Agenda Item 5: Assessment of operational requirements in order to determine the implementation of communications, navigation, and surveillance (CNS) capabilities improvement for en-route and terminal area operations

ACTIVITIES PERFORMED UNDER THE SAM ATN ARCHITECTURE PROJECT

(Presented by the Coordinator of the SAM ATN Architecture Project)

SUMMARY

The purpose of this working paper is to inform participants about the status of the deliverables foreseen for the SAM ATN Architecture Project.

REFERENCES:

- CAR/SAM ATN Architecture Project (D1);
- Sixteenth Meeting of the CAR/SAM Planning and Implementation Group - GREPECAS/16 (Punta Cana, Dominican Republic, 28 March-1 April 2011;
- Tenth Workshop/Meeting of the SAM Implementation Group (SAM/IG/10) RLA/06/901 Project (Lima, Peru, 10-14 October 2011);
- Study for the Implementation of a New South American Digital Network (REDDIG);
- Technical Specifications for REDDIG II; and
- Bidding for the modernization of REDDIG

ICAO strategic objectives:	*A – Safety* *C - Environmental Protection and Sustainable Development of Air Transport*

1. Introducción

1.1 The Ground-Ground and Air-Ground Communications Infrastructure Programme encompassed two Projects, as follows:

a) CAR/SAM ATN Architecture (D1); and
b) ATN ground-ground and ground-air applications (D2).

1.2 It should be highlighted that in the beginning, the CAR/SAM ATN Architecture Project ended with the selection of the optimum IP-based platform for the CAR and SAM Regions. The Project did not deal with the implementation of the new network (REDDIG II), to replace the current structure.

1.3 On the basis of the above paragraph, the Programme Coordinator and Project D1 Coordinator reviewed all the deliverables involved and arrived to the conclusion that the Project should be extended to include the monitoring tasks pertaining to REDDIG II implementation, estimated to be implemented by the first quarter of 2015.

1.4 In this regard, this working paper describes all of the documents involved, the changes and adjustments made in the original documents for the CAR/SAM Infrastructure Project (D1) and the activities that were carried out in to date.

2. Analysis

2.1 The new Project Coordinators for the SAM Region were appointed at the SAM/IG/7 meeting, with Mr. Athayde Licério Vieira Frauche (Brazil), an expert who was already working on the tasks for the CAR/SAM Region, being retained as Coordinator for the SAM Architecture Project.

2.2 Changes were then made in all of the original documents to provide for the tasks involving only the SAM Region, as described in the body of this working paper.

2.3 Project Documents

2.3.1 The documents that make up the SAM ATN Architecture Project are:

a) Working Programme;
b) Project Description (DP);
c) Project File; and
d) Detailed Working Structure (EDT).

2.3.2 To the original deliverables assigned to the CAR/SAM ATN Architecture Project, and which were taken into account for the specific SAM Region Project, the monitoring of REDDIG II implementation was added, which is described under Deliverable D 1.8. The Table shown in **Appendix A** contains the updated work programme.

2.3.3 As a result of the analysis made, the deliverables of the SAM ATN Architecture Project are enumerated in the Project Description document in Appendix B. The document contains a summary of the main project phases, from inception to the completion of its full activities. The date for REDDIG II implementation was updated to March 2015, taking into account the delays in the signature of the contract with the bid winner.

2.4 Progress in the activities

2.4.1 The fifth workshop/meeting of the SAM Implementation Group (SAM/IG/5) considered the possibility of conducting studies on the implementation of a new regional satellite, ground or mixed (satellite and ground) digital network to serve as the backbone for the SAM Aeronautical Telecommunications Network (SAM ATN). This new network would have to be designed to support current fixed aeronautical requirements for voice and data transmission and exchange of radar data and flight plans, together with the new ATN ground-ground applications between States/Territories in the SAM Region that are planned for implementation in the short and medium terms.

2.4.2 At the SAM/IG/6 meeting, the studies for the choice of the IP backbone for the SAM Region were completed and submitted for evaluation to States in the Region.

2.4.3 The elaboration, in August 2011, of the technical specifications for modernizing the REDDIG envisaged the natural evolution of all elements presented in the deliverables.

2.4.4 Emphasis in made on the fact that the specifications documents were presented and approved at the Twelfth Meeting of Civil Aviation Authorities of the SAM Region (RAAC/12), held in Lima, Peru, from 3 to 6 October 2012.

2.4.5 REDDIG II will be composed by satellite (main) and ground backbones, which are to work in parallel to increase availability and flexibility of the new applications in the network. Figure 1 shows the future REDDIG II architecture.

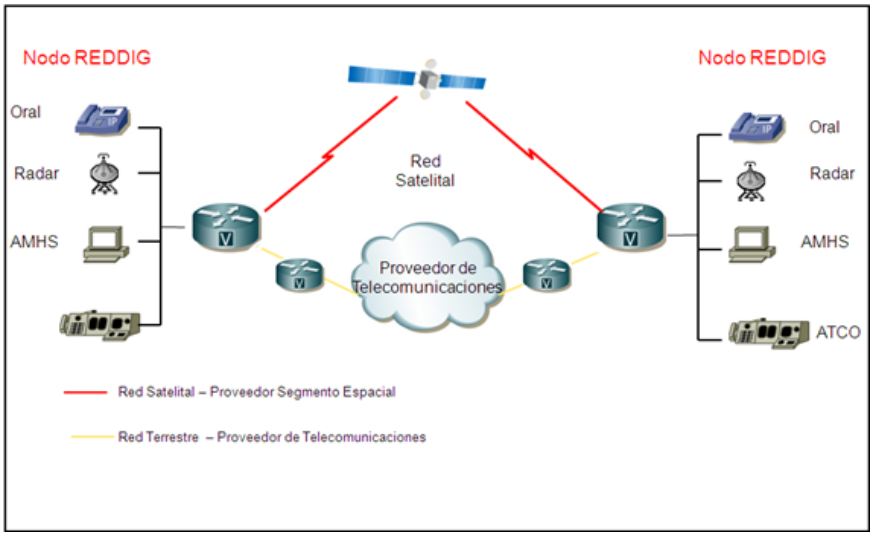


Figure 1: REDDIG II Architecture

2.4.6 With support of RLA/03/901 technical cooperation Project, two experts were hired for a one-week period each, for the development of the Safety Guide and Routing Policy for the SAM Region, presented in **Appendices C** and **D**, respectively.

2.4.7 In consequence, the only task pending for REDDIG II implementation, which mainly depends on the signature of the contract by ICAO TCB, on behalf of all REDDIG member States, with INEO, the company bid winner. In this respect, the Secretariat is preparing a working paper will all details on the evolution of REDDIG II implementation process.

3. **Action suggested**

3.1 The Meeting is invited to:

a) Take note of the information that has been presented;
b) Review the activities of the SAM ATN Infrastructure Project that are described in Section 2 of this working paper, including Appendices A, B, C and D, in the light of the adjustments made to the original CAR/SAM D1 Project Documents as regards REDDIG II implementation; and
c) Examine the progress made with the deliverables of Project 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

- - - - - - - - -

APPENDIX B

PROJECT ATN ARCHITECTURE IN THE SAM REGION

SAM Region	**PROJECT DESRICPTION (PD)**	**PD N° D1**	
Programme	**Project Title**	**Starting Date**	**Ending Date**
Ground-ground and Air-ground Telecommunications Infrastructure (*Programme Coordinator: Onofrio Smarrelli)*	ATN Architecture in the SAM Region *Project Coordinator: Athayde Licério Vieira Frauche (Brazil)* *Contributing experts: Omar Gouarnalusse (Argentina), Michel Areno (France), Jose Luis Paredes (Peru), Jesús Bolívar (Venezuela), Christian Amaris de León (Colombia) and Hernando Lara (Bolivia)*	March 2010	March 2015
Objective	Study and implementation of optimum architecture for an IP protocol backbone network (REDDIG II) for the SAM Region		
Scope	Study and implementation of an IP backbone network for the SAM Region, including an optimum configuration and considering, among other deliverables, the following: • Technical review of the regional telecommunications networks (ground, satellite or mixed) for the implementation of ATN under a cost-benefit analysis • Holding of trials to determine the ATN bandwidth necessary to support ground applications • IP addressing scheme (IPv4 and IPv6) and analysis of the data communications infrastructure in support to ATS operational requirements in the short, medium and long term • Support in the bidding process by TCB (Montreal) and in the implementation of the IP backbone network for the SAM Region • Implementation of REDDIG II		
Metrics	• Percentage concluded of the study for an IP backbone network for the SAM Region • Drafting of technical specifications for REDDIG II • REDDIG II implementation percentage		
Strategy	• All tasks will be conducted by experts nominated by States of the SAM Region members of the project *ATN Architecture in the SAM Region*, under management of the project coordinator, in coordination with the programme coordinator. Communications among project members, as well as between the project coordinator and programme coordinator, shall be carried out through teleconferences and the Internet. In addition, the programme coordinator, together with the project coordinator and the contributing experts, can convene at SAM/IG implementation meetings • Once studies are completed and REDDIG II is implemented, the results will be submitted to the ICAO programme coordinator as a final consolidated document for its analysis, review, approval and presentation at the GREPECAS PPRC		

Goals	•
Justification	• A study on an ATN IP backbone network for the SAM Region will permit defining the optimum communications network architecture for said Region, currently mainly based on REDDIG (satellite digital communications network). • To arrive to the conclusion on the better network infrastructure, the determining of the current applications demand in terms of band width is considered very important. In this respect, States are carrying out tests, mainly AMHS, to determine the associated space segment. The action is considered as the beginning of the network's cost-benefit relationship research. • In addition, the increasing band width requirements for new services such as automation, surveillance, ATFM and meteorology. Also, a close relationship with the other programmes and their respective projects is necessary, with the aim of collecting the operational requirements demanded by the mentioned applications and their respective tentative implementation dates • After developing all tasks necessary for determining the better network infrastructure, technical specifications for the purchasing and implementation of the SAM backbone network (REDDIG II) will be drafted • This project ends once the SAM IP backbone network (REDDIG II) is implemented • This project contributes to the implementation of SAM PFF CNS 01, CNS04, ATM 05, ATM 06, MET 04 and AIM 02 of the *Air Navigation System Performance-Based Implementation Plan for the SAM Region (SAM PBIP)*
Related Projects	• Air Navigation Systems in Support of PBN • Automation • Improve ATM Situational Awareness • Implementation of the ICAO New Flight Plan Format • ATN Ground-ground and Air-ground Applications

