

Puesta en marcha del CSIRT y Gestión de Seguridad de la Información de ANTEL

Eduardo Carozo
Leonardo Vidal

JIAP
agosto de 2007



Agenda

- Amenazas en Internet
- Botnets, DDoS
- Honeypots, Honeynets, Spampots
- CSIRT <--> SGSI
- Seguridad de la Información
- Riesgos e impactos
- Política de Seguridad
- Colaboración con el Gobierno Electrónico

Amenazas en Internet

100 BEST PLACES TO WORK IN IT 2007 VIEW NOW

COMPUTERWORLD
Security

JUMP TO More Resources

News > Security

Storm worm botnet threatens national security?

Liam Tung, ZDNet Australia
20 August 2007 12:49 PM

In just eight months the Storm worm has infected more than 20 million computers and built a zombie army -- or botnet -- capable of launching DDoS attacks that could be used against any organisation or even damage critical infrastructure, according to security experts.

The Storm worm was [first seen in January](#) of this year. Initially the worm spread as an executable file attached to an e-mail disguised as an electronic greeting card. However, Storm has constantly [changed its tactics](#) and was recently caught fooling victims into clicking on links that lead them to an infected file.

According to antivirus firm Sophos, almost seven percent of all spam last week seemed to be related to Storm worm activity -- much of it greeting card related. The United States Computer Emergency Readiness Team (US-CERT) last week warned Web users about the Storm worm which, it said, is "currently on the rise".

The Storm worm's build-up has concerned managed service security vendor SecureWorks, which recently speculated that the computers under Storm's control could be used to bring down virtually any online property.

The company has reported that in the four months leading to August 2007, Storm worm infections increased from 71,342 to over 20 million.

IBRS security analyst, James Turner said the Storm worm worked by changing its configuration through peer-to-peer networks rather than an IRC channel and that its distributed nature would make the resultant botnet particularly difficult to contain.

- rs
- rs
- ms internet ss
- Hacking e & ies ware &
- s
- operty &

Estonia recovers from massive DDoS attack

Denial-of-service onslaught may have Russian origins

Jeremy Kirk [Today's Top Stories](#) or [Other Security Stories](#)

Comments (1) Recommendations: 35 — [Recommend this article](#)

May 17, 2007 (IDG News Service) -- A spree of denial-of-service attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the [European Union](#).

The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aareleid, chief security officer for Estonia's Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restart service.

"Yes, it's serious problem, but we are up and running," Aareleid said.

Aareleid said analysts have found postings on Web sites indicating Russian hackers may be involved in the attacks. However, analysis of the malicious traffic shows that computers from the

TAKE BACK CONTROL WITH

Amenazas en Internet

- El tipo de amenazas que encontramos en Internet está cambiando de foco
- Antes...
 - Prevalencia de virus y gusanos
 - *Slammer, CodeRed*
- Ahora...
 - Virus, gusanos, troyanos y otros “personajes” pero operando como herramientas para obtener ganancias

La “Inseguridad” del Software

- ¿Qué factores hacen posible todo esto?
 - La propia naturaleza humana en primer lugar
 - Los usuarios de Internet en general no le dan un lugar prioritario a la seguridad de sus PCs
 - Siempre hay “elementos” buscando obtener ganancias fáciles a costa de otros
 - La propia naturaleza del software
 - Hacer software no es fácil, se parece mucho más a un arte que a una ciencia
 - La seguridad en un proyecto es algo que en general se considera sólo al final del mismo, o veces luego!, en general motivado por un incidente de seguridad

¿Para Qué Tomarse Este Trabajo?

