Cuestión 4 del Orden del Día: **Evaluación de los requisitos operacionales para determinar la implantación de mejoras de las capacidades de comunicaciones, navegación y vigilancia (CNS) para operaciones en ruta y área terminal**

SEGUIMIENTO SOBRE EL DESEMPEÑO Y ACTIVIDADES EN LA REDDIG II

(Presentada por la Secretaría)

RESUMEN

Esta nota de estudio presenta información sobre el desempeño y actividades realizadas desde la Décimo Novena Taller/Reunión del Grupo de Implantación SAM (SAM/IG/19).

Referencias

- Contrato REDDIG 22501200;
- Informe de la Vigésima Reunión del Comité de Coordinación de la REDDIG
- (RCC/20) (Lima, Perú, 21 al 23 de marzo de 2017);
- Décimo Noveno Taller/Reunión del Grupo de Implantación SAM (SAM/IG/19) (Lima, Perú, 22 al 26 de mayo de 2017); y
- Sexta Reunión Técnica Operacional de la REDDIG II (RTO/6) (Manaos, Brasil, 12 de junio de 2017).

Objetivos estratégicos de la OACI:	*A – Seguridad operacional; y* *B – Capacidad y eficiencia de la navegación aérea*

1. Antecedentes

1.1 La Reunión SAM/IG/19 analizó el desempeño y la implantación de actividades de la REDDIG II desde la Reunión SAM/IG/18, de estas se destaca el incremento de la disponibilidad de la REDDIG II desde agosto de 2016 con la implantación completa de los cambios en los LNB (Bloque convertidor de bajo ruido).

1.2 Asimismo, la Reunión tomó nota del análisis inicial de seguridad en la REDDIG II realizada por el grupo ad hoc, conformado por Argentina, Brasil, Colombia, Guyana Francesa (Francia), Paraguay y Perú y de la necesidad de preparar un plan de acción especificando fechas de implantación de las acciones propuestas, para mitigar las amenazas identificadas que podrían afectar la seguridad en la REDDIG II.

2. Análisis

2.1 A continuación se presentan las principales actividades realizadas en la REDDIG II y un análisis del desempeño de su operación desde la SAM/IG/19 acordadas en la última Reunión del Comité.

La descripción cubre principalmente los siguientes aspectos:

a) Programa de entrenamiento de la REDDIG II;
b) Operación de la REDDIG II y análisis de implantación de nuevos servicios.

Programa de entrenamiento de la REDDIG II

2.1. En referencia a las actividades de entrenamiento, se realizaron los siguientes cursos:

c) Curso avanzado de Operación de la REDDIG II
d) Curso de Redes IP aplicado a la REDDIG II
e) Curso de Fundamentos de Redes (Básico) para personal NCC Manaos

Curso avanzado de Operación de la REDDIG

2.2 Este curso estuvo dirigido al personal técnico responsable de la operación y mantenimiento de la estación REDDIG II que recibió los respectivos cursos básicos. Entre los aspectos que se trataron, se enfatizó en la operación y supervisión del modem Skywan 1070/7000 con una descripción teórica-práctica del software '*Line Up Manager'* así como '*troubleshooting*' de los componentes de la estación.

2.3 Este curso se realizó del 13 al 16 de junio de 2017 en las instalaciones de la Sección de Instrucción y Actualización Técnica (SIAT) del Cuarto Centro Integrado de Defensa Aérea y Control del Tránsito Aéreo – CINDACTA IV, Manaos, Brasil. Para este evento se asignó una beca por Estado miembro del proyecto RLA/03/901 y se contó con traducción simultánea.

2.4 El curso contó con la participación de 36 delegados pertenecientes a los Estados de Argentina, Brasil, Chile, Colombia, Ecuador, Guyana, Paraguay, Perú, Surinam, Trinidad & Tobago y Venezuela. A los participantes del curso, se les entregó la versión digital del contenido, así como archivos electrónicos complementarios.

