



Security Management in RED.ES

Ricardo Marin Beltran
Security Area

Ricardo.Marin@red.es

INDEX

- 1.- Introduction to RED.ES
- 2.- Security Management
- 3.- Summary



1.1 Who's RED.ES?

- **Red.es** is a public company, appointed to the Spanish Science and Technology Ministry across the Telecommunication State Secretarial.



1.2 Company Functions

- a)** Register country name domains .ES.
- b)** Participate in the ICANN Organs that coordinate the management of the domain and name registration.
- c)** Observe the telecommunication sector and Information Society.
- d)** Make studies, reports and the advisement to the Spanish State in all matters relative of Information Society.
- e)** Promote and develop the Spanish Information Society.



1.3 Current Services

- Registration of second and third level (com/edu/gob/nom/org.es) country name domains .ES
<http://www.nic.es>



Second Level domains 50.000 (Jan'04)

Third Level domains 20.000 (Jul'03-Jan'04)

1.3 Current Services

- Antivirus Alert Center
<http://www.alerta-antivirus.es/>






FREE SERVICE:
 Security and virus
 information, On-line
 subscription to receive
 alerts of new viruses and
 security problems,
 Forums about virus and
 security

1.3 Current Services

- Development of E-Administration plan:
 - Telematic Notification to citizens and Administrations.



- Home Change. 
- Documentary Archive. 
- Telematic Register. 

1.3 Current Services

- Web pages construction for the development of the Spanish Information Society.

www.lssi.es



www.constitucion.es



www.navegacion-segura.es



- Introduce Internet in Schools and Libraries.



1.4 Future Services

- Spanish Historical Inheritance digitalization.
- IPv6 plan.
- Mail Quality.

INDEX

- 1.- Introduction to RED.ES
- 2.- Security Management
- 3.- Summary

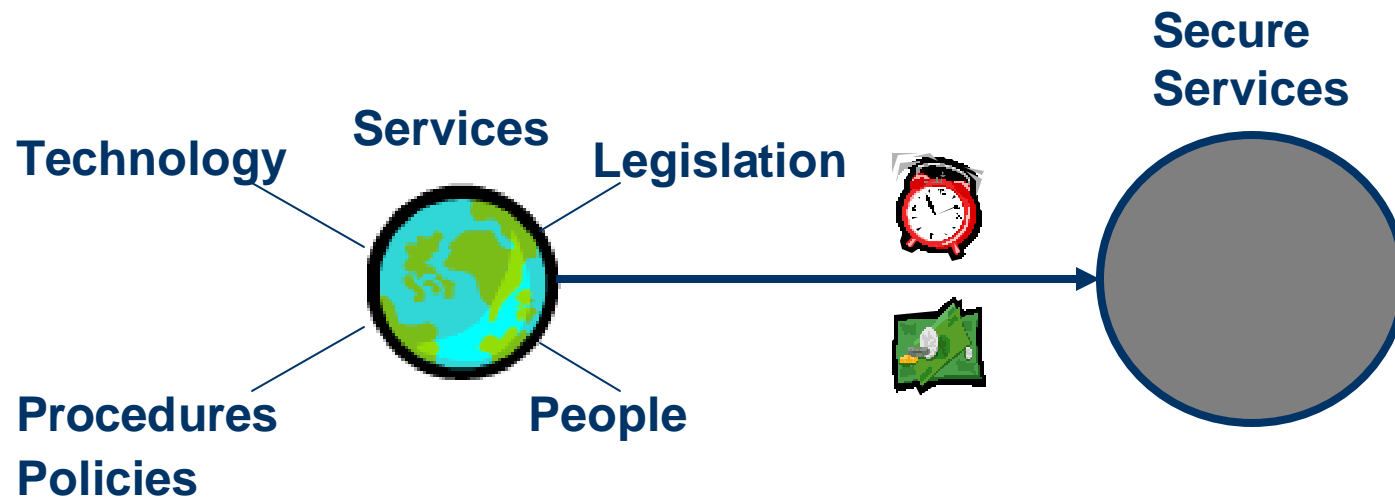
2.1 The starting point



The three main milestones of the security for RED.ES are:






- “It’s necessary guiding the security to the business identifying the assets value of information for the company and minimizing its risks”.
- “We have to apply a global security strategy”.
- RED.ES must offer reliable and secure services to the information society.

2.2 Secure Services





Services: DNS Servers, Web Servers, Mail Servers, Application Servers (Web, Client/Server), Databases, Communications (equipment, lines, networks), Logon Servers, Users

2.3 Technology

- Routers: Internet and internal connectivity with ACLs. 
- Firewalls: External and Internal. 
- Antivirus: Desktop and Servers with automatic pattern update. 
- IDS: Host (HIDS) and Network (NIDS) that analyze traffic of Internet, public servers, and internal networks.  IDS
- NAT: applied in routers and firewalls.
- Encrypt: Database, data sent (SSL). 

2.3 Technology

- Certificates and digital signatures: Communications between organism and citizen or organism and organism. 
- Monitoring Systems: Availability of networks and systems. 
- Logs Analyzers: Tools for classifying logs and detect possible failures and/or attacks in the equipment.
- Ethical Hacking tools: Sniffers, Port scanners, detector of vulnerabilities to determine systems's security.

2.4 Procedures and policies

- Preventives: Before a security incident. Like review logs, monitoring/update systems, backups, contingency plan of systems, ethical hacking.
- Detection: During a security incident. For example: warnings of users/systems, detection of strange behaviour in the systems.
- Correctives: After a security incident. We must do: evaluate the damages, fix the cause, repair the damages, learn and write about the incident, implement the contingency plan of affected system/s.

2.5 People



- Security formation of users, administrators and responsables people.
- Definition of responsables people of the company's information.
- Definition of access roles to the information (users , administrators, responsables people).
- Definition, execution, implantation of procedures and policies.
- The revision of procedures and policies.
- Analysis and study of new technologies.

2.6 Legislation



- Adaptation to the Spanish Data Protection Law.
It establishes a set of security measures of compulsory fulfilment for companies and organisms.
- Orientation toward the regulations ISO 17799.
Code of good practices for the management of the information security.
- Know and fulfil current and future laws related with information society that affect our company (LSSI, Electronic Signature).

3. SUMMARY

- Our business comes from the connectivity to Internet, for that reason we must protect strongly our systems of internal and/or external attacks.
- RED.ES guides the security to the business utilizing technology, procedures/policies, people and fulfilling with the applicable laws.

Questions?

Questions?

Ricardo Marin Beltran

Security Area

Ricardo.Marin@red.es

<http://www.red.es>