- Primera etapa
 - Demostrar conocimiento, obtener prestigio personal en ciertos ámbitos
- Segunda etapa
 - Diseminación de información
 - “a ciegas”, en general enviando trozos de documentos a direcciones de correo electrónico
- Tercera etapa
 - Obtención de ganancias económicas
 - *Phishing*, DDoS

Botnets

- Una "*botnet*" está formada por un conjunto de sistemas comprometidos (*zombies* o *herd*) y bajo el control de un operador central (*bot herder* o *bot master*)

"*robot*" + "*network*"

- En cada sistema comprometido hay instalado alguna forma de *malware* que permite al operador controlarlo
- Se compran, se venden, se alquilan "*customizadas*"
 - news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf

Utilización de una Botnet

- Envío de correo electrónico no solicitado (*spam*)
- Ataques de DDoS
- *Phishing*
- Instalación de *adware*
- *Sniffing* de tráfico
- *Keylogging*
 - Guardar las "teclas" pulsadas por el usuario y enviar esa información al "*bot herder*"
- Fraude del clic
 - Generación de clicks fraudulentos a herramientas de promoción en Internet (Google, Yahoo)

DDoS

- DDoS: *Distributed Denial of Service* o “ataques de denegación de servicio distribuidos”
 - Nombre por el cual se conocen a ataques que provienen de una nube “difusa” de direcciones IP con destino a un blanco único
 - Generación de suficiente tráfico como para saturar enlaces WAN y servidores

Estonia recovers from massive DDoS attack

Denial-of-service onslaught may have Russian origins

Jeremy Kirk [Today's Top Stories >](#) or [Other Security Stories >](#)

Comments (1) Recommendations: 35 — [Recommend this article](#)

May 17, 2007 (IDG News Service) -- A spree of denial-of-service attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union.

The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aarelaid, chief security officer for Estonia's Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restore service.

"Yes, it's serious problem, but we are up and running," Aarelaid said.

Regional News: [Boston](#) | [D.C.](#) | [New York](#) | [Silicon Valley](#) | [More Tech News: Newsline](#)

| | | | | | |
|----------|-----------|-----------|-----------------|------------|------------|
| Business | Developer | Ecommerce | Enterprise | Networking | Security |
| Storage | Wireless | xSP | Special Reports | Stats | Commentary |

7 day summary

[Add the power and flexibility of SlickEdit to Eclipse. The SlickEdit Plug-In provides developers with a powerful set of symbol analysis and navigation tools to save time and maximize control over code.](#)

