International Civil Aviation Organization
South American Regional Office
Nineteenth Workshop/Meeting of the SAM Implementation Group (SAM/IG/19) - Regional Project RLA/06/901
(Lima, Peru, 22 to 26 May 2017)

SAM/IG/19-WP/07
10/05/17

Agenda Item 4: **Assessment of operational requirements to determine the implementation of improvements in communication, navigation, and surveillance (CNS) capabilities for operations en-route and terminal area**

FOLLOW-UP TO REDDIG II PERFORMANCE AND ACTIVITIES

(Presented by the Secretariat)

SUMMARY

This working paper presents information on REDDIG II performance and activities carried out since the SAM/IG/18 meeting.

REFERENCES

- Twentieth meeting of the Coordination Committee of Project RLA/03/901 (RCC/20) Lima, Peru, 21-23 March 2017.
- Eighteenth workshop/meeting of the SAM Implementation Group (SAM/IG/18) Lima, Peru, 17-21 October 2017.
- Summary of teleconferences on security in REDDIG II (5 May 2017).

ICAO strategic objectives:	*A – Safety* *B – Air navigation capacity and efficiency*

1 Introduction

1.1 The SAM/IG/18 meeting analysed the performance and the activities carried out in REDDIG II since the SAM/IG/17 meeting, highlighting the increased availability of REDDIG II since August 2016 as a result of partial introduction of changes to LNBs (low-noise block converters), the implementation of the Brasilia-Lima AMHS circuit, the conduction of two basic courses of REDDIG II, in which 41 new technicians were trained, the analysis of threats that could affect REDDIG II security, and the implementation of an ATS speech circuit (hot line) between Maiquetía and San Juan, Puerto Rico through the MEVAIII-REDDIG II interconnection.

2 Analysis

2.1 An analysis follows of the progress made in REDDIG II-related activities since the SAM/IG/18 meeting on the following aspects:

- Pending activities in REDDIG II
- LEVEL 3 ground network
- Training activities and technical-operational meeting
- Analysis of REDDIG II security

- Analysis of the connection setup in REDDIG II for SITA datalink services
- Relocation of the REDDIG II node of Bogota
- New REDDIG II node in Ezeiza
- New services in REDDIG II
- Satellite ADS B services in REDDIG II
- MEVAIII/REDDIG II interconnection activities

Pending activities in REDDIG II

2.2 In order to solve the problem of random freezing in some REDDIG II nodes, INEO replaced the LNBs in the 11 remaining nodes of REDDIG II between November 2016 and the first week of April 2017. The replacement in six nodes (Argentina, Manaus-Recife, Cayenne, Lima, and Guayaquil) was reported at the SAM/IG/18. Thus, the replacement of all LNBs has been completed.

2.3 It is important to note that since November 2016 there have been no problems related to random freezing of REDDIG II nodes. Thus, the main problem of REDDIG II since it started operations in February 2015 has been solved, increasing its availability.

2.4 Another major problem in REDDIG II is a recurrent failure in the Modem Master of the Manaus NCC. In this regard, INEO obtained from the modem manufacturer (NDSATCOM) an updated sotware version whose installation is foreseen for 16 May 2017.

2.5 The following are also pending resolution by INEO before the end of the first half of 2017:

- Configuration of the IP administrative channel in the Asunción node in Paraguay
- Procedure for calculating satellite bandwidth (BW or ‘payload’) consumption in each network station.
- Software/files for initial installation of NMS servers and “WhatsUp Gold” in all network stations.
- Correction of database server connections to introduce redundancy in the Manaus node.
- Solution of “Ethernet Switch-A” malfunction in the Brasilia node.

2.6 In this regard, it is expected that final acceptance tests of REDDIG II (FSAT) will be conducted by the end of the first semester of 2017. The FSAT will only be carried out for the VSAT network, since the final acceptance test for the ground network was carried out and approved on 31 December 2015.

