INTERNATIONAL CIVIL AVIATION ORGANIZATION

SOUTH AMERICAN REGIONAL OFFICE

GUIDANCE ON SECURITY

FOR THE IMPLEMENTATION

OF IP NETWORKS

SUMMARY

This document provides guidance to SAM States for the implementation of the best security practices in the data communication networks of the SAM ATN.

April 2013

TABLE OF CONTENTS

1. INTRODUCTION

This document is a guide to enable SAM States and Organizations to implement the SAM ATN data networks, applying the best information security practices.

1.1 Background

1.1.1 The need for Guidance on Security for the Implementation of IP Networks emerged from the work of the ATN Task Force under the former ATM/CNS Subgroup of GREPECAS (CAR/SAM Regional Planning and Implementation Group). A preliminary document of guidance on security for the implementation of IP networks was presented at the First Coordination Meeting of the ATN Ground-Ground and Ground-Air Applications Project of the GREPECAS CNS/ATM Subgroup (Lima, Peru, 19-20 May 2010). The CNS/ATM had replaced the ATM/CNS Subgroup.

1.1.2 The Sixteenth Meeting of GREPECAS (Punta Cana, Dominican Republic, 28 March to 1 April 2011) approved a new organisation for GREPECAS, dismantling all Subgroups (GREPECAS contributory bodies) and turning them into Programmes and Projects (Decisions 16/45 and 16/47).

1.1.3 All ATN-related tasks, including the drafting of a guide on IP security, were included in Project D1, SAM ATN Architecture, whose main deliverable is the implementation of the new digital network architecture for the SAM Region to replace the exiting REDDIG.

1.1.4 Follow-up on activities under Project D1 is done at the meetings of the SAM Implementation Group (SAM/IG), and submitted for review to the GREPECAS Programmes and Projects Review Group, whose first meeting (PPRC/1) was held in Mexico City on 25-27 April 2012.

1.1.5 With respect to the drafting of a guide on security for the implementation of IP networks, the SAM/IG/10 meeting (Lima, Peru, 1-5 October 2012) analysed the importance of completing such drafting and presenting the guide at the SAM/IG/11 meeting (Lima, Peru, 13-17 May 2013). To this end, the Sixth Meeting of the Coordination Committee of Project RLA/06/901 (Lima, Peru, November 2012) approved the hiring of an expert to draft such document.

1.2 Document Layout

1.2.1 This document has 4 chapters that cover the following information:

Chapter 1 contains introductory information on the guide, as described in section 1.1 of the document.

Chapter 2 describes the main information security aspects, with some concepts contained in ISO/IEC 27000 standards, which depict security as a process that requires the existence of a management system.

Chapter 3 broadly addresses the networks that make up the SAM ATN, with emphasis on the REDDIG II and its interconnection with networks of SAM States, as well as the applications running on it.

Chapter 4 presents the security practices involved in managerial, operational, and technical aspects. These practices aim at the establishment of security controls, which are implemented through technological devices and procedures.

2. INFORMATION SECURITY

2.1 Introduction

2.1.1 The current period in the history of humankind may be called the Information Era, where systems are highly connected through networks, creating, processing, and distributing large volumes of information at high speed.

2.1.2 With the development of new technologies, focused on the intensive use of IT and communication networks, the world has become smaller, creating a global information-based society connected by complex and interconnected networks, using information as a high-value asset. It is an environment where information travels at higher speeds and is accessed through different devices and means of communication, is used for different purposes, generating new information that, in turn, creates new businesses in a cycle of economic and social growth. The paradigm has changed from analogue to digital.

2.1.3 In this context, where information has an economic and strategic value for organisations and is available at any time through different devices connected to the Internet, there is a need for protection mechanisms that guarantee its availability, integrity, authenticity, and confidentiality, among other information security requirements.

2.1.4 It is usually stated that information security is the area of knowledge that seeks to protect information assets from unauthorised access, tampering, or unavailability.

2.1.5 According to ISO/IEC standard 17799:2005, information is an asset that is essential to an organisation's business and consequently needs to be suitably protected, especially in the highly interconnected business environment of today, which exposes information to wide variety of threats and attacks.

2.1.6 Information is available in many forms: it can be printed on paper, spoken, transmitted using electronic media, sent by e-mail, for instance, and stored in magnetic disks or other storage devices. What matters is that all types of information need to be protected to safeguard the organisation's business.

2.1.7 Therefore, information security may be described as the protection of all information from threats in order to ensure business continuity, mitigate business risks, maximise return on investments (ROI) and create new business opportunities.

2.1.8 Within this context, information security is achieved by implementing a set of controls, including policies, processes, procedures, organisational structures, and hardware and software functions.

2.1.9 Since this is a dynamic activity, with new threats emerging every day, a systemic approach should be applied based on process management principles, executing the whole PDCA (*Plan, Do, Check, Act*) cycle, always seeking continuous improvement of the whole system.

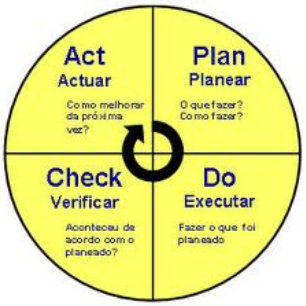


Fig. 1 – The PDCA cycle

2.1.10 Security controls are defined based on legal requirements and market best practices. From the legal point of view, essential controls include:

a) Protection of data and confidentiality of personal information;

b) Protection of business records; and

c) Intellectual property rights

2.1.11 Controls associated to market best practices include:

a) Information security policy document;

b) Assignment of responsibilities;

c) Information security education, awareness, and training;

d) Proper processing in applications;

e) Management of technical vulnerabilities;

f) Business continuity management; and

g) Information security incident and improvement management.