Developer

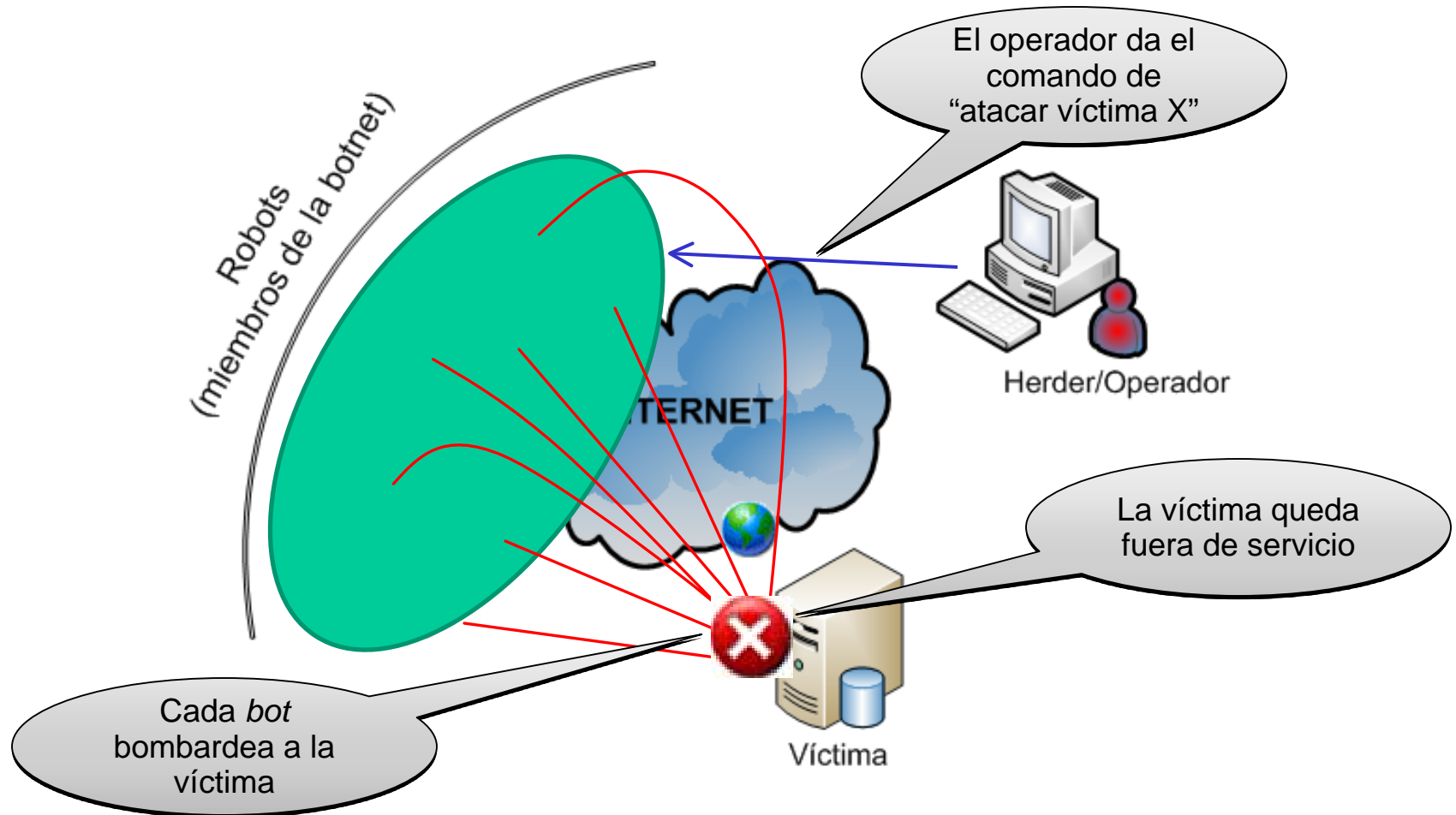
October 23, 2002
Massive DDoS Attack Hit DNS Root Servers
 By [Ryan Naraine](#)

A massive distributed denial-of-service (DDoS) attack ([define](#)) of unknown origin briefly interrupted Web traffic on nine of the 13 DNS "root" servers that control the Internet but experts on Wednesday dismissed the overall threat as "minimal."

- [Apple Laptops](#)
- [MacBook](#)
- [MacBook Pro](#)

Botnets para DDoS

- Lanzamiento de un DDoS utilizando una *botnet*



Honeypots

- En términos muy generales:
 - *Un honeypot es un recurso de red cuyo valor mismo es el de ser atacado o vulnerado. Los beneficios se obtienen mediante mantener un cuidadoso monitorizado del mismo.*
- En resumen
 - Ofrecer un blanco interesante
 - Observarlo
 - Sacar conclusiones

Honeypots

- Taxonomía:
 - Baja interacción
 - Interacción limitada, servicios y topologías emuladas
 - Sencillos de utilizar y mantener. Bajo riesgo.
 - Alta interacción
 - Interacción con sistemas reales (S.O.'s, hardware)
 - Más complejos de mantener. Algún riesgo.