Curso de Redes IP aplicado a la REDDIG

2.5 El curso estuvo dirigido al personal técnico con conocimientos de redes IP y que participó de los cursos "*Interconnecting Cisco Network Devices Part 1 (ICND1)*" e "*Interconnecting Cisco Network Devices Part 2 (ICND2)"*, y que tiene la responsabilidad de la operación y mantenimiento de la estación REDDIG II.

2.6 Se llevó a cabo del 13 al 17 de noviembre de 2017 en las instalaciones de la Sección de Instrucción y Actualización Técnica (SIAT) del Cuarto Centro Integrado de Defensa Aérea y Control del Tránsito Aéreo – CINDACTA IV, Manaos, Brasil. Para este evento se asignó una beca por Estado miembro del proyecto RLA/03/901 y se contó con traducción simultánea.

2.7 El contenido se basó en los tópicos (*Lessons*) de los cursos Cisco ICND1 e ICND2 pero focalizados en los equipos y servicios que se brindan actualmente en la REDDIG con laboratorios virtuales empleando el "*Packet Tracer*".

2.8 El curso contó con la participación de 24 delegados pertenecientes a los Estados de Argentina, Brasil, Chile, Guyana, Paraguay, Surinam, Trinidad & Tobago y Venezuela.

Curso de Fundamentos de Redes (Básico) para personal NCC Manaos

2.9 Este curso estuvo dirigido al personal que desarrolla sus tareas diarias en el NCC Manaos y se corresponde con el compromiso de capacitación continua a la cual está comprometido el proyecto. Este curso no estaba en el plan de actividades considerada en la RCC/20, pero se consideró necesario realizarlo. No representó costo alguno al proyecto.

2.10 El curso tuvo como fin renovar y complementar los conceptos fundamentales y avanzados en sistemas de transmisión empleados en el transporte de voz y datos aplicados a la aviación civil.

2.13. El esquema del curso propuesto se basó en los fundamentos de redes orientados a las aplicaciones aeronáuticas sobre IP del proyecto RLA/03/901 de la Oficina SAM de la OACI; en el curso teórico-práctico CCNA (*Cisco Certified Networking Associate*), *Networking Fundamentals* y de diferentes fuentes las cuales tratan de forma lógica los temas en telecomunicaciones.

Operación de la REDDIG II y análisis de implantación de nuevos servicios

Nodo REDDIG II Brasilia

2.15 El nodo de Brasilia entró en operación en abril de 2016, no obstante, se observaron durante su funcionamiento algunas novedades que debieron ser corregidas.

2.16 En tal sentido, se realizó una misión a Brasilia del 16 al 25 de octubre de 2017 con la participación de la Administración de la REDDIG, la empresa INEO y personal de CINDACTA I.

2.17 Las tareas en resumen se circunscribieron a los siguientes temas:

a) comprobación del estado de los cables seriales y chequeo del funcionamiento de la cadena B;
b) inconvenientes con los circuitos de voz de mantenimiento y administrativos
c) verificación del cableado coaxial
d) causas de las pérdidas de paquetes en el módem Skywan A
e) verificación del funcionamiento del Gorgy timing
f) procedimiento de backup de los servidores en discos externos
g) comprobación general e integra del funcionamiento de la estación y sus componentes

2.18 Las tareas realizadas durante la misión resolvieron los últimos problemas e inconvenientes pendientes en el nodo REDDIG II de Brasilia, quedando pendiente solucionar definitivamente un inconveniente de la conexión de 10Mhz. No obstante, se implementó una solución temporal instalando un DC-Block en el camino de Tx de la conexión de 10MHz. Un DC-Block no fue suficiente.

2.19 Este DC Block necesitó ser reemplazado por cuatro DC-Blocks definitivos, adaptados al rango de frecuencias del sistema REDDIG; para lo cual INEO envió al sitio SBBR cuatro DC Block BLK-6-N + (Mini-Circuitos). Estos fueron instalados definitivamente el 10 de enero de 2018 quedando la estación Brasilia con todos los inconvenientes resueltos.