2.2 Basic Concepts

2.2.1 In order to better understand information security aspects, some basic concepts are listed below, based on the ISO/IEC 27000:2007 standards.

a) **Asset:** anything that has value to the organisation. Accordingly, each organisation will determine what is important and requires protection.

b) **Threat:** a potential cause of an unwanted incident, which may result in harm to a system or organisation. Also, any person, entity, or malicious software that may have a reason to exploit a weakness.

c) **Vulnerability:** a weakness of an asset that can be exploited by one or more threats.

d) **Risk probability:** the possibility that a threat exploits some vulnerability and

compromises one or more security principles.

e) **Impact:** the degree of damage that can be caused to an asset when a potential threat exploits a weakness. It is relative, since it depends on the owners' perceived value of the information.

f) **Risk criticality:** a combined assessment of the probability of occurrence and the impact of a risk. Criticality depends on three factors: threats and probabilities—which determine risk probability—and impact. Once criticality has been defined, it is possible to establish security controls to protect the asset.

g) **Risk:** combination of the propability of an event and its consequences.

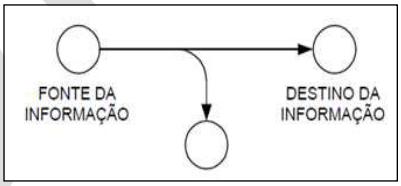
h) **Incident:** one or a series of unwanted or unexpected information security events that have a high probability of compromising business operations and threatening information security.

i) **Event:** an identified occurrence of a condition of the system, service, or network that indicates a possible information security breach, lack of controls, or a previously unknown situation that may be relevant to information security. Take note that an information security event is anything that merits investigation by those responsible for information security. However, not every event is an information security incident.

2.3 Information Security Principles

2.3.1 According to ISO/IEC 27002:2007, the most important properties of information, also called information security principles, that need to be preserved are:

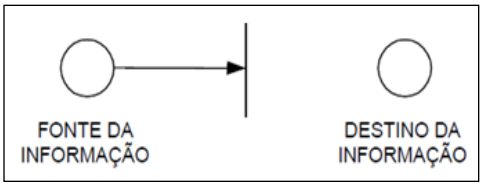
a) **Confidentiality:** property of a system that prevents unauthorised users from accessing information delegated to authorised users only. Breaches of confidentiality may occur through interception. The following figure illustrates that situation:



Source: SANTOS (2011)

Fig. 2 – Breach of confidentiality

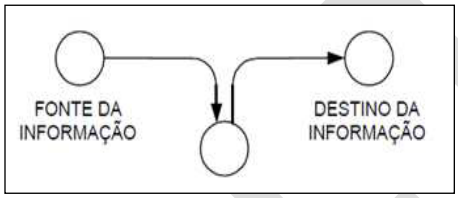
b) **Availability:** the number of times the system performed a task requested without internal failures, for the number of times the task was requested. Loss of availability may occur due to power outage.



Source: SANTOS (2011)

Fig. 3 – Loss of availability

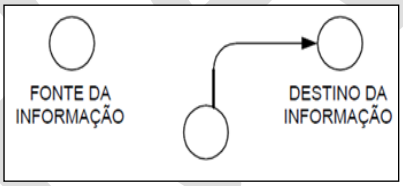
c) **Integrity:** security attribute that indicates if a piece of information can be altered only as authorised. Loss of integrity may occur due to modification.



Source: SANTOS (2011)

Fig. 4 – Loss of integrity

d) **Authenticity:** capacity to guarantee that a user, system, or piece of information is **what it claims to be**; and



Source: SANTOS (2011)

Fig. 5 – Loss of authenticity

e) **Non-repudiation:** the ability of the system to prove that a user has executed an action in the system. Consequently, the user cannot deny being the author of the action.

2.4 Current Scenario

2.4.1 Modern world dynamics impose a series of threats on information system managers that can have a significant impact on the business. Such threats seek to exploit the existing vulnerabilities of networks and applications. Consequently, it is important to know the threats, but even more important is to know the vulnerabilities and apply controls to mitigate them.

2.4.2 The current scenario is affected by modern network features, mainly:

a) **Automation:** current networks are highly interconnected, which has changed the way attacks are performed. Attacks are made in a distributed manner, using thousand of computers to do in minutes what would take years with a single piece of equipment. One example is the DES (data encryption standard) encryption being broken sooner than expected.

Fig 6 – Automation increases the power of the attacker

b) **Remote action:** Progress in network interconnection has eliminated physical barriers and shortened distances, enabling attacks on assets to be made from miles away, or hindering identification and the adoption of punitive action, since legal aspects of different States are involved.

c) **Anonymity:** The sensation of anonymity, of being "invisible", is appealing to the bad guys in committing their criminal acts, and results in a large number of attacks for different purposes.

d) **Collaboration:** Nowadays, it is very easy to share information through the interconnected networks, enabling fast and long-distance dissemination of vulnerabilities in networks, applications and operating systems, based on which an individual can develop and disseminate an application to exploit a given vulnerability.

2.5 Threats, Attacks and Vulnerabilities

2.5.1 Vulnerabilities are weaknesses in information systems, processes, equipment, and networks, which can have an impact on organisations, affecting their business.