Honeynets

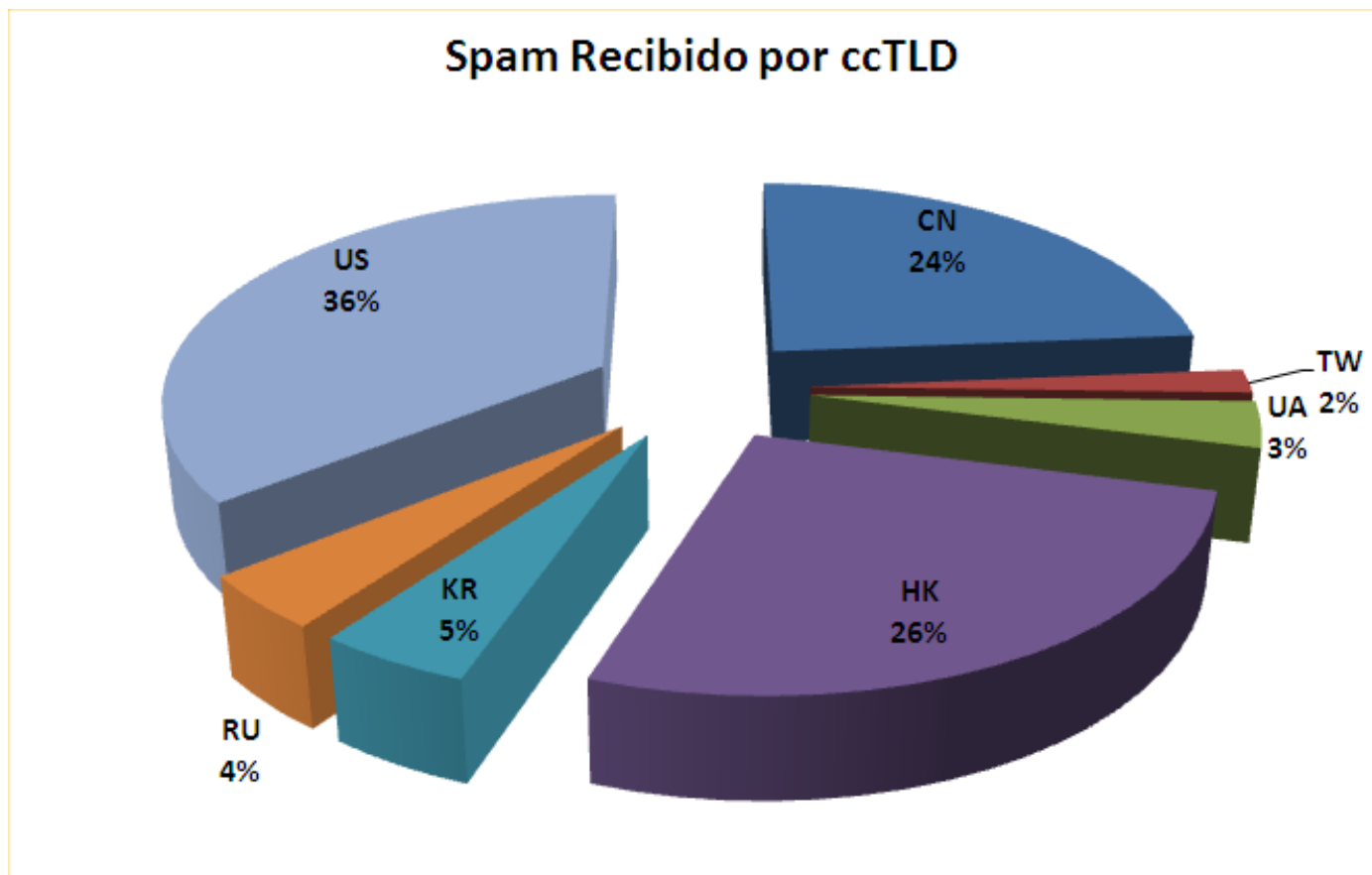
- Un *honeypot* individual tiene visibilidad limitada sobre un rango (usualmente pequeño) de direcciones IP
- Honeynets
 - Instalar *honeypots* de la forma mas distribuida posible
 - Colectar información de los mismos
 - Realizar correlación de eventos y comparar información

Spampots

- Idea similar a la de la honeynet pero aplicada al problema del spam (correo electrónico no solitado)
- Todo el tráfico que pasa por él, es spam