Project Deliverables	Relationship with Performance Based Regional Plan (PFF)	Responsible	Status of Implementation[1]	Delivery Date	Remarks
Analysis of the current SAM communications network (REDDIG)	PFF SAM CNS01	REDDIG Administration, Project Coordinator and Omar Gouarnalusse (Argentina)		August 2010	Completed
Analysis of the current MEVA II/ REDDIG interconnection	PFF SAM CNS01	REDDIG Administration		June 2011	Completed
Analysis of the AMHS band width impact on the current REDDIG satellite infrastructure	PFF SAM CNS01	Project Coordinator and Omar Gouarnalusse (Argentina)		September 2010	Completed
Long term applications requirements in the SAM Region	PFF SAM CNS01 PFF SAM CNS 04 PFF SAM MET 04 PFFs SAM ATM 05 and 06 PFF SAM AIM 02	ICAO		September 2010	Completed

[1] ***Gray**: Activity has not started*
***Green**: Activity has or will deliver planned milestone as scheduled*
***Yellow**: Activity is behind schedule on milestone, but still within acceptable parameters to deliver milestone on time*
***Red**: Activity has failed to deliver milestone on time, mitigation measures need to be identified and implemented*

Project Deliverables	Relationship with Performance Based Regional Plan (PFF)	Responsible	Status of Implementation[1]	Delivery Date	Remarks
Comparative study on satellite, ground and mixed (satellite and ground) IP based network models for the SAM Region	PFF SAM CNS 01	Project Coordinator, Omar Gouarnalusse (Argentina) and REDDIG Administration		October 2010	Completed Approved by REDDIG Member States
Definition of ATN IP network infrastructure model for the SAM Region	PFF SAM CNS 01	Project Coordinator, Omar Gouarnalusse (Argentina) and REDDIG Administration		October 2010	Completed Approved by REDDIG Member States
Completion of IPv4 addressing plan for the SAM Region	PFF SAM CNS 01	Project Coordinator and Omar Gouarnalusse (Argentina)		August 2010	Completed The addressing scheme was approved through GREPECAS Conclusion 16/37
Drafting of technical specifications for REDDIG II	PFF SAM CNS01 PFF SAM CNS 04 PFF SAM MET 04 PFFs SAM ATM 05 and 06 PFF SAM AIM 02	Project Coordinator, Omar Gouarnalusse (Argentina) and REDDIG Administration		August 2011	Completed and approved by REDDIG Member States
Drafting of safety guidelines for REDDIG	PFF SAM CNS 01	REDDIG Administration		May 2012	Completed for presentation at SAM/IG/11 meeting

Project Deliverables	Relationship with Performance Based Regional Plan (PFF)	Responsible	Status of Implementation[1]	Delivery Date	Remarks
Drafting of IP Routing Policy	PFF SAM CNS 01	Project Coordinator		October 2013	Completed for presentation at SAM/IG/11 meeting
Support in the bidding process and in the offer evaluation		Project Coordinator, Omar Gouarnalusse (Argentina), Michel Areno (France), José Luis Paredes (Peru), Jesus Bolívar (Venezuela), Hernando Lara (Bolivia), Christian Amaris (Colombia) and REDDIG Administration		April 2012	Completed. The bidding was conducted by TCB, under coordination with the ICAO Regional office. The evaluation process will count with the REDDIG Administration and CNS experts selected by the REDDIG Member States
Support in the implementation of REDDIG II		REDDIG Administration, Project Coordinator and Omar Gouarnalusse (Argentina) REDDIG II focal points		November 2013-March 2015	This activity is scheduled to start at the end of 2013
Monitor the ATN architecture project activities in the SAM Region		ICAO		March 2010-December 2015	
Resources necessary	Economic contribution necessary for the implementation of 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.

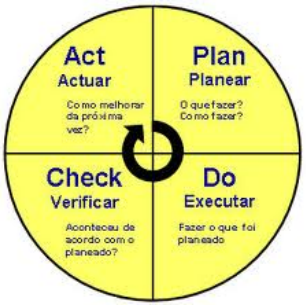


Fig. 1 – El Ciclo PDCA

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.

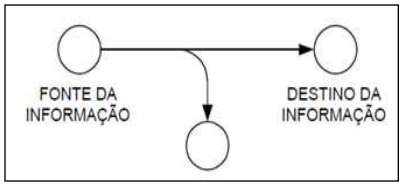
- **Incidente:** una o más serie de eventos de seguridad de la información no deseados o no esperados, que tengan una gran probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **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:

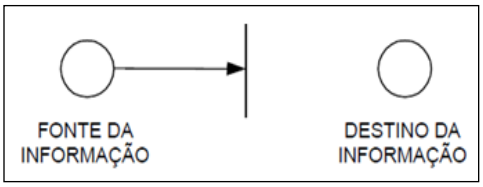
- **Confidencialidad:** capacidad de un sistema de impedir que usuarios no autorizados tengan acceso a determinada información que fue delegada a solamente usuarios autorizados. La pérdida de la confidencialidad puede ser obtenida por medio de la interceptación. La figura siguiente ilustra dicha situación:



Fuente: SANTOS (2011)

Fig. 2– Pérdida de la Confidencialidad

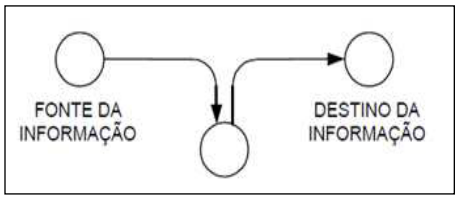
- **Disponibilidad:** indica la cantidad de veces que el sistema cumplió una tarea solicitada sin fallas internas, para un número de veces en que fue solicitado a hacer la tarea. La pérdida de la disponibilidad pode ocurrir por media de una interrupción.



Fuente: SANTOS (2011)

Fig. 3 – Pérdida de la Disponibilidad

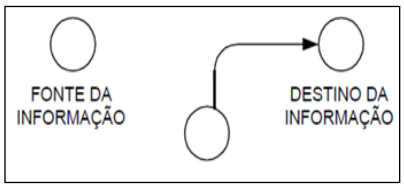
- **Integridad:** atributo de seguridad que indica si una información puede ser alterada solamente de forma autorizada. La pérdida de la integridad puede ocurrir por modificación.



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.

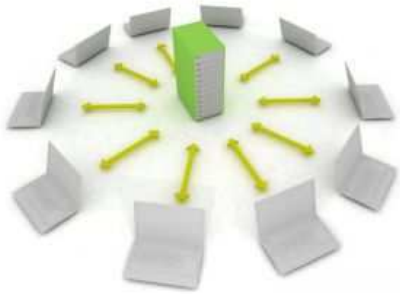


Fig 6 – La automatización multiplica el poder del atacante

- **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:

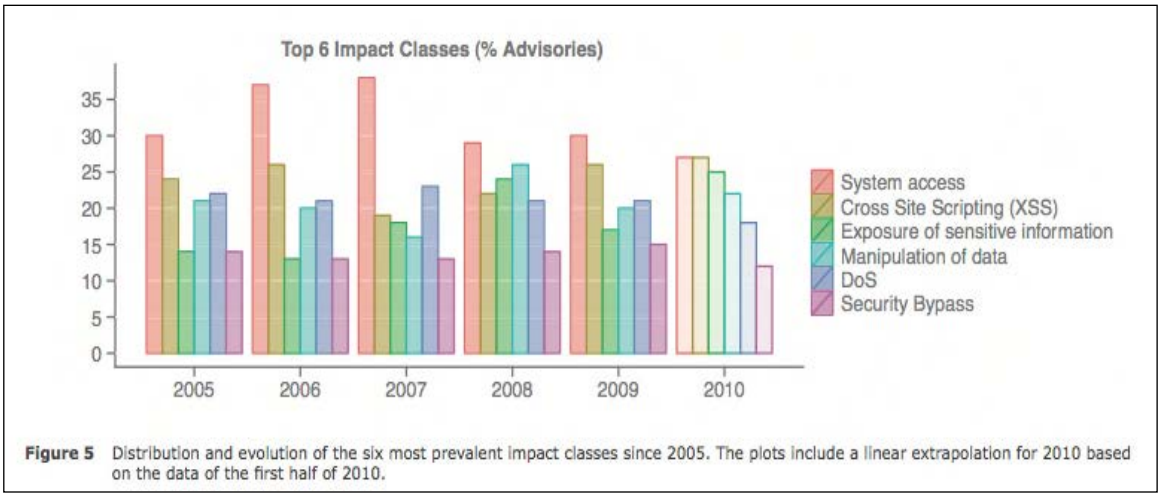


Figure 5 Distribution and evolution of the six most prevalent impact classes since 2005. The plots include a linear extrapolation for 2010 based on the data of the first half of 2010.

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:

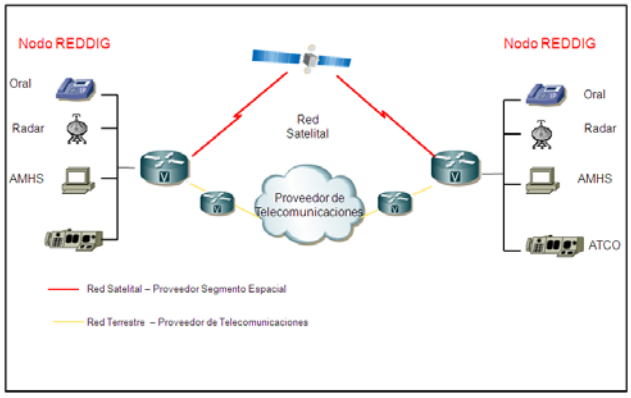


Fig 8 – La REDDIG II – Topología

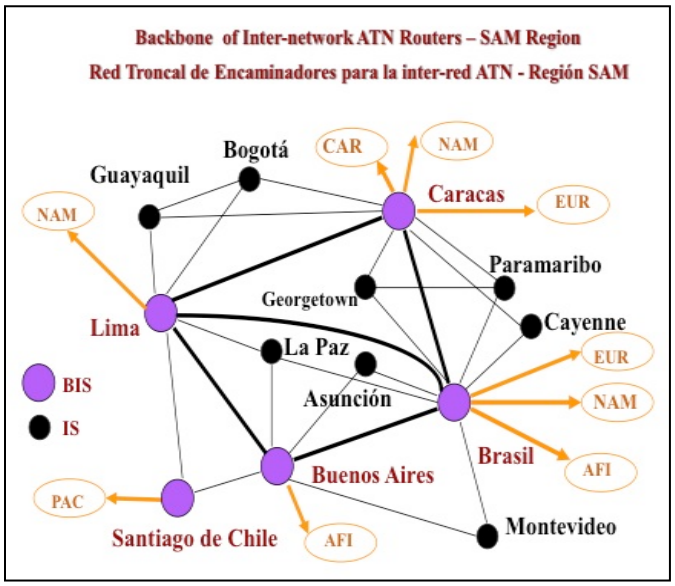


Fig 9 – La REDDIG II – Puntos de Interconexión

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:

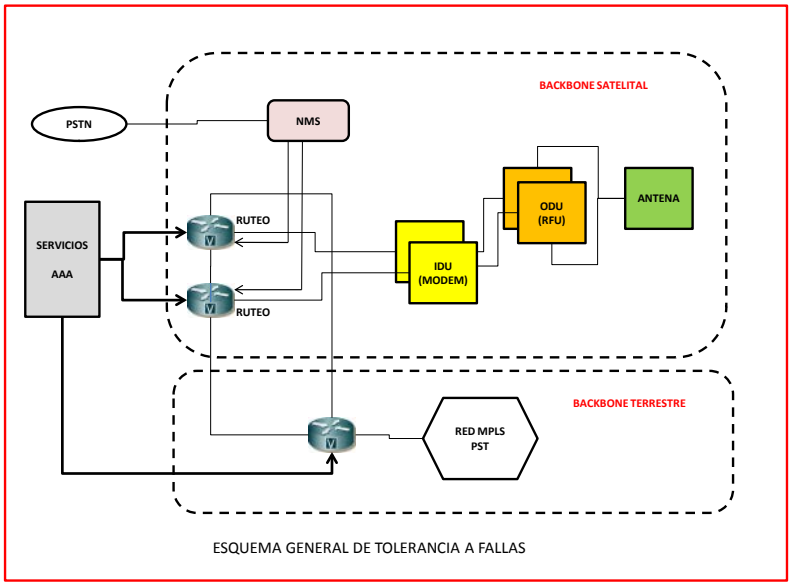


Fig 10 – Tolerancia a Fallas

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:

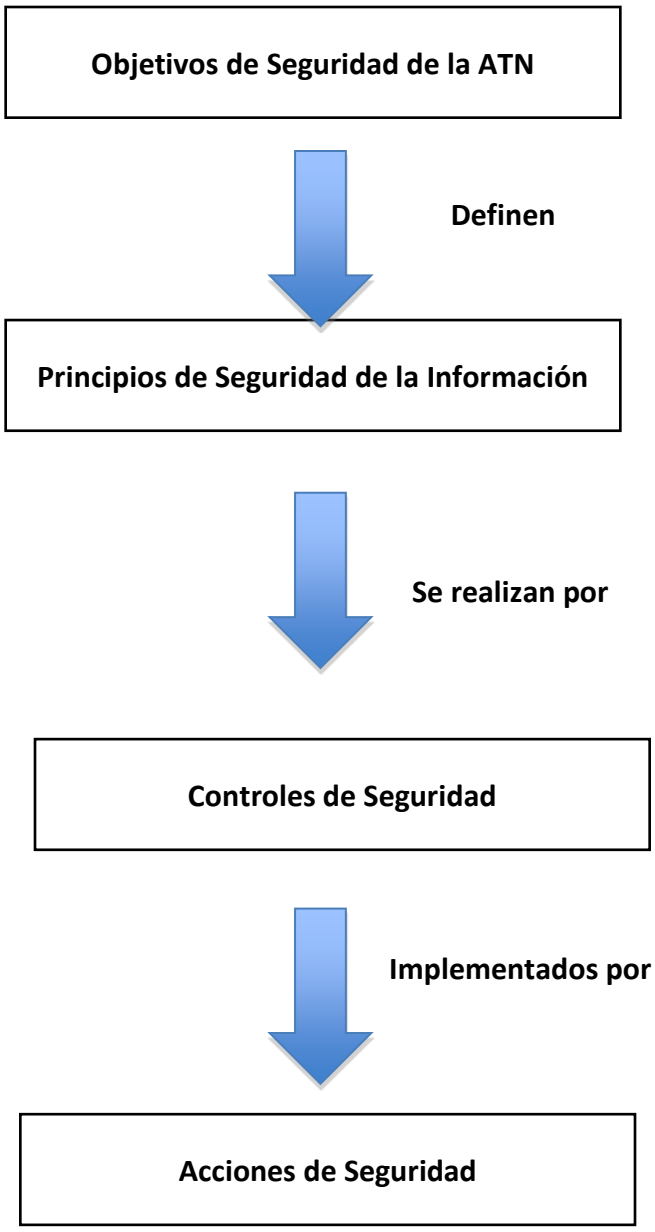


Fig 11– Objetivos de Seguridad

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:

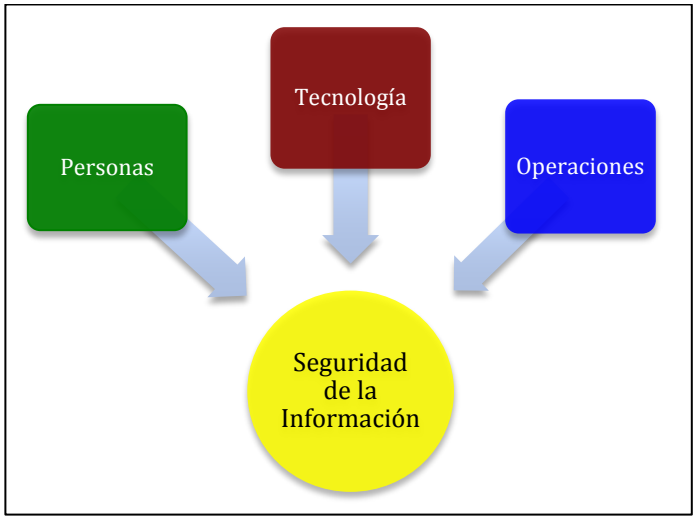


Fig 12– Elementos de la Seguridad

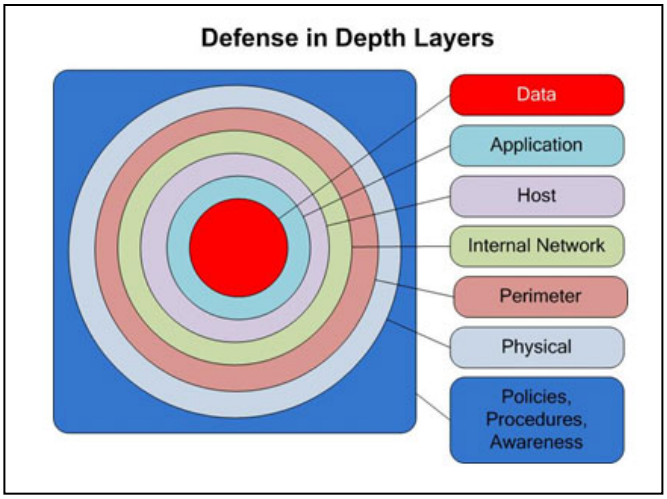
a) **Personas:** Involucra los aspectos relacionados al establecimiento de políticas y procedimientos para la definición de reglas y responsabilidades; la realización de entrenamientos para la creación de una mentalidad de seguridad tanto del personal técnico cuanto de los operadores, así como medidas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

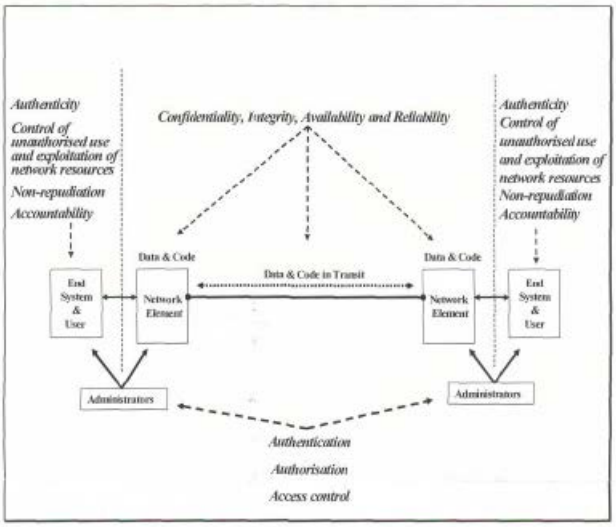
3.5) Protección de las Instalaciones: garantiza que los ambientes poseen acceso controlado.

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.

APPENDIX D

AERONAUTICAL TELECOMMUNICATION NETWORK OF THE SAM REGION (REDDIG II)

ROUTING POLICY FOR THE SAM REGION

TABLE OF CONTENTS

REFERENCES

- Doc 9855 – Guidelines on the Use of the Public Internet for Aeronautical Applications
- Doc 9896 – Manual for the Aeronautical Telecommunication Network (ATN) using IPS Standards and Protocols
- Guidance for the Implementation of National Digital Networks that Use the IP Protocol to Support Current and Future Aeronautical Applications (SAM Region)
- Air Navigation Plan for the Caribbean and South American Regions – FASID – Tables CNS1A and CNS1C
- SAM Regional IP Addressing Plan
- RFC 4271 –BGP-4 Specifications
- RFC 4360 – BGP Extended Communities Attribute
- CNS Table 1Ba – Regional Router Plan / SAM Region

GLOSSARY OF ACRONYMS

- AMHS ATS Message Handling System
- ANSP Air Navigation Service Provider
- ARIN American Registry for Internet Numbers
- ATN Aeronautical Telecommunication Network
- BER Bit Error Rate
- BGP Border Gateway Protocol
- EGP Exterior Gateway Protocol
- ES End System
- EUR/NAT European and North Atlantic Region
- FASID Facilities and Services Implementation Document
- GREPECAS Caribbean/South American Regional Planning and Implementation Group
- IANA Internet Assigned Numbers Authority
- IGP Interior Gateway Protocol
- IPS Internet Protocol Suite
- ISO International Organization for Standardization
- MPLS Multiprotocol Label Switching
- OSI Open System Interconnection
- OSPF Open Shortest Path First
- PBR Policy-Based Routing
- QoS Quality of Service
- REDDIG South American Digital Network
- 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 Transmission Control Protocol
- TSP Telecommunication Service Provider
- VoIP Voice Over IP
- VPN Virtual Private Network
- UDP User Datagram Protocol
- WACAF Western and Central African Region
- WAN Wide Area Network

DEFINITIONS

The following definitions are applicable for purposes of this document:

Bandwidth: maximum packet rate from a dedicated connection port, expressed in kbits/s or Mbits/s.

REDDIG II Applications: services to be provided by REDDIG II as defined in the main body of the document.

Physical Layer (Level 1): The physical layer defines the technical characteristics of the system's electrical and optical (physical) devices. It contains the cabling or other communication channels that communicate directly with the network interface controller. Accordingly, it is concerned with allowing for simple, reliable communication, in most cases with basic error control:

Layer functions:

- It moves bits (or bytes, in accordance with the transmission unit) through a transmission medium;
- It defines the electrical and mechanical characteristics of the medium, the bit transfer rate, voltages, etc.
- It executes or controls the data transmission volume and rate.