LEVEL 3 ground network

2.7 **Appendix A** shows the performance of the LEVEL 3 ground network in 2016 and in the months of January and February 2017. The chart shows the nodes that did not attain the availability specified in the SLA (service level agreement) signed with the LEVEL 3 ground network provider, and the penalties applied.

Training activities and technical-operational meeting

2.8 No training activities or technical-operational meetings were scheduled for the period between the SAM/IG/18 meeting and this date. The following activities are foreseen for 2017, as approved by the Twentieth meeting of the REDDIG Coordination Committee (RCC/20):

- Advanced course on REDDIG II operation
- Course on IP networks applied to REDDIG II
- Sixth REDDIG II technical-operational meeting

Advanced course on REDDIG II operation

2.9 This course is addressed to the technical staff in charge of the operation and maintenance of the REDDIG station, who have already followed the basic course. Emphasis will be placed on the operation and supervision of the Skywan 1070/7000 modem, on a theoretical-practical description of the 'Line Up Manager' software, and on troubleshooting of station components.

2.10 This course is scheduled to be held in Manaus, Brazil, on 13-16 June 2017.

Course on IP networks applied to REDDIG

2.11 The course is aimed at technical personnel with knowledge of IP networks and who are responsible for the operation and maintenance of the REDDIG station. The course will be offered in Manaus, on 16-20 October 2017. Arrangements will be made for the course to be prepared and given by two participants who took part in the 2 Cisco courses mentioned above.

Sixth REDDIG II technical-operational meeting

2.13 The Sixth REDDIG II technical-operational meeting will be held in Manaus, Brazil, on 12 June 2017, one day before the advanced course on REDDIG II operation.

REDDIG II security analysis

2.14 The Twentieth REDDIG Coordination Meeting (RCC/20) agreed that the *ad hoc* group in charge of analysing REDDIG II security, comprised of Argentina, Brazil, Colombia, French Guiana (France), Paraguay, and Peru, should prepare an action plan specifying the implementation dates for the actions proposed for mitigating identified threats that could affect the security of REDDIG II. The threats analysed by the SAM/IG/18 meeting are presented again as **Appendix B** to this working paper.

2.15 On 5 May 2017, the *ad hoc* group held a teleconference to agree on the following actions:

Internal threats to REDDIG II

Installation of boundary switches and routers

2.16 Following an analysis of REDDIG II internal threats, the *ad hoc* group recalled the need to install, in each REDDIG II node, a redundant router, together with an "Ethernet switch", to support all VLANs of all existing and future IP services.

2.17 In order to standardise the configuration and technical characteristics of routers and switches, IP addressing, firewalls, and the NAT application in each REDDIG II node, the *ad hoc* group agreed that Mr. Christian Vittor, of Argentina, should conduct an initial study by 30 May 2017. This initial study would be circulated to the delegates of the *ad hoc* group for comments and submitted to the Sicth REDDIG II Technical-Operational Meeting to be held in Manaus, Brazil (12-16 June 2017) for discussion. This study would then be submitted to the RCC/21 meeting (March 2018) for approval and implementation through the REDDIG project (RLA/03/901).

Implementation of VPN access in REDDIG II nodes

2.18 In order to standardise VPN access in REDDIG II, it was agreed that Mr. Víctor Moran, of Paraguay should prepare a tutorial on the steps required for the implementation of VPN access in REDDIG II nodes, to be used as a reference. The tutorial will be presented on 30 May 2017 and at the Sixth REDDIG II Technical-Operational Meeting (Manaus, 12-16 June 2017) for final review. At present, VPN has been installed in Brasilia, Manaus, Ezeiza, and Asunción.

Installation of antivirus in the NMS

2.19 At present, all REDDIG II nodes have antivirus installed in the REDDIG II management system, with the exception of the Georgetown, Paramaribo, and Maiquetía nodes. In this regard, the focal points of these States were urged to complete the installation as soon as possible; the date envisaged by the RCC/20 meeting was 14 April 2017.