Nodos REDDIG II

2.20 Durante la misión realizada a Brasilia, también se atendieron novedades relacionadas con la red en general.

2.21 En tal sentido, además de las tareas consignadas y propias del nodo Brasilia se atendieron las siguientes novedades:

a) Verificación del funcionamiento de los NMS de Venezuela y Ecuador
b) Análisis sobre inestabilidad en el funcionamiento de Venezuela
c) Soporte para NDSatCom
d) Verificación y comprobación del funcionamiento del nodo La Paz
e) Inconvenientes en la estación Ezeiza
f) Establecer procedimiento para cálculo de consumo de ancho de banda

2.22 En el caso particular de Ezeiza, obedece a un acontecimiento que ocurrió y coincidió con el período de la misión, y que fue producto de las condiciones climáticas que afectaron la estación durante la noche del 18 al 19 de octubre de 2017.

2.23 En cuanto al soporte para NDSatCom, está referido a las tareas que se realizaron para facilitar el acceso remoto del personal de mencionada empresa, al módem Skywan A de Manaos para intervenir en la novedad del congelamiento periódico que sufría este equipo.

Novedades IBUC de Surinam y Módem de Bolivia

2.24 El 17 de octubre de 2017 el IBUC B del nodo Paramaribo (Surinam) queda fuera de servicio. Si bien se realizaron todas las acciones inherentes para recuperar la funcionalidad del equipo, fue necesario coordinar con INEO para enviar el mismo a reparar en fábrica y enviar un equipo IBUC 80W de repuesto desde la Oficina Regional en Lima. El equipo enviado desde la Oficina SAM permaneció en la en las oficinas de Aduana, en Paramaribo unos cinco meses, su retiro e instalación se realizó la semana del 7 de mayo de 2018.

2.25 Referente al módem de La Paz (Bolivia), presentó fallas el 15 de junio de 2017.. El módem enviado desde la Oficina Regional a La Paz, luego de varias complicaciones logísticas en Bolivia, finalmente fue recibido en el mes de noviembre e instalado en la estación el 20 de noviembre de 2017. El equipo con falla fue enviado desde Bolivia, por intermedio de INEO, a fábrica para su reparación.

Pruebas de aceptación final de la REDDIG II (FNAT)

2.26 Las pruebas de aceptación Provisional de la REDDIG II (documento PSAT – NAT - 2022 NT - 2141167C Rev. H) se realizaron del 31 de enero al 05 de febrero de 2015. Una vez que concluyeron las pruebas, los puntos focales de los Estados miembros de la REDDIG II procedieron a firmar el certificado de PSAT con comentarios en cada uno de los nodos.

2.27 Los resultados de las pruebas PSAT con los comentarios en cada uno de los nodos fueron registrados en el documento PSAT (versión H). Este documento se colocó en la siguiente página web www1.lima.icao.int/reddig.

2.28 De acuerdo al artículo 13.1 del contrato Nº 2250120 (Provisión de una nueva red de tele comunicaciones regional (REDDIG II)), el consorcio INEO&Level 3 tenía un plazo de 40 días para

corregir las deficiencias encontradas en la PSAT. En el periodo de 40 días, el consorcio INEO&Level 3 procedió a la corrección de muchas de las deficiencias a excepción de las siguientes fallas mayores:

- Congelamiento en forma aleatoria del modem satelital (Skywan ID 1070) en algunos de los nodos de la REDDIG II
- Congelamiento aleatorio del modem satelital de Manaos cadena A (Skywan ID 7000)

2.29 Estas fallas mayores, el consorcio INEO&Level 3 las completó a finales del año 2017. En este sentido, del 29 al 30 de enero del 2018, se procedió a la realización de las pruebas de aceptación final de la REDDIG II (FNAT). El 30 de enero, se procedió a la firma del certificado de la FNAT. Esta actividad se realizó en las instalaciones de CINDACTA IV en Manaos, Brasil donde se encuentra el nodo de la REDDIG II de Manaos y el NCC.