2.5.2 According to Carnegie Mellon University's CERT, 99% of network intrusions result from attacks against known vulnerabilities or configuration errors that can be fixed. Secunia published a report showing the top 6 impact classes occurred during the first half of 2010, namely:

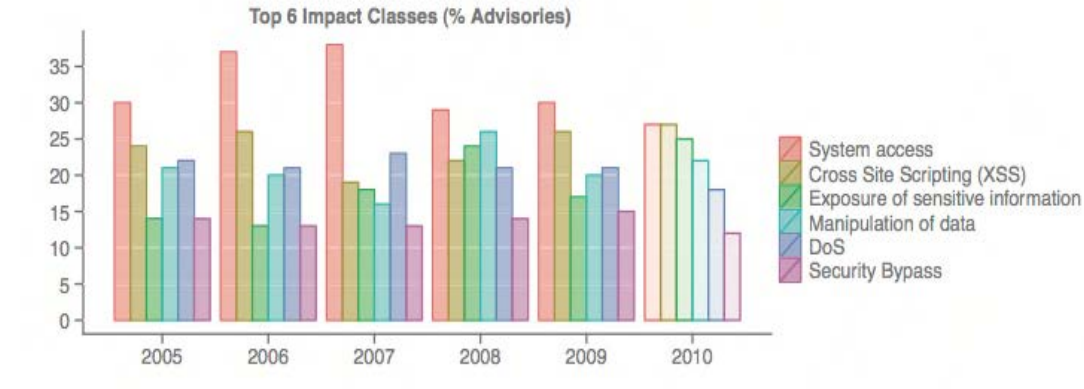


Figure 5 Distribution and evolution of the six most prevalent impact classes since 2005. The plots include a linear extrapolation for 2010 based on the data of the first half of 2010.

Source: Secunia – Half-Year Report, 2010

2.5.3 Vulnerabilities can be classified into the following types:

a) Physical: those related to facilities, such as access control, electric power, air conditioning, fire, flood, etc.

b) Hardware and software: those related to equipment and application failures.

c) Communication: weaknesses associated to data communication systems; and

d) Human: those related to weaknesses in awareness raising and training of technicians and system and equipment operators.

2.5.4 Attacks exploit vulnerabilities in order to cause damage to some organisation, affecting one or several information security principles, whether to interrupt its operation or to obtain strategic information or to modify some financial document. Some damages are listed below:

a) Unauthorised network access;

b) Exposure of confidential information;

c) Damage to, or tampering with, information;

d) Provision of data for identity theft;

e) Exposure of organisational secrets;

f) Fraud;

g) Interruption of business operations; and

h) Triggering life-threatening accidents.

2.5.5 Attacks may be against data, lines of communication (networks), or hardware and software.

a) Data: attacks on data affect the following security principles: confidentiality, integrity, authenticity, and non-repudiation;

b) Networks: attacks on networks affect the following security principles: availability, confidentiality, and integrity;

c) Hardware: attacks on hardware mainly affect the availability principle; and

d) Software: attacks on software affect the following security principles: confidentiality, integrity, and authenticity.

2.5.6 The following table summarises the types of threats to security principles:

THREAT	SECURITY PRINCIPLE			
	AVAILABILITY	**INTEGRITY**	**CONFIDENTIALITY**	**NON-REPUDIATION**
HARDWARE	Theft of equipment Deactivation Power outage Fire Flood Heat	NA	NA	NA
SOFTWARE	Programmes disabled	Tampering with a running programme	Unauthorised copy	Log files disabled
DATA	Files disabled	Creation of new files Tampering with existing files	Unauthorised access	Tampering with file properties
NETWORKS	Messages disabled or destroyed	Tampering with messages	Unauthorised access to messages	Log files disabled

Table 1 – Security threats

2.5.7 Attackers can be from outside or inside the organisation. External attackers use external connections to the organisation's networks. Insiders already have direct access to systems, networks, hardware, and business data.

2.5.8 Basically, an attack is made in two stages:

a) Search for vulnerabilities; and

b) Exploitation of vulnerabilities.

2.5.9 Therefore, it is important to know some information gathering techniques used by attackers, as well as some applications that exploit such vulnerabilities.

Information gathering techniques

2.5.10 There are several techniques to gather information on network infrastructure and information systems. The most common are listed below:

- **Social engineering**

2.5.11 This technique does not require much knowledge about networks or applications, since it uses persuasion, exploiting the naivety or trustfulness of the user to acquire information that can be important for breaching the security of a system. Consequently, the attacker focuses on individuals rather than technology.

- ***Phishing***

2.5.12 This technique is aimed at acquiring information by sending an unsolicited message to the victim, purporting to be a legitimate message from a trustworthy financial institution, a government body, a multinational company, or a popular website. The message contains a link to a fake website, almost identical to the legitimate one, directing the user to enter data, such as logins and passwords.

- ***Packet Sniffing***

2.5.13 These are software tools installed in devices promiscuously connected to a network to capture data contained in message packets passing over the network.

2.5.14 This gathering technique is also used by network administrators to monitor network performance, and is also known as protocol analyser.

2.5.15 The search for vulnerabilities is done using software tools to identify the features of the most frequently used applications and systems of the organisations. The technique consists of obtaining responses from the system to some queries made by the scanner.

2.5.16 It is a technique used by attackers to search for information about services available in a network or system through the ports used by communication protocols, such as TCP/IP.

2.5.17 Knowing a port is open the attacker can invade the network and gain information or interrupt the operation of a network or system. There is no way of preventing the identification of open ports, since the technique consists of sending connection requests, similar to those from a legitimate network user.

- **Vulnerability Scanning**

2.5.18 The search for vulnerabilities is made using software tools that identify the features of the applications and systems most widely used in the organisations. The technique consists of obtaining responses from the system to some queries made by the scanner. Examples of the information that may be acquired:

a) Type and version of the operating system;

b) Manufacturer of the network interface;

c) Network (IP) or link (MAC) address;

d) Open communication ports;

e) Software versions; and

f) Password defaults in network and security assets.

Exploits or malicious codes

2.5.19 Better known as malware, they trigger a sequence of events for exploiting vulnerabilities and compromising the network or system.