Procedure concerning codes for accessing REDDIG II nodes

2.20 During the teleconference, it was agreed that the REDDIG Administrator should prepare a tutorial to be presented at the RTO/6 meeting on the procedure to be followed for the management, configuration and registration of codes for accessing REDDIG II, which would be applicable following final acceptance of REDDIG II with INEO.

Procedure for installing NMS back up hard disks

2.21 INEO delivered the hard disks for each REDDIG II node. These hard disks will be used for storing NMS back-up files in each of node. The hard disks have already been installed in all the nodes, except for Recife and Guayaquil, which still need to confirm reception thereof. The REDDIG Administrator will conduct the verification once the hard disks have been installed in all REDDIG II nodes.

External threats to REDDIG II

2.22 Mr. Andrés Arango, of Peru, with the support of the REDDIG Administration, was entrusted with conducting a survey of REDDIG II nodes in terms of the circuits connected to REDDIG II that might be part of a national public network. The first part of the survey would be ready by 30 May 2017, with the full survey to be completed for the RTO/6 meeting.

Analysis of the REDDIG II connection setup for SITA datalink services

2.23 Regarding the setup of REDDIG II connections for the transport of SITA datalink services, the REDDIG group considered that, in the setup proposed by SITA (see Appendix F to WP/06 of SAM/IG/18), the router(s) in all the nodes involved in REDDIG II should be installed 'behind' the boundary router/switch of the 'gateway' node rather than directly to the REDDIG switch. Note was also taken of SITA's requirement to have two geographically alternate paths in REDDIG II from each node that requires service disk.

Relocation of the REDDIG II node of Bogota

2.24 On 20-21 February 2017, INEO conducted an on-site inspection to present a new proposal for the relocation of the existing REDDIG II node of Bogota to the new ACC facilities in Bogota. Colombia considered that the relocation of the node should be carried out by INEO so as not to affect the REDDIG II guarantee, thus moving away from the previous opinion that considered that technical personnel of the Aviation Administration of Colombia should carry out the relocation.

New REDDIG II node in Ezeiza

2.25 The installation of the new REDDIG II node in Ezeiza, at the site where the new control tower and ACC are being built within the premises of the international airport of Ezeiza, is foreseen for the first quarter of 2018. With respect to the relocation of the current REDDIG II node of Ezeiza to Córdoba, the date is still to be defined.

New services in REDDIG II

2.26 A new Santiago-Lima AMHS circuit was implemented and connectivity tests at P1 level have been conducted between: Brasilia-Montevideo, Brasilia-Bogota, Ezeiza-Santiago, and Ezeiza-Montevideo.

Satellite ADS B services in REDDIG II

2.27 The RCC/20 meeting considered that REDDIG II would be able to support network requirements for the distribution of satellite ADS-B surveillance data, such as availability, latency, multicasting, unicast, and surveillance data segregation to each ANSP connected to it.

2.28 The RCC/20 meeting analysed the connection setup between the satellite ADS-B data processing centre and REDDIG II, which used two communication channels acting in geographical redundancy. In this regard, it was felt that, when defining the two geographical points to be connected to REDDIG II, consideration should be given to the effect of sun outage on REDDIG II to ensure that only one location is affected.

2.29 Likewise, regarding bandwidth usage, it was noted that ADS-B messages were small in terms of bytes and that the link between AIREON and the ANSPs did not require much bandwidth.

2.30 In this sense, in order to determine if the bandwidth available in REDDIG II satellite and ground networks would support a satellite ADS-B bandwidth requirement in a setting in which all REDDIG II member States required satellite ADS-B services to support national procedures in the en-route, approach and terminal areas, the RCC/20 meeting asked AIREON to provide the bandwidth requirement for such environment. The results of this analysis are presented in WP XX prepared by AIREON.

