo de la MEVA II de COCESNA (Honduras).

2. B2 - Arquitectura futura de la red

2.1 La REDDIG II surge de la necesidad de mantener las comunicaciones y servicios de la Navegación Aérea entre las diferentes dependencias de tránsito aéreo de la región que actualmente son provistos por la REDDIG e implementar el *backbone* de la Red de Telecomunicaciones Aeronáuticas (ATN).

2.2 En la Figura 3 se presenta un esquema de la topología básica exigida para a REDDIG II.

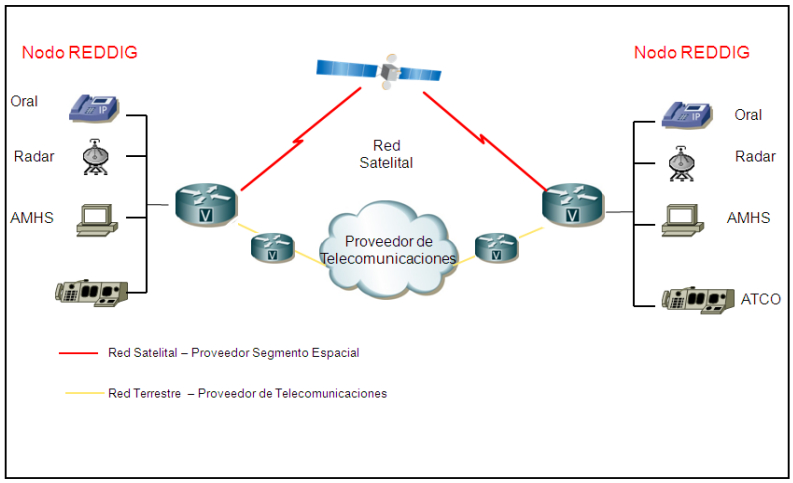


Figura 3: Topología Básica REDDIG II

2.3 Como se pode notar de la Figura 3, la REDDIG II será conformada por dos segmentos, uno por transmisión por satélite (VSAT) y el otro terrestre con la adopción de la tecnología *Multiprotocol Label Switching* (MPLS). El *backbone* satelital será el principal y el terrestre funcionará para aumentar la flexibilidad para la carga de nuevas aplicaciones, ya que es IP, además del incremento de la disponibilidad conjunta de la red. Caso ocurra cualquier falla en la red principal, la conmutación al *backbone* terrestre será automática.

2.4 La topología de las redes satelital y terrestre será totalmente mallada, flexible y escalable para facilitar el crecimiento de la infraestrutura. Además de eso, presentará alta disponibilidad, con: inteligencia distribuida en sus nodos y sin punto común de fallo, priorización del tráfico, administración dinámica y por demanda del ancho de banda, enrutamiento alterno automático del tráfico en caso de falla y sistema de gestión de red (NMS) común, integrado, y global a "prueba de futuro" para permitir la migración a otras tecnologías de redes.

2.5 El sistema de ruteo que será implantado posee características importantes para el propósito de este documento, ya que deberán soportar protocolos de enrutamiento internos (IGP), tales como RIP (Versión 1 y 2) y OSPF, y el protocolo de enrutamiento externo BGP-4.

2.6 Los requisitos principales del sistema VSAT serán:

a) Red HUBLESS, sin punto común de falla. Todas las estaciones serán idénticas, no deben existir estaciones especializadas. Cualquier estación debe ser capaz de actuar como una estación de referencia de tiempo para la red satelital, con solo una eventual actualización de software.
b) Esquema seguro de control mediante rotación preestablecida y programable que define la terminal maestra y la de respaldo, cambio automático en caso de avería de la estación maestra, o arquitectura con auto sincronización que no requiere de estación maestra.
c) Topología completamente *mallada*: deben establecerse los enlaces para satisfacer la topología de la red y los requerimientos de comunicaciones.
d) Todas las comunicaciones deberán ser establecidas mediante un solo salto satelital (*simple hop*).
e) Los enlaces satelitales presentarán una Tasa de Error de Bit (BER) mejor que 1 E-7.
f) Funcionamiento en la banda C.