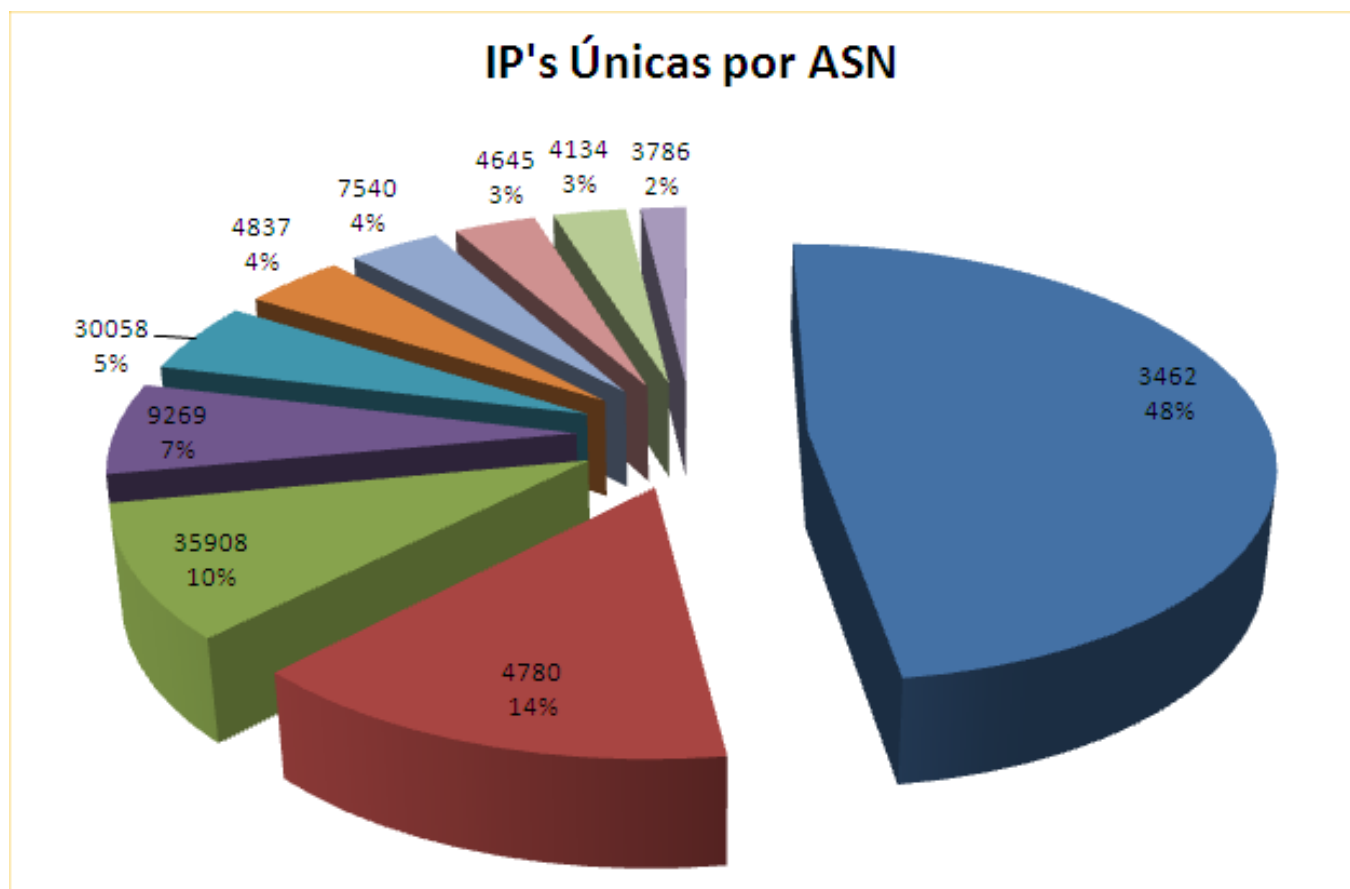
Resultados

- Spampot



Resultados

- Spampot



Proyectos de Colaboración

- Las iniciativas presentadas han surgido en un entorno de inserción internacional
 - Membresía FIRST
 - Colaboración con CERT.br
- A futuro
 - AusCERT
 - Otros