MEVAIII/REDDIG II interconnection activities

2.31 Arrangements were made for the conduction of AMHS trials between the Bogota MTA and the Panama MTA through the MEVA III/REDDIG II interconnection. The MEVA III service provider configured the Panama and Bogota nodes for the trial period at no cost for REDDIG II (maximum circuit of 64Kbits/sec). Following the trials, the MEVA III provider will submit the cost of that service. Likewise, Brazil started coordination with the FAA to migrate the Brasilia-Atlanta AFTN circuit to AMHS through the MEVAIII/REDDIG II interconnection. The FAA is analysing the proposed solution. Furthermore, Peru will start coordinating with the FAA to migrate the Lima-Atlanta AFTN circuit to AMHS through the MEVA III/REDDIG II interconnection.

3 Suggested action

3.1 The Meeting is invited to:

a) take note of the information presented in this working paper;

b) review the activities carried out within REDDIG II as described in section 2 and the associated appendices; and

c) discuss any other related matters it may deem appropriate.

APÉNDICE A

Level3_Unavailability Credits_2016

	January 2016		February 2016		March 2016		April 2016		May 2016		June 2016		July 2016		August 2016		September 2016		October 2016		November 2016		December 2016		TOTAL
	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	Availability	USD Credit	USD Credit
SAEZ																									-
SBBR																					98,99%	8,52			**8,52**
SBCT											99,20%	4,13	99,60%	0,87									99,01%	5,74	**10,74**
SBMN	96,48%	45,36	96,05%	51,83	94,55%	74,31	97,20%	34,52	90,97%	127,98	97,85%	24,78	98,82%	10,26	86,87%	189,45	92,01%	112,43	93,77%	85,93	96,84%	39,94	98,17%	19,89	**816,67**
SBRF			99,59%	1,15					92,31%	77,62					96,58%	32,76					99,06%	6,68			**118,21**
SCEL							99,44%	2,20																	**2,20**
SEGU	93,57%	50,87																							**50,87**
SGAS	97,78%	34,56	99,60%	1,75			97,00%	48,64			99,40%	5,45													**90,40**
SKED																					95,69%	42,13			**42,13**
SLLP																	97,98%	46,39					98,52%	31,78	**78,17**
SMPM							99,41%	16,76																	**16,76**
SOCA	16,68%	1.620,00					99,62%	4,59																	**1.624,59**
SPIM							99,48%	1,85																	**1,85**
SUMU			98,75%	17,08			95,41%	77,31							99,20%	9,00			93,22%	116,73					**220,12**
SVMI							97,13%	56,33			89,77%	217,55	92,82%	150,69									99,53%	3,74	**428,32**
SYGC							99,52%	7,05																	**7,05**
TTZP			99,39%	1,91			99,46%	0,79							99,37%	2,34	94,97%	81,47			97,84%	29,92			**116,42**