Implantación de nuevos servicios

2.30 Desde la RCC/20 a la fecha, se implantaron y entraron en operación en la REDDIG II, los siguientes circuitos AMHS:

Brasilia - Bogotá (mayo 2017)
Brasilia - Georgetown (julio 2017)
Bogotá - Caracas (diciembre 2017)
Brasilia - Caracas (marzo 2018)
Brasilia –Ezeiza (marzo 2018)

2.31 Asimismo, se implantaron otros circuitos AMHS, los cuales todavía no están en operación. Se espera que los mismos entren en operación en el transcurso del 2018:

Ezeiza - Lima
Ezeiza - Santiago
Ezeiza - Montevideo
La Paz - Lima
Lima - Guayaquil
Bogotá - Guayaquil
Caracas - Guayaquil
Bogotá - Panamá (Interconexión MEVAIII REDDIG II)
Brasilia - Montevideo

2.32 Además, se realizaron conexiones a nivel de red para el intercambio de datos radar entre:

Ezeiza - Santiago
Ezeiza - Asunción

Se espera que, en el transcurso de 2018, el intercambio de datos radar entre las localidades indicadas, entren en fase operacional.

Disponibilidad REDDIG II

2.33 Como **Apéndice A** de esta nota de estudio se presenta un cuadro de disponibilidad de la REDDIG desde el inicio de sus operaciones , en la misma se puede observar que en los años 2015 y 2016 los dos primeros años de la REDDIG II por los problemas de asentamiento de la REDDIG II los niveles de disponibilidad estuvieron por debajo del 99.99% pero a partir de finales de 2016 al haberse

solucionado los problemas de congelamiento aleatorio de los modem satelitales la disponibilidad alcanzó la disponibilidad esperada mayor que el 99.99%.

Análisis de seguridad de la REDDIG II

2.34 La Sexta Reunión Técnico-Operacional de la REDDIG II (RTO/6), presentó un plan de acción inicial para la implantación de las acciones para mitigar las amenazas identificadas que podrían afectar la seguridad en la REDDIG II, la misma se presenta como **Apéndice B** de esta nota de estudio.