2.5.20 Some malware examples are listed below:

- **Viruses**

2.5.21 A computer programme that infects a computer by executing a legitime but infected software. Consequently, a virus relies on another software to infect the computer and spread.

- ***Worm***

2.5.22 A programme that spreads automatically throughout the networks and does not need to be explicitly executed by a user or software. Thus, it does not rely on another software to infect the computer. A characteristic of worms is that they consume much of the network and system resources.

- ***Spyware***

2.5.23 These are malicious codes aimed at gathering information entered in web forms, website hits, etc. Consequently, this data gathering technique requires prior infection by malware.

- ***Loggers***

2.5.24 Basically, this is software that captures information contained in computers. There are *keystrokeloggers*, that record the keys struck on the keyboard, and *screenloggers*, which capture the image on the screen.

- ***Trojans***

2.5.25 These are programmes that appear to contain something useful for the user but instead contain malicious codes.

- ***Exploits***

2.5.26 Programmes (or programme *kits*) that make it easy to exploit known vulnerabilities of operating systems and applications. Do not require much knowledge about networks or information systems.

2.5.27 Some denial-of-service attacks are described below:

- ***IP spoofing***

2.5.28 In a *spoofing* attack, an entity successfully impersonates another entity. In the case of IP *spoofing*, the attacker can forge a source IP address by sending source IP packets from an IP address other than its own, pretending to be another machine. The forging of IP addresses is mainly used in denial-of-service attacks, where the attacker needs many of the responses to be sent not to him/her but to the target machine.

- ***DNS spoofing***

2.5.29 In this attack, the DNS server of the target host is invaded and incorrect name and address entries are introduced. Consequently, when a user application uses a specific name that has been modified, it will communicate with a fake entity. For example, if the IP address DNS of a web page has been changed the browser will redirect the user to a fake page without reporting what address is being used (that is what DNS, browsers, etc. are used for). The server hosting this fake page is prepared by the attacker to capture user information without the user being aware of it.

- ***ARP spoofing***

2.5.30 ARP *spoofing* is an identity theft technique in which the attacker tries to impersonate a legitimate addressee of a communication in response to ARP queries sent by the traffic source. The attacker's response is sent under the broadcast domain before the addressee has a legitimate chance to do so. Thus, both the source equipment and the switch learn a fake mapping between the MAC address (the attacker) and the IP address (the legitimate addressee). All frames are incapsulated by the source with the MAC address of the attacker and are switched using the switch in the port where the attacker is based in the MAC.

- ***DoS***

2.5.31 A DoS (*Denial of Service*) attack is an attempt to make a given service, system, or network unavailable. Many of the techniques used are known as flooding and target the servers used by several users, such as a DNS and websites.

2.5.32 An expanded version of this type of attack is the DDOS (*Distributed Denial of Service*), where the attacker uses several machines to attack a given service, server, or system.

3. THE SAM ATN

3.1 Introduction

3.1.1 The ICAO CNS/ATM concept contemplates that the new services will be supported by the ATN (*Aeronautical Telecommunication Network*), which encompasses the regional networks. In the case of the SAM Region, the SAM ATN consists of a regional digital network--the REDDIG II--and the networks of each State.

3.1.2 In order to meet operational requirements, the REDDIG II was conceived with two backbones—a satellite and a ground backbone-- and must guarantee:

a) That it has satellite routing devices, equipment and links, as well as ground services, with all the channel interfaces that the existing network (REDDIG) currently has, adding those required to support future services based on the CNS/ATM concept;

b) Widespread application of the IP protocol in the transportation network for aeronautical voice and data communications;

c) The establishment of suitable service quality parameters;

d) Continued operation of analogue services where still required (AFTN, radar data of old equipment, etc.);

e) Continued connection with the MEVA II network;

f) Continued centralised and common network administration;

g) That the high degree of availability achieved by the existing REDDIG is maintained;

h) That it serves as the means for regional integration of national network systems developed by the States of the Region; and

i) Cost-effective support to regional communications with a high level of reliability, availability, and minimum delay.

3.1.3 The minimum characteristics of REDDIG II are:

a) Satellite and ground access;

b) Meshed, flexible, multiprotocol, multiservice and external area topology;

c) Scalability and easy expansion;

d) Satellite and ground redundancy and routings;

e) Open architecture, based on the IP protocol;

f) Possibility of migrating to other network technologies.

3.1.4 Note is taken that the IP protocol has been defined for the implementation of the new REDDIG, and that there are two backbones—a ground and a satellite backbone—with redundant equipment to guarantee high reliability, availability and a minimum delay.

3.1.5 Another important feature is compatibility with the protocols and services of the current REDDIG, including analogue services, like AFTN.

3.1.6 Plans involve using the TCP/IP protocol for the satellite network, under the administration of the SAM States, and operated by ICAO, while the ground network will use MPLS, as a service provided by a private company.

3.1.7 Studies conducted by experts suggest an availability of 99.999985002% of the combined (satellite and ground) network, amounting to a monthly unavailability of 0.02 min/month.