Note: SLA-Availability for all nodes: 99.70%
Except for SBMN and TTZP : 99.50%

TOTAL USD 3.633,02

APÉNDICE B

ANÁLISIS INICIAL DE AMENAZAS DE RIESGOS

AMENAZAS	IDENTIFICADAS	CONSIDERACIONES	ACCIONES PROPUESTAS
INTERNAS DE LA REDDIG (Subred Satelital y Subred Terrestre)	Subred Terrestre MPLS LEVEL 3	La red terrestre es sobre MPLS VPN, brindada por un proveedor Level 3, en la cual, el administrador de la REDDIG II, al igual que cualquiera de sus usuarios, no tiene una gestion sobre los dispositivos y mucho menos sobre esta red, supuestamente mallada, y supuestamente, con QoS prevista para priorizar los paquetes pertinentes.	***** Que el proveedorde servicio de la subred terrestre (Level 3) deberia informar si utiliza el estandar de seguridad RFC 592. (actividad realizada) ***** Que se haga uso de NAT en los routers de frontera de los estados entre el nodo de la REDDIG II y la subred terrestre de Level 3, adicionalmente se prodian proceder a la encriptacion de la informacion.
	Accesos remotos a través del internet Publico en la REDDIG II por VPN	En la REDDIG II, el consorcio INEO & LEVEL 3 ha considerado que cada nodo de la REDDIG II tenga instalada una interfaz VPN con el fin de poder acceder remotamente a los equipos de la Red (Routers, MODEMs, amplificadores) en casa de falla o cambios de configuración. A la fecha se tiene VPN en operación en los nodos de Brasilia, Ezeiza y Manaus. Se han instalados VPN en Montevideo (Uruguay) y Guayaquil (Ecuador), pero no están en operación, el consorcio INEO & Level 3 esta utilizando este acceso para corregir problemas en los equipos de los nodos o cambios de configuraciones y lo seguira utilizando hasta que proceda la entrega de la red al Proyecto (RLA/03/901) que ocurrira una vez que se haya realizado la aceptación definitiva de la red, tambien este acceso sera utilizado durante el periodo de garantia (dos años a partir de la aceptación final de la red).	***** Cuando la red pase bajo el control de la OACI, el acceso VPN sera manual bajo requerimiento del Administrador de la REDDIG. De esta forma se reducirian los peligros que presentan al tener siempre conectada a la REDDIG II, redes publicas IP.
	Factores Humanos	La intervencion humana en los nodos de cada sitio, la carga de nuevas configuraciones de software, cargar informacion almacenada en los equipos, etc, debe hacerse con mucha precaucion evitando instalar virus posiblemente instalados en CD o memorias USB.	***** En vista que las manipulaciones ocurren a traves del Sistema de Gestion (NMS) se debera actualizar constantemente el antivirus de la aplicación Whats Up Gold. ***** Una vez que la red sea administrada completamente por OACI, se procedera a cambiar todos los passwords de acceso. Tener en cuenta que en este momento todos los que operanla red conocen los passwords de todos los nodos de la REDDIG II. Solamente el Administrador de la red y aquel personal de cada NCC que este autorice el mismo con un login y password que lo identifique, tendran el acceso a la red. La administracion, configuracion y registro de actividades, estaran a cargo del Administrador de la Red. ***** Las personas a cargo del mantenimiento del nodo solamente tendran acceso a su propio nodo con login y password personales y asignados por el Administrador. ***** Todas las actividades que se realicen en las configuraciones de los equipos de networking quedaran registrados en un servidor al cual tendran acceso el Administrador y donde quedaran registrados todos los accesos y cambios que el personal autorizado haya realizado.