Vinculación institucional del CSIRT

- El nacimiento del CSIRT ANTEL se favoreció por la existencia de un Sistema de Gestión de Seguridad de la Información.
- Marco normativo.
 - Políticas de Seguridad de la Información.
 - Procedimientos de Gestión de Incidentes.
- Medio ambiente favorable.
 - Propensión a la investigación en la organización.
 - Cercanía con el ambiente académico.
 - Avidéz de los involucrados en los temas de seguridad.

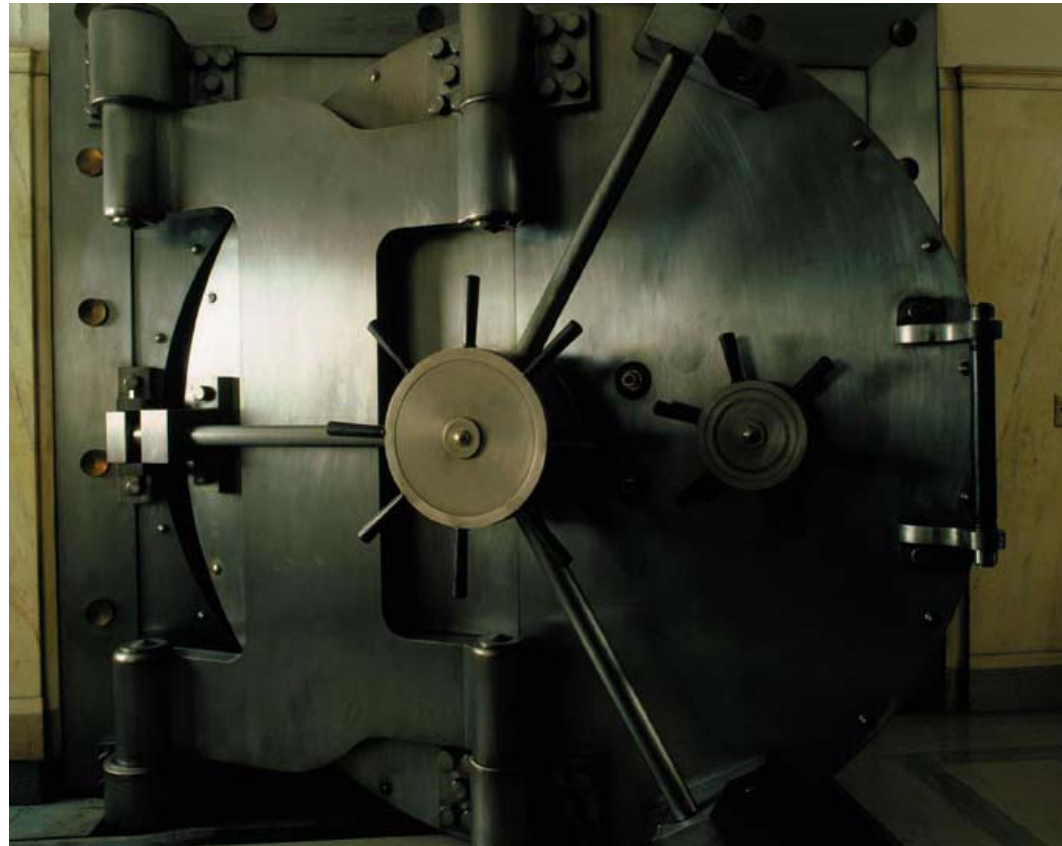
Ejemplos de Incidentes de Seguridad

- Pérdida de integridad de documentos en el Banco Central de Uruguay
- Pérdida de datos de estudiantes en Instituto Universitario en Uruguay
- Extorsión para evitar difusión de bases de datos de tarjetas de crédito internacionales (American Express y otras...)
- Ataques de Denegación de Servicio a ISP
- Basados en Ingeniería social
 - Phishing, a diversas entidades bancarias en y desde Uruguay.
 - SCAM (Nigeria - "Four - One - Nine")