2.7 El *Backbone* Terrestre de la REDDIG II 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. Los requisitos principales son descriptos a seguir:

a) La disponibilidad mensual de cada enlace deberá ser el mínimo de 99,5%.
b) El retardo (*delay*) deberá ser inferior a 60 ms.
c) El RTT en la comunicación entre dos estaciones**,** para un paquete de 64 bytes, no podrá ser mayor que 150 ms en 95 % de las medidas hechas en una ventana de tiempo mínima de 10 segundos.
d) La BER deberá ser menor que 10^{-7} para el 99,5% del tiempo.

APENDICE D

1. C1 - Requerimientos de servicios para el apoyo a la navegación aérea en la Región SAM, incluyendo los previstos a corto, mediano y largo plazo

1.1 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 nueva red digital, se compone de los:

1.1.1 Servicios actuales

1.1.1.1 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).
b) Tabla CNS1C (Plan de circuitos orales directos ATS).

1.1.2 Servicios futuros

a) Los que surgieron de la interconexión MEVA II – REDDIG.
b) 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.
c) 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.
d) Los requerimientos de interconexión AMHS, reemplazando progresivamente el servicio AFTN, de acuerdo a los respectivos MoU (Memorandos de Entendimientos) suscriptos o a subscribirse.
e) Los requerimientos de interconexión AIDC, reemplazando progresivamente el servicio Oral ATS.
f) El Intercambio de datos ADS-B y multilateración, entre todos los ACCs de FIRs colindantes.
g) La Interconexión de sistemas automatizados utilizando Asterix 62 y 63, entre todos los ACCs de FIRs colindantes.
h) Los requerimientos AIM: respecto a este particular, a la fecha no se dispone de un requerimiento concreto.

1.2 En la Tabla B-1, se describen las *interfaces* mínimas con que deberán contar los encaminadores a instalar en cada Estado por la ocasión de la implantación de la REDDIG II.

Estado	Lugar	Interfaces mínimas					
		I/O Universal	Ethernet	Digital	E&M	FXO	FXS
Argentina	Ezeiza	11	1	0	11	0	1
Bolivia	La Paz	4	1	0	4	0	4
Brasil	Curitiba	4	1	0	6	2	1
	Manaos	6	1	0	7	0	5
	Recife	1	1	0	7	0	1
Chile	Santiago	2	1	0	8	0	0

Estado	Lugar	Interfaces mínimas					
		I/O Universal	Ethernet	Digital	E&M	FXO	FXS
Colombia	Bogotá	7	1	1	0	0	0
Ecuador	Guayaquil	3	1	1	0	0	0
Guyana Francesa	Rochambeau	2	1	0	0	0	5
Guyana	Georgetown	4	1	0	0	0	5
Paraguay	Asunción	3	1	0	3	0	3
Perú	Lima	9	1	1	0	0	0
Surinam	Panamaribo	3	1	0	0	0	4
Trinidad y Tobago	Piarco	2	1	0	0	0	6
Uruguay	Montevideo	2	1	0	0	4	5
Venezuela	Maiquetía	10	1	0	7	0	4

Tabla B-1: Interfaces Futuras para la REDDIG II

1.3 La Tabla B-2 presenta el ancho de banda estimativo, para la REDDIG II, con fines a soportar los nuevos servicios que deberán ser implantados en la Región SAM