The physical layer is not responsible for dealing with issues like transmission errors, which are addressed by other layers of the OSI model.

Network Layer (Level 3): This is the network layer responsible for addressing network packets, also known as datagrams, by associating logical addresses (IP) with physical addresses, so that network packets reach their destination properly. This layer also determines the routes packets will take to reach their destination, based on elements like network traffic conditions and priorities.

This layer is used when the network has more than one segment and, as a result, a packet can take more than one path from origin to destination.

Layer functions:

- To move packets from their original source to their destination over one or more links.
- To define how network devices discover each other and how packets are routed to their final destination.

Availability: performance measurement parameter consisting of the percentage of time the PP/node (as the case may be) is operational within a specified service provision time period.

Router: equipment endowed with IP processing capacity for the purpose of determining the routes over which packets must be routed.

Inter-regional Routers: this is equipment that interconnects the routers with other ICAO Regions. In practical terms, these are routers belonging to a State AS that link up the Region with the EUR/NAT and WACAF Regions by means of the CAFSAT network, with the CAR Region via the interconnection of the MEVA II and REDDIG networks and with the APAC Region through contractual Telecommunication Service Providers (TSP).

Intra-regional Routers: for purposes of this document, these are the routers used for communication within the SAM Region.

Inter-domain routing*:* Data packet routing by an AS with different administrative authorities.

Intra-domain routing: Data packet routing by a single AS.

Path Vector Protocol: Protocol used for routing information interchanges among different Autonomous Systems (AS), as in the case of BGP-4. The term "path vector" bears in mind that BGP-4 routing information has a sequence of AS numbers that indicate the path taken by a given route.

Routing Protocol: that used among routers to exchange information about the network topology. It permits the updating of the routing table used by routers to choose the best path for sending a packet between network segments.

Internet Gateway Protocol (IGP): routing protocol that exchanges information within an Autonomous System (AS); for example: RIP (Routing Information Protocol) and OSPF (Open Shortest Path First).

Exterior Gateway Protocol (EGP): routing protocol that interconnects different Autonomous Systems (AS). BGP is a type of EGP.

REDDIG II Member States' Network: set of interconnected equipment, cables and software belonging to those represented by the Contracting Party.

Delay (or latency): service performance measurement parameter consisting of the average transit time of a 64-byte packet between two of the Contracting Party's PPs.

Delay: in this document, delay is understood to be an inherent characteristic of statistical and deterministic networks that consists of the end-to-end application propagation time.

Physical security of the data: for purposes of this tender, physical security is understood to mean protection against unauthorized access to the successful bidder's communication circuits and devices. Inclusion of cryptography in the communication circuits by the successful bidder is not part of this process.

Autonomous System: set of systems administered by a single administrative authority following an internal policy established by the authority. In the SAM Region, this could be a State or an Air Navigation Service Provider (ANSP). Autonomous Systems can also be called Routing Domain systems.

1. INTRODUCTION

1.1 Background

1.1.1 When referring to the Aeronautical Telecommunication Network (ATN), it is necessary to return to the year 1989, when the Secondary Surveillance Radar Improvements Panel (SICASP), at the instruction of the Special Committee on Future Air Navigation Systems (FANS), started developing documents for voice and data interchanges via different digital communication platforms.

1.1.2 To ensure the success of the SICASP's endeavours, the FANS Committee recommended adoption of open protocol principles--International Organization for Standardization's (ISO) Open Systems Interconnection (OSI)--, so as to provide for the interoperability of existing network platforms.

1.1.3 It is important to stress that many ICAO provisions were developed, insofar as air-ground and ground-ground applications are concerned, based on the OSI platform. Furthermore, although ICAO Member States gave significant support to the use of the OSI topology, the industry promoted equipment based on the Internet Protocol Suite (IPS) platform.

1.1.4 The International Civil Aviation Organization (ICAO) Air Navigation Committee (ANC) created the Aeronautical Communications Panel (ACP) in 2003 by combining the Aeronautical Mobile Communications Panel (AMCP) and the Aeronautical Telecommunication Network Panel (ATNP).

1.1.5 One of the main recommendations made, from the very beginning of the Panel's activities, was that ICAO should concern itself with developing ATN documentation based on TCP/IP protocols.

1.1.6 The ACP Working Group I (IP) (WG-I) was set up to effectively support development of the new provisions. Among its functions are security matters and the convergence and adaptation of ATN/OSI provisions for ATN/IP. It also deals with the development of documents for new applications directly based on ATN/IP.

1.1.7 The Caribbean/South American Regional Planning and Implementation Group (GREPECAS), through the former CNS/ATM Subgroup, already had the ATN Task Force (ATN/TF) operating to develop guidance material based on TCP/IP protocols for the CAR/SAM States.

1.1.8 One of the ATN/TF deliverables was the preparation of an addressing system based on version 4 of the IP protocol (IPv4) for all CAR/SAM States; it is currently under implementation in those Regions, as reflected in **Appendix A** to this document, insofar as the SAM States are concerned.

1.1.9 The CAR/SAM addressing plan was presented at the First Meeting of the ACP Working Group of the Whole, held in September 2008. Emphasis was placed on the fact that the ultimate purpose was to implement IPv6, but that IPv4 would be used as a way to further implementation of ATN applications in the CAR and SAM Regions, especially of the ATS Message Handling System (AMHS).

1.1.10 It should be stressed that the provisions being developed by ICAO Headquarters in Montreal are based on IPv6. Nevertheless, ICAO itself is seeking ways to make the acquisition of address blocks viable for use in all Regions.

1.1.11 It is also noted that the routers implemented in the SAM States that need to exchange data with other Regions are dual stack, meaning that they can handle IPv4 or IPv6 packets.

1.1.12 Once ICAO and the Internet Assigned Numbers Authority (IANA), responsible for worldwide provision of addresses, and its regional offices, called Regional Internet Registry (RIR) are able to obtain IP addressing blocks, the conditions will be favourable for implementation of the new IP addressing system for the SAM Region through a transition plan to be developed in due time.

1.2 Document Organization

1.2.1 The initial part of this document consists of References, the Glossary of Acronyms and Definitions that serve as a guide to the entire document, in view of the large amount of information this policy encompasses. Section 1.1 of the Background, in Chapter 1, supplements this segment with a historical account of ICAO activities to promote ATN/IPS use in communication networks.

1.2.2 Chapter 2 contains a general description of the SAM Regional IPv4 addressing plan, developed as a transitional phase toward the future implementation of the IPv6 addressing system.

1.2.3 Considering that the core IP structure links up a series of Autonomous Systems (AS) of different States and other Regions, Chapter 3 sets out the main concepts of the Border Gateway Protocol (BGP) in the version being currently implemented (BGP-4).

1.2.4 To conclude, Chapter 4 covers the use of BGP-4 routing as specifically applied to the South American Region and its interconnection with other ICAO Regions.

2. THE SAM ATN

2.1 SAM IPv4 Addressing Plan

2.1.1 With a view to the adoption of the IP addressing plan, the ATN/TF of the former CNS/ATM conducted a study contemplating the application of IPv4 in all ICAO Regions. Accordingly, an analysis was conducted of the number of States/Territories per Region, the number of addresses that each State/Territory could use and the number of addresses reserved for the interconnection of States/Territories.

2.1.2 It should be noted, first, that in order for the networks assigned to each State/Territory to be private networks (RFC 1918), the first of the four bytes that make up the assigned addresses will always have a decimal value equal to 10. The three other bytes will be used to hierarchically distribute the address blocks corresponding to each State.

2.1.3 The conclusions of that study were that:

a) The first four bits of the second byte (4 bits) would be used to identify the Regions into which the world's States/Territories are grouped:
   - 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) Seven bits would be used at the State/Territorial level. This means that it is possible to have up to 128 States per Region. To give a real example, even the most numerous region, EUR/NAT, has only 53 States/Territories; this would leave many numbers vacant.

c) The last five bits of the third byte, and the eight bits comprising the fourth byte (13 bits), would be reserved for the hosts. This would make it possible to address 8,190 hosts per State/Territory. It should be noted that this figure was considered because of current requirements and possible future applications to be implemented, mainly in the more developed States.

2.1.4 In the light of the foregoing, the scheme adopted has the format set out in Table 1:

IPv4 Address							
10		Region	State/Territory		Host		
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	
1st Byte	.	2nd Byte	.	3rd Byte	.	4th Byte	

Table 1: IPv4 Addressing Scheme

2.1.5 In summary, the proposed assignment scheme could cover:

a) 16 Regions.

b) 128 States/Territories per Region.
c) 8,190 hosts per State/Territory.

2.1.6 The corresponding addresses have been assigned to each SAM State/Territory, bearing in mind the contents of the table attached as Appendix A. In said table, the last available network is labeled “RESERVED,” so that it can be used for inter- and intra-regional links.

2.1.7 Although planned for possible application in all Regions, the IP addressing plan was only adopted and is being used massively by the SAM Region, while ICAO and IANA are working to obtain IPv6 addressing blocks for all Regions.

2.1.8 REDDIG is the communication platform used in South America. It links up State routers for transmission of IP applications based on the addressing plan that has been developed. The characteristics of the existing REDDIG and the data for modernizing its infrastructure are to be found in **Appendix B**.

.

3. THE BASICS OF ROUTING BY DOMAIN

3.1 BGP Protocol

3.1.1 The BGP protocol, in its most recent version (4), is a path vector protocol used for the exchange of routing information between different autonomous systems.

3.1.2 The main features of BGP-4 are:

a) Origin: reports the origin of the BGP-4 route. If generated by an Internet gateway protocol (IGP), the metric is so announced in the BGP route (the router always chooses the path with the lowest metric generated by the IGP).
b) AS-Path: indicates the ASs traversed by the route. The BGP-4 databank keeps all path alternatives, but chooses the one that traverses the smallest number of ASs.
c) Next-hop: indicates the interface of the originating router where the BGP-4 route was announced. All BGP-4 routers will route the route data if there is connectivity with the IP address described in the NEXT-HOP attribute.
d) Local-preference: this attribute has a local significance and ensures that BGP-4 selects the best exit path based on the available WAN links.
e) Multi-exit-discriminator*:* defines the path along which neighbouring BGP-4 routers will send packets addressed to their internal networks.

3.1.3 Unlike other interior routing protocols that use the User Datagram Protocol (UDP), BGP-4 employs the Transmission Control Protocol (TCP) as its transport protocol. This means that the circuit is connection-oriented and guarantees reliable packet delivery. As a result, BGP-4 has no need for relay mechanisms, inasmuch as the TCP fulfills that function.

3.1.4 In order for BGP-4 to establish router adjacency, the neighbourhood must be explicitly configured. In that way, relationships are formed among routers configured as neighbours, with the result that the exchange of keepalive messages at regular time intervals reveals the conditions of each.