3.1.8 The following figures illustrate the topology contemplated for REDDIG II:

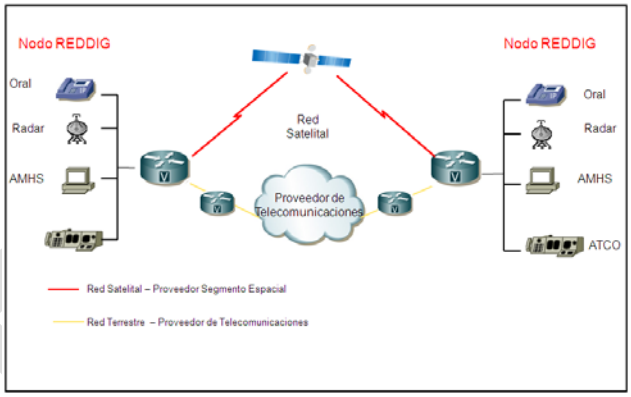


Fig 8 – REDDIG II – Topology

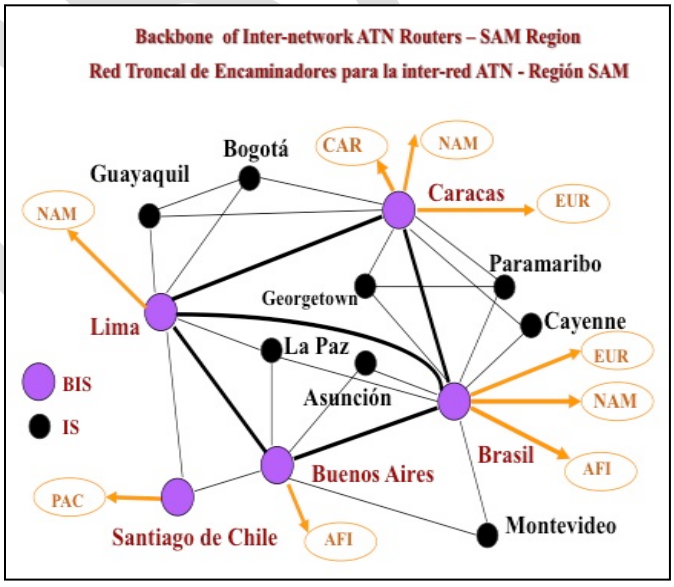


Fig 9 – REDDIG II – Points of interconnection

3.2 ATN Services

3.2.1 The list of service requirements to support air navigation in the SAM Region, including those for the short, medium, and long term, to be carried over the REDDIG II, include:

Current Services

3.2.2 Those resulting from the requirements contained in the CAR/SAM Air Navigation Plan and which, at present, are mostly operational, namely:

a) Table CNS1A (AFTN Plan); and

b) Table CNS1C (ATS direct speech circuits plan).

Future Services

c) Those resulting from the MEVA II – REDDIG interconnection;

d) Teleconferencing service for flow management units (FMUs) or flow management positions (FMPs), to be provided on a daily basis among all the units of the Region, initially for twenty users;

e) Flight plan and/or radar information exchange using conventional methods, in accordance with the respective MoUs (Memoranda of Understanding) signed or to be signed;

f) AMHS interconnection requirements, to gradually replace the AFTN service, in accordance with the respective MoUs (Memoranda of Understanding) signed or to be signed;

g) AIDC interconnection requirements, to gradually replace the ATS speech service;

h) ADS-B data exchange and multilateration among all the ACCs of adjacent FIRs;

i) Interconnection of automated systems using Asterix 62 and 63, among all the ACCs of adjacent FIRs.

j) AIM requirements: In this regard, there is no concrete requirement to date.

3.3 Technical Characteristics of the Routing System

3.3.1 From an information security viewpoint, one of the most important assets of REDDIG II are the routers, which have the following technical characteristics:

a) The minimum amount of memory necessary to perform all the functions required, in accordance with the recommendations of the manufacturer.

b) SNMP and MIB-II management protocols implemented in accordance with RFC 1157 and RFC 1213, respectively.

c) Gateway functionality for voice over IP for all the required functions.

d) Features required for the implementation of RTP/RTCP and RTP "header compression" protocols in accordance with RFC 2508.

3.3.2 Routers permit:

a) Traffic prioritisation by type of protocol and by service of the TCP/IP protocol stack.

b) The use of protocol to establish service classes, with band reservation, to ensure prioritisation of critical applications, in accordance with the defined IP standards (RFCs).

c) Interoperability, including for VoIP, with various types of Cisco routers that already exist in the REDDIG nodes.

d) Remote access allowing for at least five (5) simultaneous connections, using different levels of coding to restrict equipment and command configuration that could alter its operation.

e) Interconnection with the routing system of the ground service provider.

f) Management of alternate routing to the automatic ground MPLS backbone in case of failure.

g) Header compression, TCP acceleration, and load balancing techniques.

h) The availability of all ports needed to meet current and future requirements.

i) The establishment of permanent and switched voice and data communications. Switched communications will be established at the request of the user.

j) The establishment of closed user groups for telephone and data traffic.

k) The inclusion of metrics for automatic establishment of paths to minimise delay in communications within the available network bandwidth.

l) Facilities for defining circuits, addressing, transmission rates, and traffic prioritisation, applying quality of service (QoS).

m) The establishment of private IP networks (VPN) and the interconnection with public networks.

n) The inclusion of the elements required for network synchronisation.

o) Integration into the network management system (NMS).

3.3.3 Routers implement routing protocols:

a) RIPv1 (RFC 1058).

b) RIPv2 (RFCs 2453, 1723, and 1724).

c) EIGRP.

d) OSPF version 2, in accordance with the following RFCs (RFC 2328, RFC 1793, RFC 1587, and RFC 2370).

e) BGPv4, in accordance with RFCs 4271, 4272 4360, 4374, 4451, 4456, 1966, 1997, 2796, 2439, 2858, 2918.