		En el caso de que usuarios realicen cambios en la configuracion de equipos de networking de la REDDIG, y estos cambios resulten contrarios a los deseados o afecten servicios.	* Realizar tareas de Backup de todos los equipos de la red de manera automatica y con tiempos predeterminados para contar ante contingencias, con las configuaciones actualizadas. * Asi mismo el grupo considero la necesidad que el servidor del NMS esta constantemente registrando las configuraciones de los diferentes equipos de forma tal de poder tener grabada versiones anteriores, de esta forma se garantizaria regresar a versiones anteriores en caso de problemas en las nuevas versiones.
Externas a la REDDIG II	Externas de la REDDIG, es decir a nivel de los usuarios que acceden a la Red	Esta parte se refiere del lado de los usuarios de la REDDIG II. A nivel de usuario los tipos de servicio entrante en la REDDIG son circuitos de voz y datos representarian el factor mas importante de vulnerabilidad en cuanto a seguridad de la red.	* A fin de poder identificar los potenciales peligros, se deberia realizar un relevamiento de como estan conectados los circuitos a las interfaces de entrada de las REDDIG II. Este relevamiento permitiria identificar si algunos de los circuitos o servicios que entran en la red vienen de algun red publica. * Que los servicios y circuitos se interconecten a traves de un router de frontera y no directamente a los routers de la REDDIG. * Que los routers de frontera deben tener los firewall adecuados. * Realizar un estudio sobre un firewall estandar para aplicar a todos los routers de frontera y estandarizar el nivel de seguridad en todas las entradas a los nodos REDDIG.
Otras Consideraciones	Los aspectos a considerar tienen que ver con la protección de las frecuencias de la REDDIG II	Otros aspectos a considerar para evitar riesgos en la REDDIG II	* Hacer un inventario de equipamiento licenciado (frecuencia-espectro satelital) por cada nodo. *Registro de los equipos de Estados ya licenciados nacionalmente y/o MIFR, volcados en Base de Datos (software) *Monitoreo y Tracking constante del espectro radioelectrico empleados por los nodos REDDIG, a fin de no ser interferidos y tampoco causar eventuales interferencias. *Con el apoyo o soporte de la UIT hacer control de las amenazas de interferencias invocando al Articulo 45 CS y 15.1 del RR de la UIT. *Grupo de trabajo capacitado para realizar trabajos de control y mitigacion de interferencias.
	Los aspectos tendientes a implementar una adecuada política de Seguridad		* Implementar politicas de Seguridad. * Tener actualizada y disponible la topologia de la red. * Asignar login y password a los responsables de cada nodo, de forma tal de limitar y controlar las facilidades con que cada uno gestionara los dispositivos de networking pertenecientes a la red. *En principio determinar dos tipos: administradores con acceso a toda la red; y usuarios responsables designados con acceso solo a los equipos de su nodo. *Prevenir intentos de acceso por fuerza bruta estableciendo parametros de tiempo para el ingreso de claves en el dispositivo.