Estado	Lugar	Servicio (cada uno en Kbps)			
		AFTN	Radar	AMHS	ADS-B
Argentina	Ezeiza		76.8	28.8	19.2
Bolivia	La Paz		115.2	14.4	19.2
Brasil	Curitiba		76.8	19.2	19.2
	Manaos	9.6	134.4	33.6	19.2
	Recife		0	4.8	19.2
Chile	Santiago		57.6	9.6	19.2
Colombia	Bogotá	19.2	76.8	38.4	19.2
Ecuador	Guayaquil		38.4	14.4	19.2
Guyana Francesa	Rochambeau		38.4	9.6	19.2
Guyana	Georgetown		57.6	19.2	19.2
Paraguay	Asunción		57.6	9.6	19.2
Perú	Lima	9.6	96	43.2	19.2
Surinam	Panamaribo		76.8	14.4	19.2
Trinidad y Tobago	Piarco		19.2	9.6	19.2
Uruguay	Montevideo		19.2	9.6	19.2
Venezuela	Maiquetía		76.8	38.4	19.2
Parciales (Kbps)		38.4	1017.6	316.8	307.2
Parcial global (Kbps)		1680			

Estado	Lugar	Servicio (cada uno en Kbps)			
		AFTN	Radar	AMHS	ADS-B
Diferencia AFTN		-103.2			
Incremento neto ancho de banda		**1576.8**			

Tabla B-2: Ancho de banda adicional estimativo

APENDICE E

TABLE/TABLA CNS 1Ba –ROUTERS REGIONAL PLAN / PLAN REGIONAL DE ENCAMINADORES SAM REGION / REGIÓN SAM

Administration and Location/ Administración y Localidad	Type of Router / Tipo de Encaminador	Type of Interconnection/ Tipo de interconexión	ConnectedRouter- Encaminador Conectado	Link Speed- Velocidad del enlace	Link Protocol- Protocolo del Enlace	Via Vía	Target Date / Fecha Meta	Remarks Observaciones
1	2	3	4	5	6	7	8	9
Argentina/Buenos Aires	IP	Inter Regional	AFI (Johannesburgo)	64K	IPv6	CAFSAT	TBD	
	IP	Intra Regional	Bolivia (La Paz)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Chile (Santiago)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Brazil (Brasilia)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Paraguay (Asunción)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Perú (Lima)	64K	IPv4	REDDIG	2011	
	IP	Intra Regional	Uruguay (Montevideo)	64K	IPv4	REDDIG	2011	
Bolivia/La Paz	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Brazil (Brasilia)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Perú (Lima)	64K	IPv4	REDDIG	2014	
Brazil/Brasilia	IP	Inter Regional	AFI (Dakar)	TBD	IPv6	CAFSAT	TBD	
	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Bolivia (La Paz)	64K	IPv4	REDDIG	2014	
	IP	Inter Regional	EUR(Madrid)	64K	IPv6	PTT	2014	
	IP	Inter Regional	NAM (Atlanta)	64K	IPv4	MEVA II/ REDDIG	2014	Circuito via Bogotá
	IP	Intra Regional	Paraguay (Asunción)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Uruguay (Montevideo)	64K	IPv4	REDDIG	2014	
Brazil/Manaus	IP	Intra Regional	Colombia (Bogotá)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Guyana (Georgetown)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Guyana Francesa (Cayena)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Perú (Lima)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Surinam(Paramaribo)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2012	