3.4 Fault tolerance and recovery

3.4.1 The REDDIG II satellite backbone architecture and the systems involved in the provision were designed as fault-tolerant, and there is not a single common element whose failure will disrupt the services provided by the network. Any failure will only cause gradual degradation of services provided by the network. The following figure illustrates the general fault-tolerant structure:

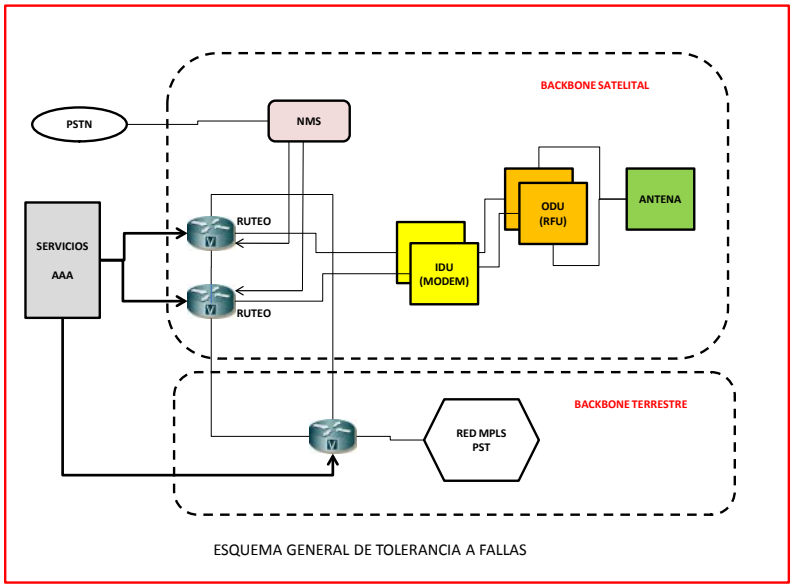


Fig 10 – Fault tolerance

3.5 Access Network

3.5.1 The ground backbone will be provided by a private enterprise and will have a monthly availability of at least 99.5%, with a delay of less than 60 ms and an error rate of less than 10-7, 99.5% of the time. It will act as a multi-service infrastructure and shall run on a multi-service IP platform, logically independent and isolated from any other network, especially from the public environment of the Internet. This network will permit the creation of VPN and the implementation of QoS.

4. SECURITY PRACTICES FOR THE SAM ATN

4.1 Security Objectives

4.1.1 In order to meet the operational requirements of ATM services, the ATN must meet the following fundamental security objectives:

a) ATN data protection against unauthorised access, modification or unavailability; and

b) ATN asset protection against unauthorised use and denial of service.

4.1.2 These objectives require the application of the aforementioned information security principles, but with different degrees of relevance, as follows:

a) Integrity;

b) Availability;

c) Confidentiality;

d) Authenticity;

e) Non-repudiation; and

f) Accountability.

4.1.3 Based on the intrinsic characteristic of civil aviation whereby it is very important for all stakeholders to have access to flight information, confidentiality is not as critical as integrity and availability. Consequently, security measures, or controls, must recommend the adoption of actions that guarantee compliance with these principles as a matter of priority, based on a cost-benefit analysis of each action. That is, the protection effort must be proportional and suited to the need for protection. In this regard, it is important to take into account the criticality of the risks associated to the activity, based on knowledge of the threats, probabilities, vulnerabilities, and the respective impact.

4.1.4 Security principles are implemented through a series of information security controls, as defined in ISO/IEC standard 27000, which may be classified as:

a) Management controls;

b) Operational controls; and

c) Technical controls

4.1.5 The following figure describes the relationships between ATN security objectives, security principles, security controls and security actions:

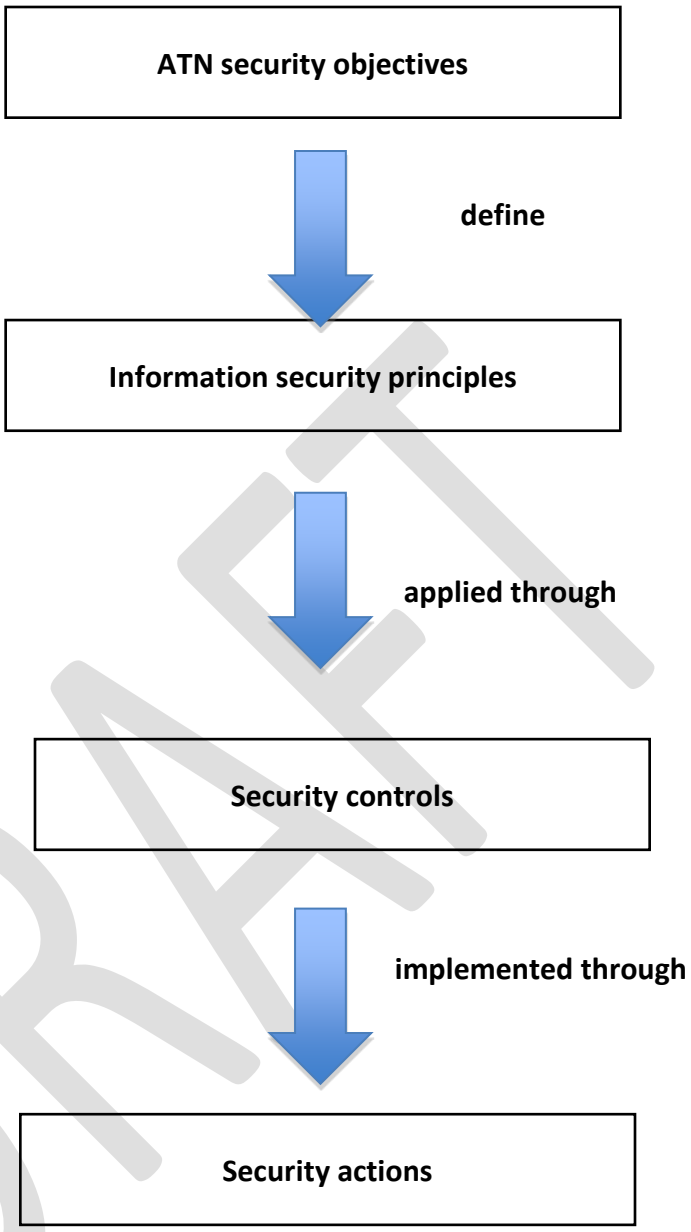


Fig 11– Security objectives

4.2 Security Strategy

4.2.1 The security strategy adopted is based on the "Defence in Depth" concept, whereby multiple security layers are implemented to create a broad defence structure that protects information against attacks. Its conception is strongly supported on the intensive use of current techniques and technologies, involving cost balancing, protection capacity, performance, and operational aspects.