APÉNDICE B

ANÁLISIS INICIAL DE AMENAZAS DE RIESGOS

AMENAZAS	IDENTIFICADAS	CONSIDERACIONES	ACCIONES PROPUESTAS
INTERNAS DE LA REDDIG (Subred Satelital y Subred Terrestre)	Subred Terrestre MPLS LEVEL 3	La red terrestre es sobre MPLS VPN, brindada por un proveedor Level 3, en la cual, el administrador de la REDDIG II, al igual que cualquiera de sus usuarios, no tiene una gestion sobre los dispositivos y mucho menos sobre esta red, supuestamente mallada, y supuestamente, con QoS prevista para priorizar los paquetes pertinentes.	***** Que el proveedorde servicio de la subred terrestre (Level 3) deberia informar si utiliza el estandar de seguridad RFC 592. (actividad realizada) ***** Que se haga uso de NAT en los routers de frontera de los estados entre el nodo de la REDDIG II y la subred terrestre de Level 3, adicionalmente se prodian proceder a la encriptacion de la informacion.
	Accesos remotos a través del internet Publico en la REDDIG II por VPN	En la REDDIG II, el consorcio INEO & LEVEL 3 ha considerado que cada nodo de la REDDIG II tenga instalada una interfaz VPN con el fin de poder acceder remotamente a los equipos de la Red (Routers, MODEMs, amplificadores) en casa de falla o cambios de configuración. A la fecha se tiene VPN en operación en los nodos de Brasilia, Ezeiza y Manaus. Se han instalados VPN en Montevideo (Uruguay) y Guayaquil (Ecuador), pero no están en operación, el consorcio INEO & Level 3 esta utilizando este acceso para corregir problemas en los equipos de los nodos o cambios de configuraciones y lo seguira utilizando hasta que proceda la entrega de la red al Proyecto (RLA/03/901) que ocurrira una vez que se haya realizado la aceptación definitiva de la red, tambien este acceso sera utilizado durante el periodo de garantia (dos años a partir de la aceptación final de la red).	***** Cuando la red pase bajo el control de la OACI, el acceso VPN sera manual bajo requerimiento del Administrador de la REDDIG. De esta forma se reducirian los peligros que presentan al tener siempre conectada a la REDDIG II, redes publicas IP.
	Factores Humanos	La intervencion humana en los nodos de cada sitio, la carga de nuevas configuraciones de software, cargar informacion almacenada en los equipos, etc, debe hacerse con mucha precaucion evitando instalar virus posiblemente instalados en CD o memorias USB.	***** En vista que las manipulaciones ocurren a traves del Sistema de Gestion (NMS) se debera actualizar constantemente el antivirus de la aplicación Whats Up Gold. ***** Una vez que la red sea administrada completamente por OACI, se procedera a cambiar todos los passwords de acceso. Tener en cuenta que en este momento todos los que operanla red conocen los passwords de todos los nodos de la REDDIG II. Solamente el Administrador de la red y aquel personal de cada NCC que este autorice el mismo con un login y password que lo identifique, tendran el acceso a la red. La administracion, configuracion y registro de actividades, estaran a cargo del Administrador de la Red. ***** Las personas a cargo del mantenimiento del nodo solamente tendran acceso a su propio nodo con login y password personales y asignados por el Administrador. ***** Todas las actividades que se realicen en las configuraciones de los equipos de networking quedaran registrados en un servidor al cual tendran acceso el Administrador y donde quedaran registrados todos los accesos y cambios que el personal autorizado haya realizado.
		En el caso de que usuarios realicen cambios en la configuracion de equipos de networking de la REDDIG, y estos cambios resulten contrarios a los deseados o afecten servicios.	* Realizar tareas de Backup de todos los equipos de la red de manera automatica y con tiempos predeterminados para contar ante contingencias, con las configuaciones actualizadas. * Asi mismo el grupo considero la necesidad que el servidor del NMS esta constantemente registrando las configuraciones de los diferentes equipos de forma tal de poder tener grabada versiones anteriores, de esta forma se garantizaria regresar a versiones anteriores en caso de problemas en las nuevas versiones.
Externas a la REDDIG II	Externas de la REDDIG, es decir a nivel de los usuarios que acceden a la Red	Esta parte se refiere del lado de los usuarios de la REDDIG II. A nivel de usuario los tipos de servicio entrante en la REDDIG son circuitos de voz y datos representarian el factor mas importante de vulnerabilidad en cuanto a seguridad de la red.	* A fin de poder identificar los potenciales peligros, se deberia realizar un relevamiento de como estan conectados los circuitos a las interfaces de entrada de las REDDIG II. Este relevamiento permitiria identificar si algunos de los circuitos o servicios que entran en la red vienen de algun red publica. * Que los servicios y circuitos se interconecten a traves de un router de frontera y no directamente a los routers de la REDDIG. * Que los routers de frontera deben tener los firewall adecuados. * Realizar un estudio sobre un firewall estandar para aplicar a todos los routers de frontera y estandarizar el nivel de seguridad en todas las entradas a los nodos REDDIG.
Otras Consideraciones	Los aspectos a considerar tienen que ver con la protección de las frecuencias de la REDDIG II	Otros aspectos a considerar para evitar riesgos en la REDDIG II	* Hacer un inventario de equipamiento licenciado (frecuencia-espectro satelital) por cada nodo. *Registro de los equipos de Estados ya licenciados nacionalmente y/o MIFR, volcados en Base de Datos (software) *Monitoreo y Tracking constante del espectro radioelectrico empleados por los nodos REDDIG, a fin de no ser interferidos y tampoco causar eventuales interferencias. *Con el apoyo o soporte de la UIT hacer control de las amenazas de interferencias invocando al Articulo 45 CS y 15.1 del RR de la UIT. *Grupo de trabajo capacitado para realizar trabajos de control y mitigacion de interferencias.
	Los aspectos tendientes a implementar una adecuada política de Seguridad		* Implementar politicas de Seguridad. * Tener actualizada y disponible la topologia de la red. * Asignar login y password a los responsables de cada nodo, de forma tal de limitar y controlar las facilidades con que cada uno gestionara los dispositivos de networking pertenecientes a la red. *En principio determinar dos tipos: administradores con acceso a toda la red; y usuarios responsables designados con acceso solo a los equipos de su nodo. *Prevenir intentos de acceso por fuerza bruta estableciendo parametros de tiempo para el ingreso de claves en el dispositivo.