3.1.5 Once the adjacencies have been established, routers send neighbours the BGP-4 routes in their routing tables, so that those neighbours will be able to successfully establish the referred adjacencies. Each router adds to its BGP-4 topology databases all routes learned from neighbours.

3.1.6 The BGP protocol was originally used for routing between different ASs. Nonetheless, it can be used in routers belonging to the same AS and in that case is known as IBGP. Figure 4 illustrates the case in which routers B, C and D of AS 65000 are considered IBGP neighbours.

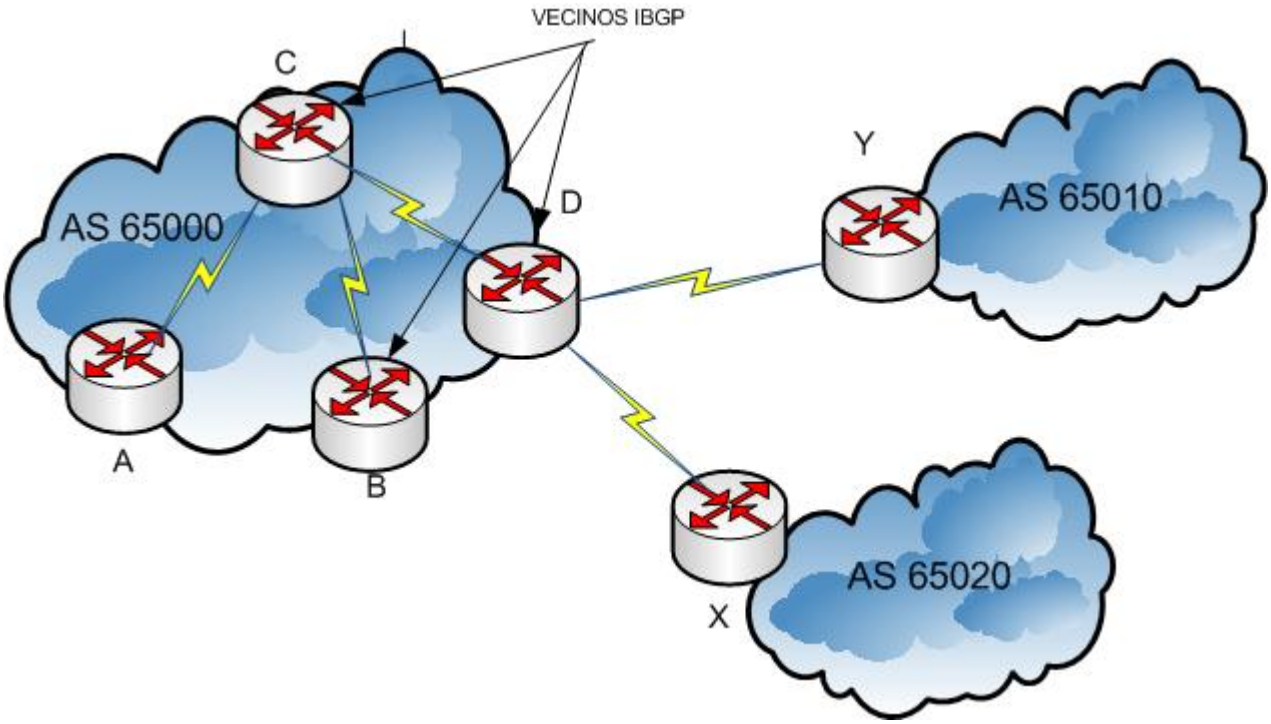


Figure 4: Internal BGP Neighbouring Routers

3.1.7 Figure 5 shows the neighbourhood between routers belonging to ASs with different administrative domains. In this case, D and Y are exterior neighbours and the same thing holds true with routers B and X.

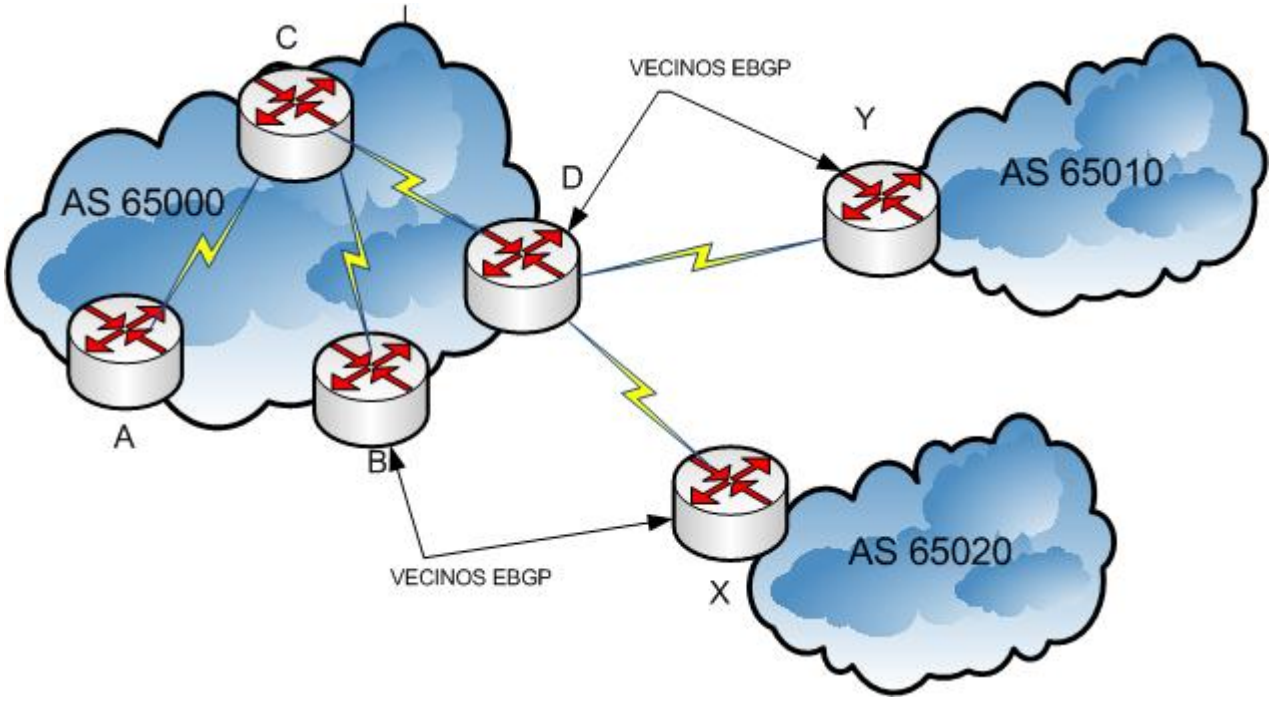


Figure 5: Exterior BGP Neighbouring Routers

3.2 BGP Autonomous Systems

3.2.1 As previously defined, an Autonomous System represents a collection of networks and their routers under a single administration. That said, the main objective of BGP-4 is to guarantee the interchange of routing information between different ASs.

3.2.2 Autonomous systems can use more than one IGP, resulting in a series of different metrics associated with each of the interior protocols in the BGP-4 AS exit router. Nonetheless, the most important characteristic of the AS is that, to other BGP-4 routers, there would seem to be only one IGP within the AS and external routers will easily know how to reach the connected internal destinations.

3.2.3 The Internet Assigned Numbers Authority (IANA) is the organization responsible for allocating AS numbers. The American Registry for Internet Numbers (ARIN) is the IANA Regional Office (RIR Regional Internet Registry) that performs that task specifically in the Americas. AS numbers range from 1 to 65535, with those in the range of 64512 to 65535 being reserved for private use.

3.3 BGP-4 Routing

3.3.1 An interior routing protocol seeks the fastest path between one point on a corporate system and another, based on metrics.

3.3.2 BGP-4, which is an exterior routing protocol, uses a different mechanism from that employed by IGPs. BGP is a policy-based routing protocol (PBR) that allows for traffic flow control over the network by using, *inter alia*, the attributes defined in 3.1. This enables the network administration to handle preferential paths.

3.3.3 BGP-4 is known as a path vector, for it takes into account that BGP-4 routing information has a sequence of AS numbers, indicating the path crossed by a given route and the routers announce the hop-by-hop path to the destination AS. Figure 6 contains a simple example of BGP routing.

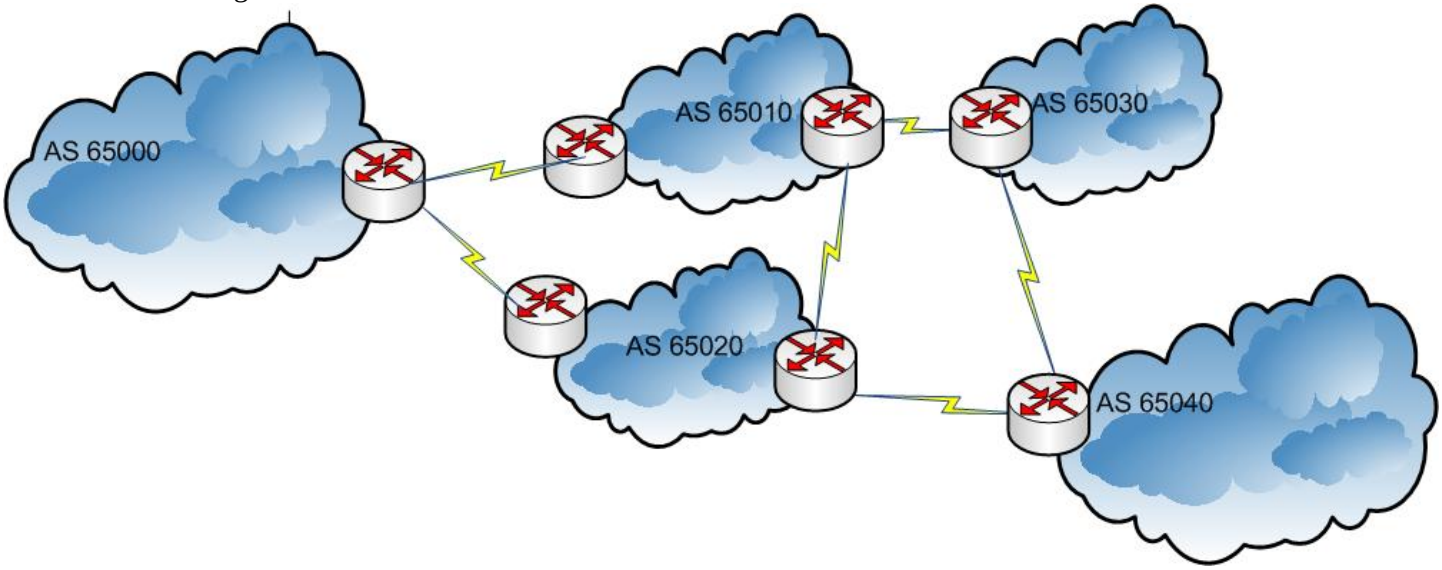


Figure 6: Routing between different ASs

3.3.4 According to Figure 6, it may be concluded that the following paths can be taken for AS 65000 to reach AS 65040 networks:

a) 65020-65040;

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

3.3.5 BGP-4 routers choose the path neighbours should use to send their packets. Accordingly, the most that AS 65000, which is the origin, can do is to decide which AS to traverse in its exit.