4.2.2 An important part of this concept is balancing the three main information security elements: People, technology, and operations:

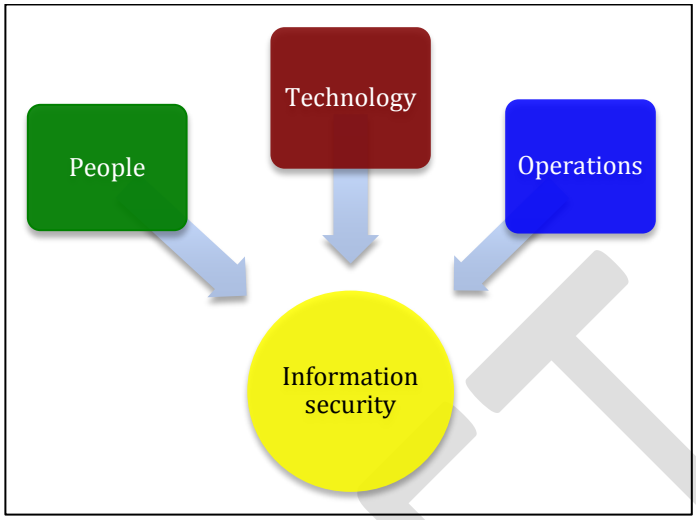
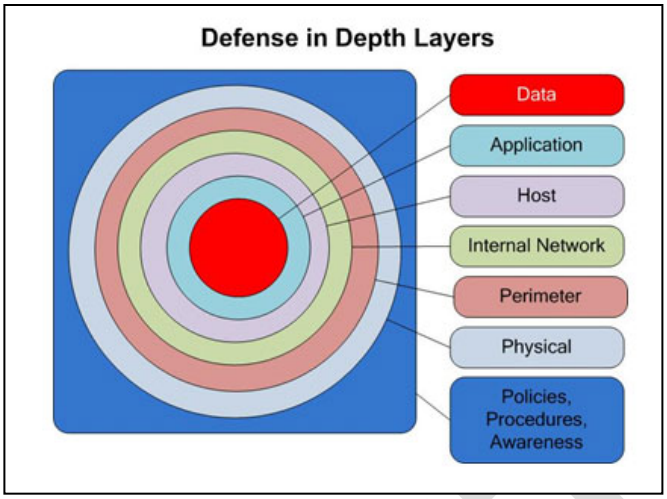


Fig 12– Security elements

a) **People:** Involves aspects related to the establishment of policies and procedures for defining rules and responsibilities; the conduction of training for creating a security culture amongst technical personnel and operators; and measures to control physical access to critical facilities.

b) **Technology:** Involves the establishment of policies and processes for acquiring quality tools and products, as well as the adoption of the following principles:

- Defence in multiple areas, focusing on the network, the infrastructure, the perimeter, and the IT environment;
- Detection and protection measures, with the necessary infrastructure to prevent intrusion, to analyse and correlate results, and to react accordingly.
- Layered defence: consists of implementing various defence mechanisms or controls between the enemy and its target. Each mechanism must present unique obstacles. The following figure illustrates this principle, showing the data, application, equipment or host, internal network, perimeter network, and physical environment layers, and encompassing them all, the policies and procedures.



Source: www.personal.psu.edu

Fig 12 – Defence in Layers

c) **Operations:** Focuses on all the activities required to keep the organisation protected on a day-to-day basis. It includes:

- Maintenance of the security policy;
- Management of the security attitude;
- Security assessments;
- Monitoring;
- Detection, alarm and response to attacks;
- Recovery and restoration.

4.3 Security Controls

4.3.1 The strategy is implemented through security controls applied to the three elements: people (considered within the context of management), technology, and operations.

4.3.2 Management Controls

4.3.2.1 **Certification, Accreditation, and Security Assessment:** To ensure that Management evaluates the security controls in its systems and authorises the operation.

4.3.2.2 **Planning:** To ensure that Management develops and executes a security plan.

4.3.2.3 **Risk and vulnerability management:** To ensure that Management assesses the risks and the criticality of damages caused by an attack.

4.3.2.4 **Awareness and training:** To ensure that technicians and operators are aware of security risks associated to their respective activities and know the security policies applicable to their areas of action, and are duly trained for responsible and proper performance of their activities.

4.3.2.5 **Acquisition of systems and servicess:** To ensure that management allocates the resources required for proper protection of information.

4.3.3 **Technical Controls**

4.3.3.1 **Access control:** The ability to limit access to services and resources to only authorised individuals, taking into account what each individual is allowed to use from a given resource or system.

4.3.3.2 **Identification and authentication:** The ability to identify and authenticate users of a system or other resources.

4.3.3.3 **Protection of communications:** The ability to monitor, control and protect communications.

4.3.4 **Operational Controls**

4.3.4.1 **Configuration management:** To ensure control of system components, including hardware, software, and system adjustment parameters.

4.3.4.2 **Response to incidents:** To ensure that security incidents are properly addressed and communicated to the respective authorities.

4.3.4.3 **Contingency plan:** To ensure that operators have a plan to ensure continuity of operations for users and of the most critical services in case of emergency.

4.3.4.4 **Data protection:** To ensure the protection of data and system storage measures.