Administration and Location/ Administración y Localidad	Type of Router / Tipo de Encaminador	Type of Interconnection/ Tipo de interconexión	ConnectedRouter- Encaminador Conectado	Link Speed- Velocidad del enlace	Link Protocol- Protocolo del Enlace	Via Vía	Target Date / Fecha Meta	Remarks Observaciones
1	2	3	4	5	6	7	8	9
Chile/Santiago	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2012	
	IP	Inter Regional	PAC (Christchurch)	TBD	IPv4	PTT	TBD	
	IP	Intra Regional	Perú (Lima)	64K	IPv4	REDDIG	2014	
Colombia/Bogotá	IP	Intra Regional	Brazil (Manaus)	64K	IPv4	REDDIG	2014	
	IP	Inter Regional	CAR	64K	IPv4	MEVAII/REDDIG	2014	
	IP	Intra Regional	Ecuador (Guayaquil)	64K	IPv4	REDDIG	2014	
	IP	Inter Regional	NAM (Atlanta)	2x 64K	IPv4	MEVA II / REDDIG	2014	Conexión Colombia y Brasil
	IP	Intra Regional	Panamá	64k	IPv4	MEVAII/REDDIG	2014	
	IP	Intra Regional	Perú (Lima)	64K	IPv4	REDDIG	2010	
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2014	
Ecuador/Guayaquil	IP	Inter Regional	CAR	64K	IPv4	MEVA II / REDDIG	2014	
	IP	Intra Regional	Colombia (Bogotá)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Perú (Lima)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2014	
French Guiana/Cayenne Guyana Francesa/ Cayena	IP	Intra Regional	Brazil (Manaus)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Surinam (Paramaribo)	64K	IPv4	REDDIG	2014	
Guyana/Georgetown	IP	Intra Regional	Brazil (Manaos)	64K	IPv4	REDDIG	2014	
	IP	Inter Regional	CAR	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Surinam(Paramaribo)	64K	IPv4	REDDIG	2011	
	IP	Intra Regional	Venezuela(Caracas)	64K	IPv4	REDDIG	2014	
Panamá/Panamá	IP	Inter Regional	CAR	64K	IPv4	CAMSAT	2012	
	IP	Intra Regional	Colombia (Bogotá)	64K	IPv4	MEVAII / REDDIG	2014	
	IP	Inter Regional	NAM (Atlanta)	64K	IPv4	MEVA II	2014	
Paraguay/Asunción	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Brazil (Brasilia)	64K	IPv4	REDDIG	2014	

Administration and Location/ Administración y Localidad	Type of Router / Tipo de Encaminador	Type of Interconnection/ Tipo de interconexión	ConnectedRouter- Encaminador Conectado	Link Speed- Velocidad del enlace	Link Protocol- Protocolo del Enlace	Via Vía	Target Date / Fecha Meta	Remarks Observaciones
1	2	3	4	5	6	7	8	9
Perú/Lima	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2011	
	IP	Intra Regional	Bolivia (La Paz)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Brazil (Manaos)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Chile(Santiago)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Colombia (Bogotá)	64K	IPv4	REDDIG	2010	
	IP	Intra Regional	Ecuador (Guayaquil	64K	IPv4	REDDIG	2012	
	IP	Inter Regional	NAM (Atlanta)	64K	IPv4	MEVAII/REDDIG	2014	Via Bogotá Colombia
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2014	
Suriname/Paramaribo	IP	IntraRegional	Brazil (Manaos)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Guyana Francesa (Cayena)	64K	IPv4	REDDIG	2011	
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2014	
Uruguay/Montevideo	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2011	
	IP	Intra Regional	Brazil (Brasilia)	64K	IPv4	REDDIG	2014	
Venezuela/Caracas	IP	Inter Regional	CAR	128K	IPv4	MEVA II / REDDIG	2014	
	IP	Inter Regional	EUR(Madrid)	64K	IPv6	PTT	2014	
	IP	Intra Regional	Brazil (Manaus)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Colombia (Bogotá)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Ecuador (Quito)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Guyana (Georgetown)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Suriname (Paramaribo)	64K	IPv4	REDDIG	2014	

APENDICE F

ESTADO	TIPO DE ENCAMINADOR	NUMERO DE AS
Argentina	IP	64517
Bolivia	IP	64529
Brasil	IP	64531
Chile	IP	64543
Colombia	IP	64545
Ecuador	IP	64558
Guyana	IP	64574
Guyana Francesa	IP	64575
Panamá	IP	65261
Paraguay	IP	65263
Perú	IP	65264
Suriname	IP	65288
Uruguay	IP	65302
Venezuela	IP	64528

- - - - - -