3.3.6 By way of example, if the AS 65000 exit router chooses to reach 65040 via AS 65020, the path to be taken from AS 65020 onward is internally chosen by the latter. In the given example, AS 65020 informs AS 65000 that the path to reach AS 65040 is 65020-65040, even if there is another path available, which, however, AS 65020 does not disclose to AS 65000, unless there is a problem with the main path.

4. ROUTINGS THROUGH SAM DOMAINS

4.1 Routing Domains

4.1.1 Private AS numbers, defined in Doc 9896 and described in **Appendix E**, are recommended for use in the SAM Region as a means for utilizing the BGP-4 routing protocol and safely guaranteeing the isolation of autonomous systems.

Note: The BGP-4 protocol makes it possible to adopt a series of optional and extension parameters. It is accordingly recommended that use of those attributes be defined in the future, in order to make the most of the protocol resources. As BGP-4 was originally developed for IPv4 use, however, its initial application will create no major problems.

4.1.2 From an administrative point of view, the SAM ATN/IPS consists of a series of administrative domains that can be represented, in the SAM Region, by a State or by a State's Air Navigation Service Provider (ANSP).

4.1.3 In terms of technical routing concepts, the interconnection of administrative domains rests on the exchange of information between different autonomous systems, each with a series of IP addresses. SAM ASs are interconnected by means of the REDDIG platform and, in the future, will be by REDDIG II.

4.1.4 Appendix B shows the basic characteristics of the existing REDDIG platform, as well as those of the future REDDIG II. The aforementioned architecture supports the existing and future services that are or will be instituted in the SAM Region. **Appendix C** describes the applications that should be transmitted via the cited communication network.

4.2 Domain Routing in the SAM Region

4.2.1 Appendix A shows the assignment of IP address ranges to be followed by the Aeronautical Authorities of each State in the Region in the national routers that link up with REDDIG. It represents the SAM Region's existing IP addressing plan.

4.2.2 As mentioned earlier, when ICAO, acting in favour of the States, together with IANA, acquires the IPv6 address blocks, it will be necessary to prepare a new SAM IP addressing plan. Furthermore, the routers used in the SAM Region are dual stack with regard to the possibility of routing inter-regional packets in which the destination is already using IPv6. Figure 7 illustrates that possibility for AMHS application.

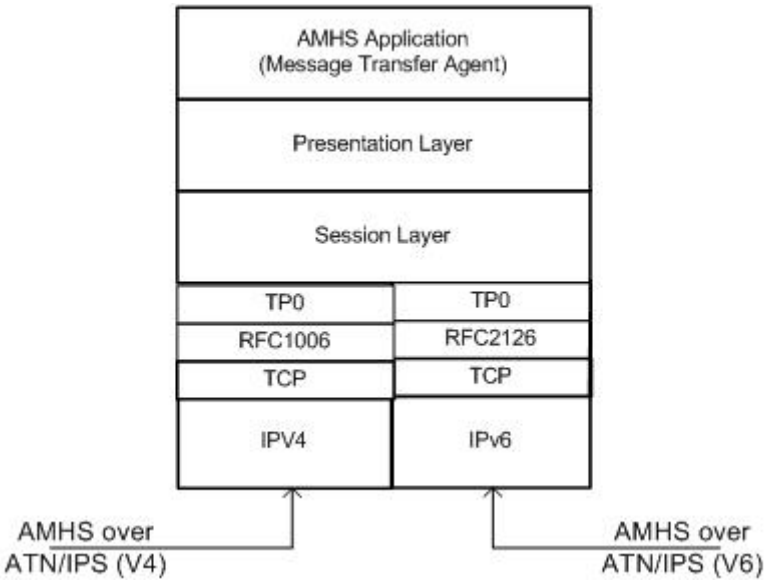


Figure 7: Translation of IPV4/IPv6 Addresses

4.2.3 The REDDIG, it is known, is used to link up the ASs of different States in such a way that one end system (ES) can reach another in a different State. Intra-regional routers are used for that purpose, as shown in Figure 8.

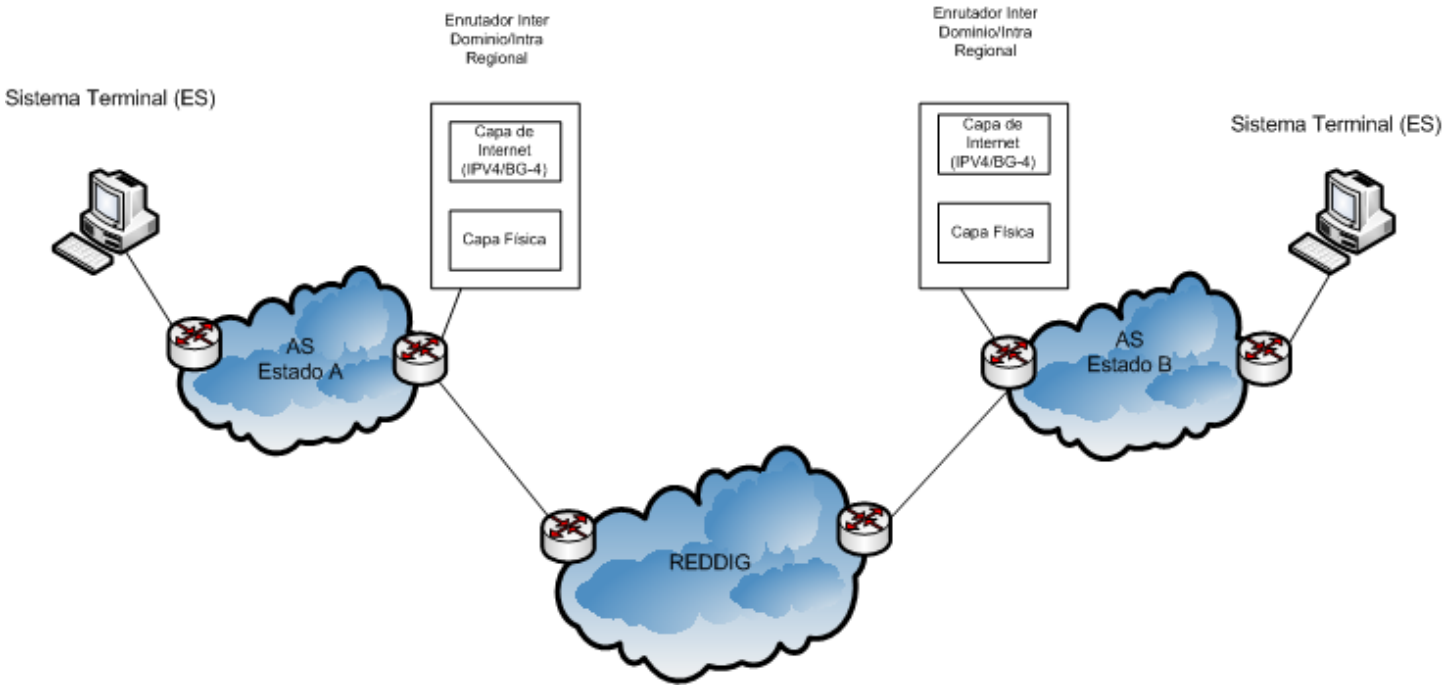


Figure 8: SAM Intra-Regional Routing

4.2.4 Figure 9 presents the basic routing topology for the SAM Region based on the requirements present in the FASID and in the Table, together with the future requirements as presented in Appendix C. Inasmuch as REDDIG II is a core IP network, the services will be transmitted from origin to destination seamlessly, using end system IP addresses and numbers of the ASs involved.

4.2.5 With the use of BGP-4, the concepts presented in Section 3.3, Routing with BGP-4, will logically have to be considered, inasmuch as it is not the origin router that chooses the path to the destination, but the router (Next hop).

4.2.6 Consequently, Figure 9 reflects the following SAM Region routings, bearing in mind the origin and destination of the applications, shown in different colors, as well as CNS Table IBa (Regional Router Plan) that appears in **Appendix D**.

a) In purple: intra-regional links using inter-domain routers (AS) of the States linked up by REDDIG;
b) In red: inter-regional links using the MEVA II/REDDIG interconnection; and
c) In black: inter-regional links in which the routers belonging to a SAM AS reach their destination via a PST or through interconnection with the CAFSAT network.