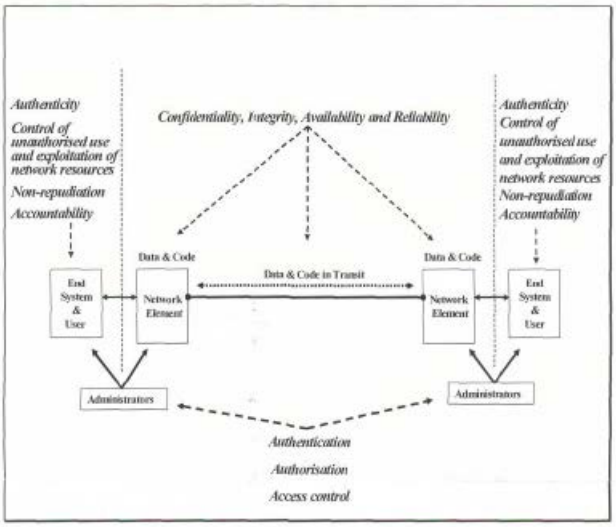
4.3.4.5 **Protection of facilities:** To ensure controlled access to premises.

4.4 **Network Security**

4.4.1 Taking into account the internal and perimeter network layers of an organisation and those of REDDIG II, based on the "defence-in-depth" strategy, some aspects that every organisation should take into account are described below.

a) Every organisation must develop, implement, and update a security plan for the networks under its responsibility, taking into account the security objectives previously described in this guide;

b) A network risk management process must be in place, taking into account the following scenario, in accordance with ISO/IEC 120-28-1:2006:



Source: ISO/IEC 18028-1:2006

Fig 13 – Network risk areas

c) Consequently, network vulnerabilities must be taken into account, based on the following possibilities:

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.	

Source: ISO/IEC 18028-1:2006

Table 2 –Network vulnerabilities

d) Management must secure the resources necessary to protect the information, including network assets (routers, switches, etc.) and security assets (firewalls, IDS, IPS, etc.).

e) Maintenance and operations teams must be aware of, and trained in, the security measures required by the security plan.

f) Equipment and systems must have security certification.

g) Network topology should contemplate security aspects, taking into account at least the following:

- The points of interconnection with other networks must have security assets, such as firewalls and IDS/IPS, installed and duly configured and monitored.
- Information about IP addresses should not be available on the Internet.
- Firewalls must be configured based, at least, on the following rules:
  - Deny all policy as default;
  - Only outgoing *web* protocols (*e.g.*, http, https)*;*
  - Two-way e-mail protocols.
- Routers must be configured taking into account the use of ACLs and NAT, and also to hide IP addresses.
- Routers must be constantly updated, using passwords and logins different from those originally set in the factory.
- Network interconnections with REDDIG II must be established with asset redundancy (including security assets) and other provisions to ensure information availability and integrity and network performance according to specifications.
- Connections with public networks (Internet) must have a topology that ensures multi-layered security.
- The SNMP v3 protocol must be used to manage the network, with activation of alerts and SNMP traps. Safe authentication must be required to access the devices.
- Administration links must be encrypted.

h) Communication lines critical for State network interconnection to REDDIG II must be constantly monitored;

i) A network configuration management process must be in place, with procedures for updating software versions and changes made to hardware and connection points, and also to keep backup copies of the installation software;

j) Specific procedures are needed to control physical and logical access to network equipment and systems, using safe codes, identity identification equipment, such as magnetic cards, biometrics, etc. The original logins and passwords of routers and other network and security assets must be deactivated;

k) Equipment and systems critical to network operation, supervision, and monitoring must have continuous power supply and proper temperature control;

l) Network and security systems, applications, and assets must be configured to execute only services that are really necessary (*hardening*), deactivating those services that are not required for the operation, such as FTP, DNS, etc.;

m) Security incident response teams must be in place to ensure the implementation of the necessary protection measures;

n) A specific team is needed to monitor the status of security equipment and assets, such as firewalls, IDS/IPS, etc.;

o) Use of VPN is recommended for providing communications that require information confidentiality and integrity. In thses cases, the following aspects must be taken into account:

- Security at endpoint and termination point;
- Protection against malicious software;
- Authentication;
- Detection of intruders with IDS/IPS;
- Use of firewalls; and
- Use of the "split tunnelling" technique.

p) The networks that support IP convergence with voice and data traffic must take into account at least the following:

- Use of QoS to define data transmission priorities;
- All VOIP servers must be configured with protection against malicious software;
- VOIP devices, such as computers with softphones, must have activated personal firewalls and constantly updated anti-virus programmes;
- VOIP servers must be located on a network protected by firewalls and IDS/IPS;
- Only communication ports that are strictly necessary to support VOIP must be available;
- All access to the servers must require authentication.

q) Remote access (RAS) must be implemented taking into account at least the following:

- The use of firewalls;
- Routers with ACL;
- Encryption of external links, especially those connected to the Internet;
- Strong authentication;
- Updated anti-virus; and
- Ongoing auditing.

r) Wireless networks (WLANs) must be implemented taking into account at least the following:

- Interconnections with the main network infrastructure must be protected by firewalls;
- Implementation of VPN for the connection between a client and a perimeter firewall;
- Clients (computers, laptops, smartphones, etc.) must have personal firewalls and anti-virus systems;
- The SNMP protocol must be configured as read-only;
- Use of SSH for link management; and
- Network access devices must be located in physically secure premises.

REFERENCES

ABNT. Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 - Tecnologia da Informação-Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação. Brazil, 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. Final version. Lima, Peru, 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. Brazil, 2011.

STALLINGS, William. Network Security Essencials - Application & Standards. 4th Edition. Prentice Hall. USA, 2011.