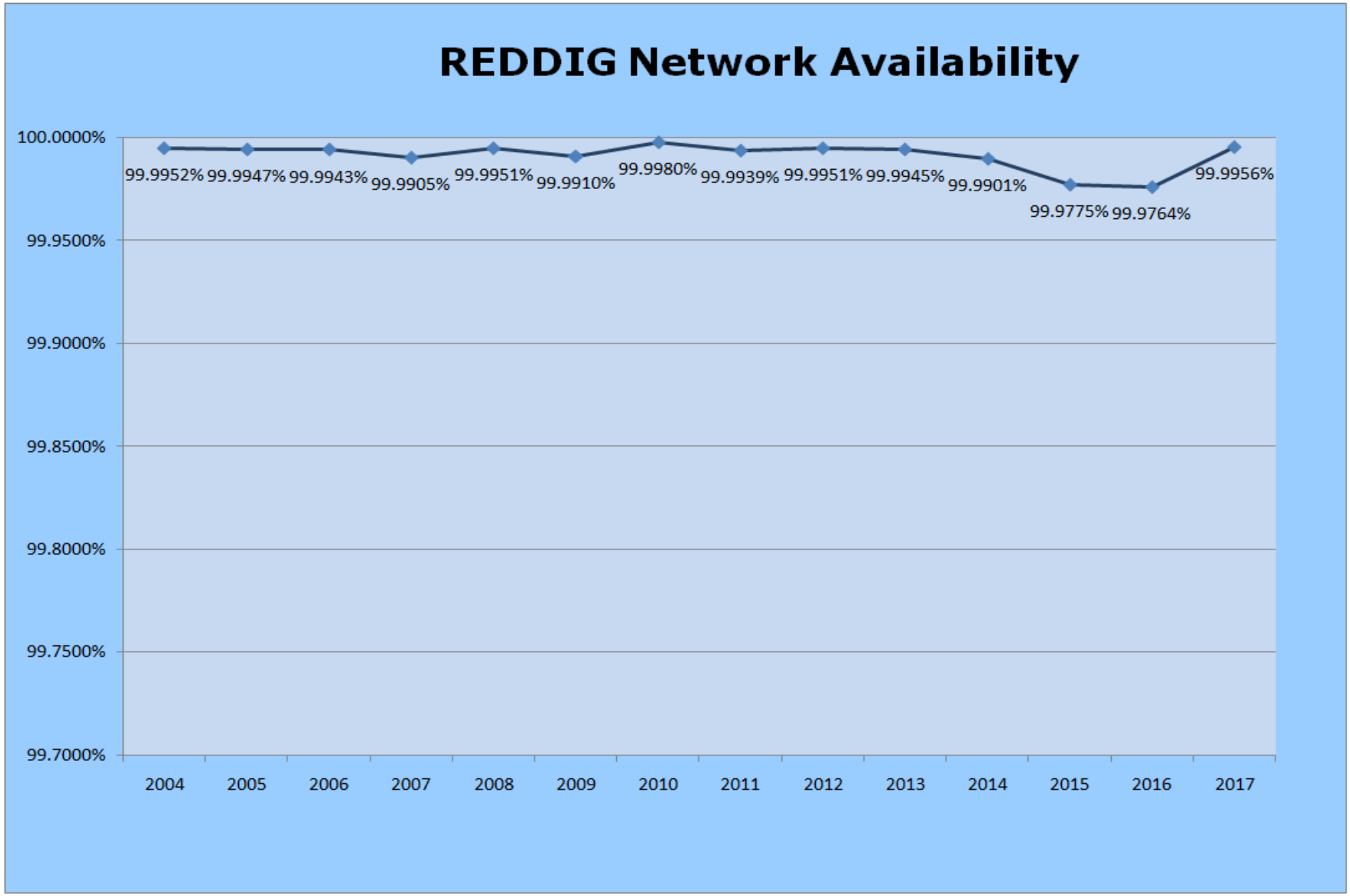
3 Acciones sugeridas

3.1 Se invita a la Reunión:

a) Tomar nota de la información suministrada;

b) analizar las actividades realizadas y el desempeño de la REDDIG II desde la SAM/IG/19 hasta la fecha que se presentan en la sección 2 y los **Apéndices A y B** correspondientes de esta nota de estudio; y

c) Otras consideraciones al respecto que la reunión considere necesaria.


REDDIG Network Availability
100.0000%
99.9500%
99.9000%
99.8500%
99.8000%
99.7500%
99.7000%
99.9952%
99.9947%
99.9943%
99.9905%
99.9951%
99.9910%
99.9980%
99.9939%
99.9951%
99.9945%
99.9901%
99.9775%
99.9764%
99.9956%
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

APÉNDICE B

ANÁLISIS DE SEGURIDAD REDDIG II

1 Introducción

1.1 En función de lo establecido en la teleconferencia del pasado 5 de mayo de 2017, relacionada con la Conclusión RCC/20-3, *Análisis de seguridad de la REDDIG II* (formulada en la Vigésima Reunión de Coordinación de la REDDIG - *Proyecto RLA/03/901* (RCC/20), y el trabajo que se encuentra realizando el grupo ad hoc nominado en la Decimonovena Reunión de Coordinación de la REDDIG, con el objetivo de analizar la seguridad de la REDDIG (conformado por Argentina, Brasil, Colombia, Guyana Francesa (Francia), Paraguay, Perú y la Secretaría), para preparar un plan de acción, especificando fechas de implantación de las acciones propuestas, que se presentan como Apéndice H de la cuestión 3 del orden del día del informe final de la RCC20.