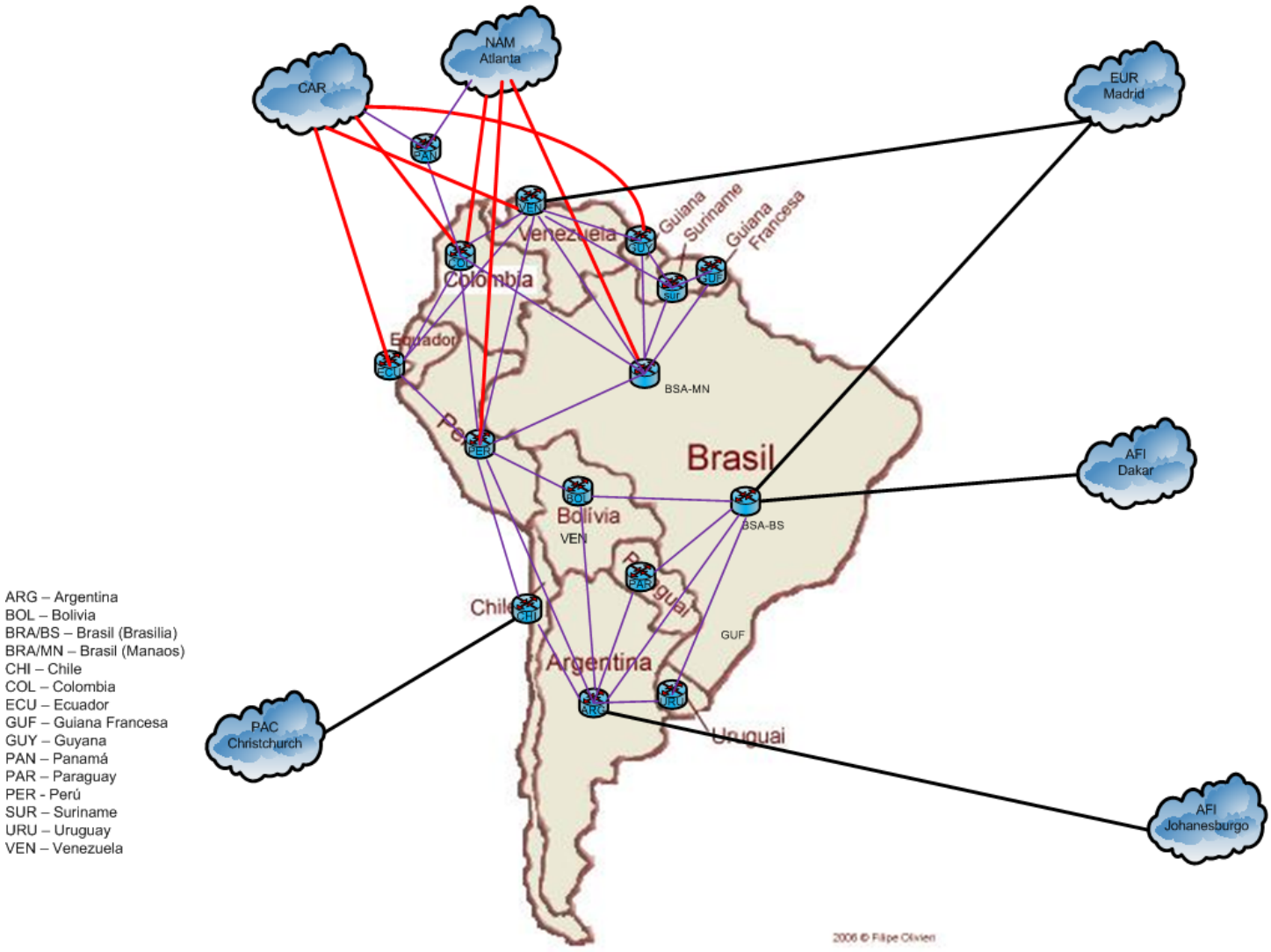


Figure 9: Basic SAM Routing Topology

4.2.7 The following BGP-4 routing policies should be observed in the SAM Region:

a) If a router has several possible paths to reach its destination, it should choose the one crossing the fewest ASs.

Note: REDDIG employs the satellite network, which operates as a deterministic network with a single hop. In the future, REDDIG II will use the satellite network as its main network, but the ground network, supplied by a PST, will have an infrastructure that could involve several different ASs.

b) All routers in the SAM Region (REDDIG and States) that are configured using the BGP-4 protocol shall do their authentication with their configured neighbours.
c) In order to reduce the size of routing tables, SAM BGP-4 routers should be configured to accept route aggregation.
d) BGP-4 routers belonging to an administrative domain should be configured to receive the aggregation of all internal AS routes.
e) The Local-Preference attribute should be configured in such a way that the BGP-4 router will choose the best exit path when the router is connected to more than one WAN.

4.2.8 In addition to the aforementioned policies, each State or ANSP has its own policies that will supplement those covered in this document.

APPENDIX 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

Assignment of networks by State/Territory

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	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 0 1 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-			-	
				-	-			-	
				Ultima	10 . 1 . 127 . 254	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 0 1 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	13	Guyana Francesa (France)	10.1.128.0 / 19	Primera	10 . 1 . 128 . 1	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 0 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-			-	
				-	-			-	
				Ultima	10 . 1 . 159 . 254	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 0 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	-	VACANTE	10.1.160.0 / 19	Primera	10 . 1 . 160 . 1	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 0 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-			-	
				-	-			-	
				Ultima	10 . 1 . 191 . 254	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 0 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	-	VACANTE	10.1.192.0 / 19	Primera	10 . 1 . 192 . 1	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 1 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-			-	
				-	-			-	
				Ultima	10 . 1 . 223 . 254	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 1 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	-	VACANTE	10.1.224.0 / 19	Primera	10 . 1 . 224 . 1	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 1 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-			-	
				-	-			-	
				Ultima	10 . 1 . 255 . 254	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 0 1 . 1 1 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	-	VACANTE	10.2.0.0 / 19	Primera	10 . 2 . 0 . 1	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 1 0 . 0 0 0	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-			-	
				-	-			-	
				Ultima	10 . 2 . 31 . 254	0 0 0 0 1 0 1 0 .	0 0 0 0	0 0 1 0 . 0 0 0	1 1 1 1 1 . 1 1 1 1 1 1 1 0
	-	-	-	-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
	-	-	-	-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
	-		-	-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
	-	-	-	-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
				-	-			-	
	126 (ULTIMA)	RESERVADA	10.15.224.0 / 19	Primera	10 . 15 . 224 . 1	0 0 0 0 1 0 1 0 .	0 0 0 0	1 1 1 1 . 1 1 1	0 0 0 0 0 . 0 0 0 0 0 0 0 1
				-	-			-	
				-	-			-	
				Ultima	10 . 15 . 255 . 254	0 0 0 0 1 0 1 0 .	0 0 0 0	1 1 1 1 . 1 1 1	1 1 1 1 1 . 1 1 1 1 1 1 1 0

APPENDIX B

1. B1 – Present Architecture of the SAM Network

1.1 ICAO, the Contracting Party on behalf of the Member States, under Technical Cooperation Project RLA03/901, is the organization responsible for coordination, tendering and management of the SAM Digital Communication Network (REDDIG).

1.2 The countries and nodes, together with their basic geographic coordinates, that are a part of this tender, are listed in Table 2.

Country	Node	Indicative	Latitude	Longitude
Argentina	Ezeiza	SAEZ	34° 49’ 25” S	58° 31’ 43” W
Bolivia	La Paz	SLLP	16° 30’ 29” S	68° 11’ 24” W
Brazil	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	Bogota	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 Guiana	Cayenne	SOCA	04° 49’ 11” N	52° 21’ 38” W
Paraguay	Asuncion	SGAS	25° 14’ 24” S	57° 31’ 09” W
Peru	Lima	SPIM	12° 01’ 19” S	77° 06’ 52” W
Suriname	Paramaribo	SMPM	05° 27’ 10” N	55° 11’ 16” W
Trinidad and Tobago	Piarco	TTZP	10° 35’ 44” N	61° 20’ 36” W
Uruguay	Montevideo	SUMU	34° 50’ 15” S	56° 01’ 49” W
Venezuela	Maiquetia	SVMI	10° 36’ 12” N	66° 59’ 26” W

Table 2: Location of the REDDIG Nodes

1.3 Figure 1 shows the basic topology of the current REDDIG with its sixteen nodes.

Figure 1: Current REDDIG Topology

In addition to that outlined in Figure 1, the REDDIG is also interconnected with the MEVAII network that serves the Central American and Caribbean countries and the United States. REDDIG uses the nodes of Bogota (Colombia) and Maiquetia (Venezuela), as described in Figure 2, to make that interconnection.

1.4

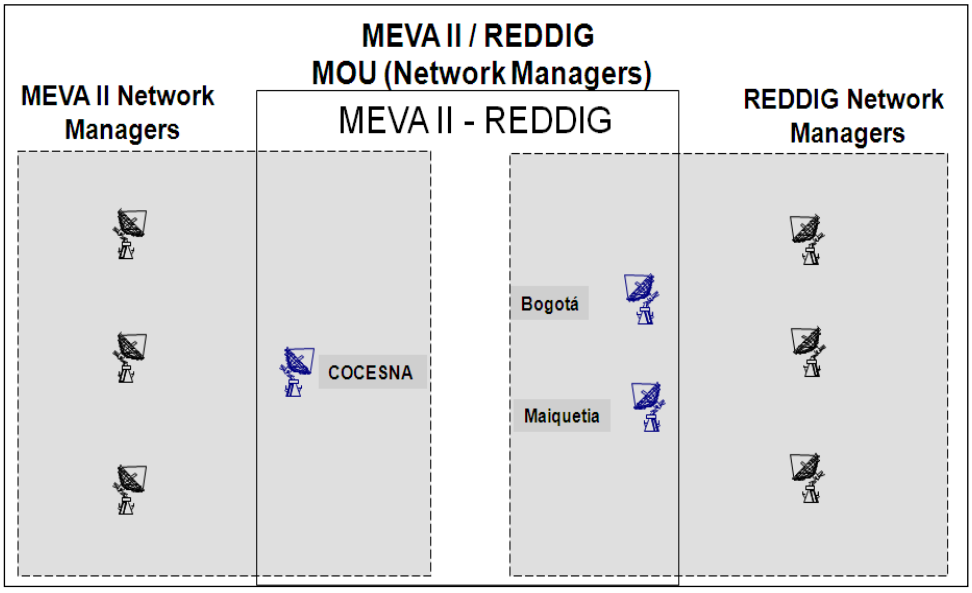


Figure 2. MEVA II - REDDIG Interconnection

1.5 The basic characteristics of the current network are the following:

a) REDDIG is a meshed network that uses VSAT (Very Small Aperture Terminal) technology with 3.7m antennas and Band C (4-6 GHz), utilizing the INTELSAT IS-14 satellite that is located at 315°E. At present, a 4.4 MHz capacity is rented to meet REDDIG application requirements.
b) REDDIG possesses a total of 1,328 Kbps to handle traffic between all network terminals, which are equivalent to 83 16 Kbit/s bursts.
c) INTELSAT is the current satellite provider, since the International Civil Aviation Organization (ICAO), as a United Nations (UN) Organization, is an INTELSAT signatory by law and thus responsible for reserving and paying for the required bandwidth.
d) The REDDIG network uses band C (4-6 GHz) because some of its nodes are located in zones where weather conditions make that use necessary.
e) The main equipment (indoor and outdoor), together with the software used, are described in Appendix A, while the main voice and data services are described in Appendix B.
f) The network also supports RC&M (Remote Control & Monitoring) for the efficient management of its resources. There are two network control centres (NCCs), the main one being located in Manaus (Brazil) and the alternate in Ezeiza (Argentina).
g) The interconnection between the MEVA II and REDDIG networks maintains the individual basic characteristics of the two networks insofar as management and control are concerned. Nevertheless, it adds a MEVA II modem in the Bogota (Colombia) and Maiquetia (Venezuela) REDDIG nodes and a REDDIG modem to the COCESNA (Honduras) MEVA II node.

2. B2 – Future network architecture

2.1 REDDIG II arose from the need to maintain air navigation communications and services among the various air traffic units of the Region that are currently being served by the REDDIG, and to implement the backbone of the Aeronautical Telecommunication Network (ATN).