Seguridad de la Información

Definición

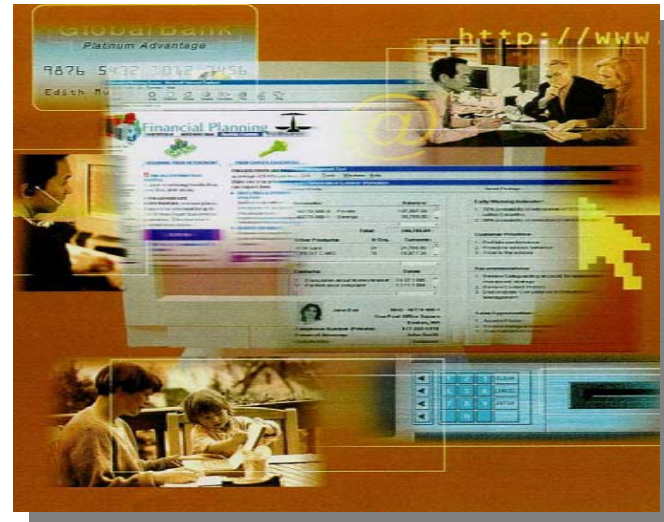
- Integridad
- Confidencialidad
- Disponibilidad



Seguridad de la Información

Medidas de seguridad

- Lógicas *(Seguridad lógica)*
- Físicas *(Seguridad física)*
- Ambiental *(Seguridad ambiental)*



Riesgos e impactos

Amenazas



Inherentes:

- Soporte TI
- RRHH
- Entorno
- Medio ambiente

Riesgos e impactos

Amenazas



Inherentes:

- Soporte TI
- RRHH
- Entorno
- Medio ambiente

Origen de la debilidad



Tecnológico

Recursos Humanos
Prácticas operativas

Ataque / Falla

- Hacking
- IP spoofing
- Virus
- Enmascaramiento
- Spamming
- Caballo de Troya
- Fallas del equipamiento
- Falla de las telecomunicaciones
- Piratería de software

Riesgos e impactos

Amenazas



Inherentes:

- Soporte TI
- RRHH
- Entorno
- Medio ambiente

Origen de la debilidad



Tecnológico

Recursos Humanos

Prácticas operativas

Ataque / Falla

- Falta de capacitación
- Errores
- Fraudes
- Negligencia

Riesgos e impactos

Amenazas



Inherentes:

- Soporte TI
- RRHH
- Entorno
- Medio ambiente

Origen de la debilidad



Tecnológico

Recursos Humanos

Prácticas operativas

Ataque / Falla

- Caballo de Troya
- Ingeniería social
- Ataques contra la privacidad de los datos
- Fraude operativo
- Piratería de software

Capítulos de la Política de Seguridad

1. Política de Seguridad
2. Organización de la Seguridad de la Información
3. Gestión de Activos
4. Seguridad de Recursos Humanos
5. Seguridad Física y del Ambiente
6. Gestión de Comunicaciones y Operaciones
7. Control de Acceso
8. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
9. Gestión de Incidentes de la Seguridad de la Información
10. Gestión de la Continuidad del Negocio
11. Cumplimiento

Contribución al Gobierno Electrónico

- AGESIC
 - Constitución del Comité de Seguridad Informática
 - Constitución e implementación del CERTuy
- Promoción y desarrollo de recursos humanos a nivel nacional
- Prevención y protección de las infraestructuras críticas nacionales
- Inserción y respuesta internacional del Uruguay al combate del *cyber-delito*

¡Muchas gracias por su atención!

Eduardo.Carozo@csirt-antel.com.uy

Leonardo.Vidal@csirt-antel.com.uy