Plan de acción para implantación del análisis de seguridad de la REDDIG II

Amenazas REDDIG II

2.1 En el análisis de las amenazas internas de la REDDIG II se recordó sobre la necesidad de que en cada uno de los nodos de la REDDIG II se instalarán Routers redundantes conjuntamente con un "Ethernet switch", los cuales soportarán todas las "VLANs" de todos los servicios en IP, tanto actuales como futuros. Este requerimiento se formuló en la tercera reunión técnica operacional de la REDDIG a través de la Conclusión RTO/3- *Instalación de un router y switch Ethernet redundante para los servicios IP nativos*

2.2 Con el fin de estandarizar la configuración de los routers y switches, las características técnicas de los mismos, el direccionamiento IP, firewall, aplicación de NAT y otros protocolos, se presenta a continuación **un estudio inicial**. Este estudio inicial se distribuirá a los delegados del grupo ad hoc para sus comentarios y se **presentará a la Sexta Reunión Técnica Operacional de la REDDIG II** a realizarse en Manaos Brasil del 12 al 16 de junio de 2017 para su revisión. Este estudio posteriormente **se presentará en la RCC/21** (marzo de 2018) para la **aprobación de la implantación** como una extensión del contrato de la REDDIG II.

2. <u>Estudio inicial</u>

2.1 Oportunamente se estableció que todos los Estados deberían tener implementado routers de borde y se podría asumir que no en todos los nodos han realizado esta acción.

2.2 Como se ha mencionado en diferentes circunstancias, la seguridad en la REDDIG II debería ser definida como el proceso mediante la cual se protegen los recursos. Los objetivos de la seguridad deben ser:

1) Proteger la confidencialidad.
2) Mantener la integridad.
3) Asegurar la disponibilidad.

2.3 Objetivos que determinan el imperativo de proteger toda la red a fin de evitar amenazas y vulnerabilidades.

2.4 Una amenaza es un acceso no autorizado a una red o dispositivo de red. Normalmente las amenazas son persistentes debido a las vulnerabilidades, que son problemas que pueden surgir como resultado de una mala configuración del hardware o del software, un diseño pobre de la red, carencias tecnológicas heredadas, falta de capacitación o el descuido del usuario final.

2.5 Los riesgos en la seguridad no pueden eliminarse o prevenirse completamente; sin embargo, una administración y una valoración eficaces de los riesgos pueden minimizar significativamente su existencia. El riesgo asumido se basa en el costo que se quiera tomar para salvaguardar la información.

2.6 Los tres objetivos principales de la seguridad parecen muy simples. Sin embargo, el desafío de asegurar la red a la vez que se tienen en consideración las necesidades operativas puede ser una tarea compleja. Los administradores deben administrar cuidadosamente las políticas de seguridad para mantener el equilibrio entre el acceso transparente, el uso y la seguridad de la red.

2.7 En relación a lo expuesto anteriormente, y a la necesidad de seguridad los accesos externos, se sugiere:

1) Se adquieran equipos de networking (routers firewall) para todos los nodos con el objeto de:

   a) estandarizar el equipamiento de seguridad en toda la red,
   b) evitar intrusiones externas e internas no autorizadas,
   c) suplir la falta de un router de borde en algunos nodos,
   d) gestión por parte del administrador de la REDDIG II de todos los firewalls (hoy supeditado a cada Estado).

2) Implementar un TACACS Server para controlar los accesos, crear una comunidad en los equipos de la red para instalar un SISLOG (monitorea todos los eventos de la red, con la posibilidad de envío ante un evento por mail), etc.

3) Definir la asignación de niveles de usuarios y llevar un registro en un servidor en donde se alojarán todos los eventos, que comandos se ejecutaron, quién ingresó, etc.