2.2 Figure 3 presents an outline of the basic topology required for REDDIG II.

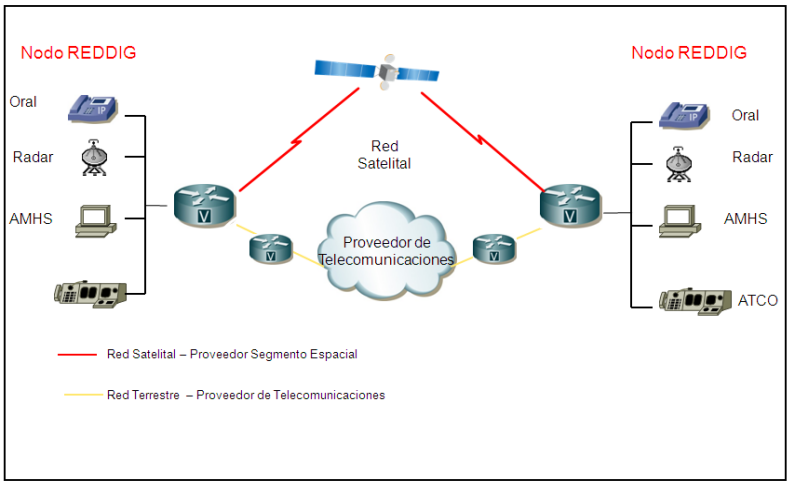


Figure 3: Basic REDDIG II Topology

2.3 As can be seen in Figure 3, REDDIG II will have two segments: a satellite transmission (VSAT) segment, and a ground segment based on Multiprotocol Label Switching (MPLS) technology. The satellite backbone will be the main system, and the ground segment, being IP, will increase flexibility for the loading of new applications, and will also increase the network's overall availability. If the main network fails, switching to the ground backbone will be automatic.

2.4 The topology of the satellite and terrestrial networks will be fully meshed, flexible and scalable in order to facilitate infrastructure growth. In addition, it will be highly available, thanks to: intelligence distributed within its nodes and with no common failure point, traffic prioritization, dynamic bandwidth management and management by demand, automatic alternate traffic routing in the event of a failure and a global, integrated, "future-proof" common network management system (NMS) to allow for migration to other network technologies.

2.5 The routing system to be implemented has important characteristics for purposes of this document, inasmuch as it must support internal gateway protocols (IGP), such as RIP (Versions 1 and 2) and OSPF, and external border gateway protocol BGP-4.

2.6 The main requirements of the VSAT system will be:

a) Hubless network with no common failure point. All stations will be identical and no specialized stations must exist. Each station must be capable of acting as a time reference station for the satellite network, with only occasional updating of software.
b) Secure control system via pre-established and programmable rotation defined by the master and supporting terminals, automatic switching if the master station fails, or synchronized architecture that does not require a master station.
c) Full-meshed topology: the necessary links should be established to satisfy network topology and communication requirements.
d) All communications should be established through a simple satellite hop.
e) Satellite links will have a better bit error rate (BER) than 1 E-7.
f) Band C operation.

2.7 The REDDIG II terrestrial backbone will operate as a multiservice infrastructure and should be provided by a Multiservice IP Platform that is logically independent and isolated from any other network, particularly the public environment of the Internet. The main requirements are described as follows:

a) Monthly availability of each link at least 99.5% of the time.
b) Delay of less than 60 m.
c) RTT for a 64-byte packet in a communication between two stations of no more than 150 m in 95% of the measurements made during a 10-second minimum time window.
d) BER smaller than 10^{-7} 99.5% of the time.

APPENDIX C

1. **C1 – Air navigation support service requirements in the SAM Region, including those foreseen for the short, medium and long term.**

1.1 The list of air navigation support service requirements in the SAM Region, including those foreseen for the short, medium and long term, to be transported over the new digital network, consist of the:

1.1.1 Current services

1.1.1.1 Those deriving from the requirements contained in the Air Navigation Plan for the Caribbean and South American Regions, almost all of which are operational, as follows:

a) Table CNS1A (AFTN Plan).
b) Table CNS1C (ATS direct speech circuits).

1.1.2 Future services

a) Those stemming from the MEVA II – REDDIG interconnection.
b) Teleconferencing Service for flow management units (FMU) or flow management positions (FMP), to be carried out daily among all of the Region's units, initially for twenty users.
c) Exchange of flight plans and/or radar information using conventional methods, in accordance with the respective MoUs (Memorandums of Understanding) that have been or are to be signed.
d) AMHS interconnection requirements, which will progressively replace the AFTN service, in accordance with the respective MoUs (Memorandums of Understanding) that have been or are to be signed.
e) AIDC interconnection requirements, which will progressively replace the ATS speech service.
f) Exchange of ADS-B data and their multilateration among all ACCs of adjacent FIRs.
g) Interconnection of automated systems among the ACCs of adjacent FIRs, using Asterix 62 and 63.
h) AIM requirements: no specific requirement is as yet available in this regard.

1.2 Table B-1 describes the minimum interfaces that routers to be installed in each State should have for REDDIG II implementation.

State	Site	Minimum interfaces					
		Universal I/O	Ethernet	Digital	E&M	FXO	FXS
Argentina	Ezeiza	11	1	0	11	0	1
Bolivia	La Paz	4	1	0	4	0	4
Brazil	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
Colombia	Bogota	7	1	1	0	0	0

State	Site	Minimum interfaces					
		Universal I/O	Ethernet	Digital	E&M	FXO	FXS
Ecuador	Guayaquil	3	1	1	0	0	0
French Guiana	Rochambeau	2	1	0	0	0	5
Guyana	Georgetown	4	1	0	0	0	5
Paraguay	Asuncion	3	1	0	3	0	3
Peru	Lima	9	1	1	0	0	0
Suriname	Panamaribo	3	1	0	0	0	4
Trinidad and Tobago	Piarco	2	1	0	0	0	6
Uruguay	Montevideo	2	1	0	0	4	5
Venezuela	Maiquetía	10	1	0	7	0	4

Table B-1: Future Interfaces for REDDIG II

1.3 Table B-2 presents the estimated bandwidth needed to support the new services to be implemented in the SAM Region for REDDIG II.

State	Site	Service (each in Kbps)			
		AFTN	Radar	AMHS	ADS-B
Argentina	Ezeiza		76.8	28.8	19.2
Bolivia	La Paz		115.2	14.4	19.2
Brazil	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	Bogota	19.2	76.8	38.4	19.2
Ecuador	Guayaquil		38.4	14.4	19.2
French Guiana	Rochambeau		38.4	9.6	19.2
Guyana	Georgetown		57.6	19.2	19.2
Paraguay	Asuncion		57.6	9.6	19.2
Peru	Lima	9.6	96	43.2	19.2
Suriname	Panamaribo		76.8	14.4	19.2
Trinidad and Tobago	Piarco		19.2	9.6	19.2
Uruguay	Montevideo		19.2	9.6	19.2
Venezuela	Maiquetia		76.8	38.4	19.2
Partial figures (Kbps)		38.4	1017.6	316.8	307.2
Partial global figure (Kbps)		1680			
AFTN difference		-103.2			

State	Site	Service (each in Kbps)			
		AFTN	Radar	AMHS	ADS-B
Net increase in bandwidth		1576.8			

Table B-2: Estimated additional bandwidth

APPENDIX D

TABLE CNS 1Ba – ROUTERS REGIONAL PLAN
SAM REGION

Administration and Location	Type of Router	Type of Interconnection	ConnectedRouter	Link Speed	Link Protocol	Via	Target Date	Remarks
1	2	3	4	5	6	7	8	9
Argentina/Buenos Aires	IP	Inter Regional	AFI (Johannesburg)	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 (Asuncion)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Peru (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	Peru (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	Circuit via Bogota
	IP	Intra Regional	Paraguay (Asuncion)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Uruguay (Montevideo)	64K	IPv4	REDDIG	2014	
Brazil/Manaus	IP	Intra Regional	Colombia (Bogota)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Guyana (Georgetown)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	French Guiana (Cayenne)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Peru (Lima)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Suriname (Paramaribo)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2012	
Chile/Santiago	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2012	
	IP	Inter Regional	PAC (Christchurch)	TBD	IPv4	PTT	TBD	
	IP	Intra Regional	Peru (Lima)	64K	IPv4	REDDIG	2014	
Colombia/Bogota	IP	Intra Regional	Brazil (Manaus)	64K	IPv4	REDDIG	2014	

Administration and Location	Type of Router	Type of Interconnection	ConnectedRouter	Link Speed	Link Protocol	Via	Target Date	Remarks
1	2	3	4	5	6	7	8	9
	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	Connection of Colombia and Brazil
	IP	Intra Regional	Panama	64k	IPv4	MEVAII/REDDIG	2014	
	IP	Intra Regional	Peru (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 (Bogota)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Peru (Lima)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2014	
French Guiana/Cayenne	IP	Intra Regional	Brazil (Manaus)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	Suriname (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	Suriname (Paramaribo)	64K	IPv4	REDDIG	2011	
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2014	
Panama/Panama	IP	Inter Regional	CAR	64K	IPv4	CAMSAT	2012	
	IP	Intra Regional	Colombia (Bogota)	64K	IPv4	MEVAII / REDDIG	2014	
	IP	Inter Regional	NAM (Atlanta)	64K	IPv4	MEVA II	2014	
Paraguay/Asuncion	IP	Intra Regional	Argentina (Buenos Aires)	64K	IPv4	REDDIG	2012	
	IP	Intra Regional	Brazil (Brasilia)	64K	IPv4	REDDIG	2014	
Peru/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	

Administration and Location	Type of Router	Type of Interconnection	ConnectedRouter	Link Speed	Link Protocol	Via	Target Date	Remarks
1	2	3	4	5	6	7	8	9
	IP	Intra Regional	Colombia (Bogota)	64K	IPv4	REDDIG	2010	
	IP	Intra Regional	Ecuador (Guayaquil)	64K	IPv4	REDDIG	2012	
	IP	Inter Regional	NAM (Atlanta)	64K	IPv4	MEVAII/REDDIG	2014	Via Bogota, Colombia
	IP	Intra Regional	Venezuela (Caracas)	64K	IPv4	REDDIG	2014	
Suriname/Paramaribo	IP	Intra Regional	Brazil (Manaos)	64K	IPv4	REDDIG	2014	
	IP	Intra Regional	French Guiana (Cayenne)	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 (Bogota)	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	

APPENDIX E

STATE	TYPE OF ROUTER	AS NUMBER
Argentina	IP	64517
Bolivia	IP	64529
Brazil	IP	64531
Chile	IP	64543
Colombia	IP	64545
Ecuador	IP	64558
Guyana	IP	64574
French Guiana	IP	64575
Panama	IP	65261
Paraguay	IP	65263
Peru	IP	65264
Suriname	IP	65288
Uruguay	IP	65302
Venezuela	IP	64528

- - - - - -