4) También, todo lo anterior, permite crear eventos para que se realicen los backups automáticos o backup cuando se realicen cambios de configuración de todos los equipos de networking.

2.8 Es sumamente necesario contar con un plan de seguridad que permita definir con precisión la arquitectura y las operaciones, Riesgos y políticas de seguridad.

2.9 Posteriormente, realizar un análisis en conjunto con el personal a cargo de la red, para determinar qué tipo de eventos es recomendable tomar registros (ejemplo: accesos a los dispositivos, cambios de estado de las interfaces de red, reinicios en caliente, cambios en los parámetros de configuración, etc).

3. Firewalls

3.1 La aplicación más utilizada en los últimos años es el conocido firewall (cortafuegos), combinación de hardware y software que utilizan las empresas y los usuarios para aislar la red privada del exterior.

3.2 Un firewall es un mero control de acceso del tráfico entrante/saliente de la red del usuario. En este control, se revisan los datagramas o paquetes que por él pasan y según las reglas que haya impuesto

el administrador de la red, actuará en consecuencia: eliminando, reenviado o preguntando al administrador.

3.3 Existen cuatro tipos de firewalls: de filtrado de paquetes, pasarelas de nivel de aplicación, inspección multinivel de estados y Circuit Level Gateways. Los dos primeros son los más utilizados, pero es el de inspección multinivel el mejor considerado. La gran diferencia que existe entre ellos, es el nivel de la capa OSI en el que trabajan.

3.4 De la "Guía de Orientación de Seguridad para la Implantación de Redes IP" se puede extraer:

3.4.1 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).

3.4.2 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 firewalls 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 fábrica.

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 e integridad de las informaciones, así como el desempeño de la red según sus especificaciones;

g) Las conexiones con las redes públicas (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.* Los accesos a los dispositivos deben ser hechos con el uso de autenticación segura

i) Los links de gerenciamiento deben ser encriptados;

3.5 En la Guía de referencia se menciona constantemente el uso de firewall.

4. <u>Adquisición de routers firewalls para toda la red</u>

4.1 El principal objetivo tiende a la seguridad, y en tal sentido la estandarización e instalación de equipos de networking de las mismas características posibilitará una mayor robustez a la mitigación de vulnerabilidades.

4.2 La administración de estos equipos por parte del Administrador de la REDDIG II, y eventualmente el acceso permitido, con determinados niveles de privilegios, a los diferentes técnicos que puedan intervenir, facilitará el control de accesos con buenas o malas intenciones.

4.3 En tal sentido, el equipamiento que se requiere deberá contar, como mínimo, con las siguientes prestaciones:

1) Firewall (cortafuegos) como combinación de hardware y software utilizado para aislar la red privada del exterior.
2) Permitir conexiones confiables a través de funciones propias de firewall y listas de acceso (ACLs).
3) Permita configurar NAT.
4) Configuración de políticas de servicio
5) Configuración de reglas de accesos
6) Configuración de AAA para el acceso
7) Permitir inspección de protocolos de cada capa de aplicación
8) Brindar información acerca de las funciones de comunicaciones del equipo
9) Permitir configurar seteos de conexión y calidad de servicio (QoS)
10) Configuraciones complejas para la protección de redes.
11) Configuración de diferentes módulos.

5. Cantidades y costos

5.1 Con la finalidad de contemplar la instalación de un firewall en todos los nodos y tener un backup, es deseable adquirir 20 equipos firewall a un valor estimado por cada uno de alrededor de los USD 1000 a USD 2000. No obstante, el valor varía en función de la marca, el modelo, las placas y las licencias.

5.2 Tener en cuenta que los equipos deberían ser de una marca y proveedor disponible en la mayoría de los Estados para poder dar una respuesta inmediata a una contingencia. Así mismo, tener presente los equipos de networking que actualmente integran los nodos de la REDDIG II.
