Tecnológico de Monterrey

Actores, protagonistas y certificaciones

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://cryptomex.org

Tecnológico de Monterrey

Los protagonistas

hackers, crackers y ...

Tecnológico de Monterrey

Los protagonistas

- Los hackers
- Los crackers
- Los phreakers
- Los script kidies

Tecnológico de Monterrey

El Hacker: La Vieja Guardia

- Origen del término a finales de los 60.
- Programador con alto dominio de su profesión, capaz de solucionar problemas a través de hacks (segmentos de código muy ingenioso).
- Verdaderos conocedores de la tecnología de cómputo y telecomunicaciones (85-93).
- La búsqueda del conocimiento siempre fue su fuerza impulsora.

Manifiesto hacker

Este mundo es nuestro ... el mundo de los electrones y los interruptores, la belleza del baudio. Utilizamos un servicio ya existente, sin pagar por eso que podría haber sido más barato si no fuese por esos devoradores de beneficios. Y nos llaman delincuentes. Exploramos... y nos llaman delincuentes. No diferenciamos el color de la piel, ni la nacionalidad, ni la religión... y ustedes nos llaman delincuentes. Construyen bombas atómicas, hacen la guerra, asesinan, estafan al país y nos mienten tratando de hacernos creer que son buenos, y aún nos tratan de delincuentes. Si, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que ustedes, algo que nunca me perdonarán.

The Mentor

Tecnológico de Monterrey

The Mentor

Tecnológico de Monterrey

El cracker

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas computacionales.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado.
- No necesariamente tiene el mismo nivel de conocimientos que el hacker.

Los phreakers

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas telefónicos privados.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado, o se beneficia del mismo.

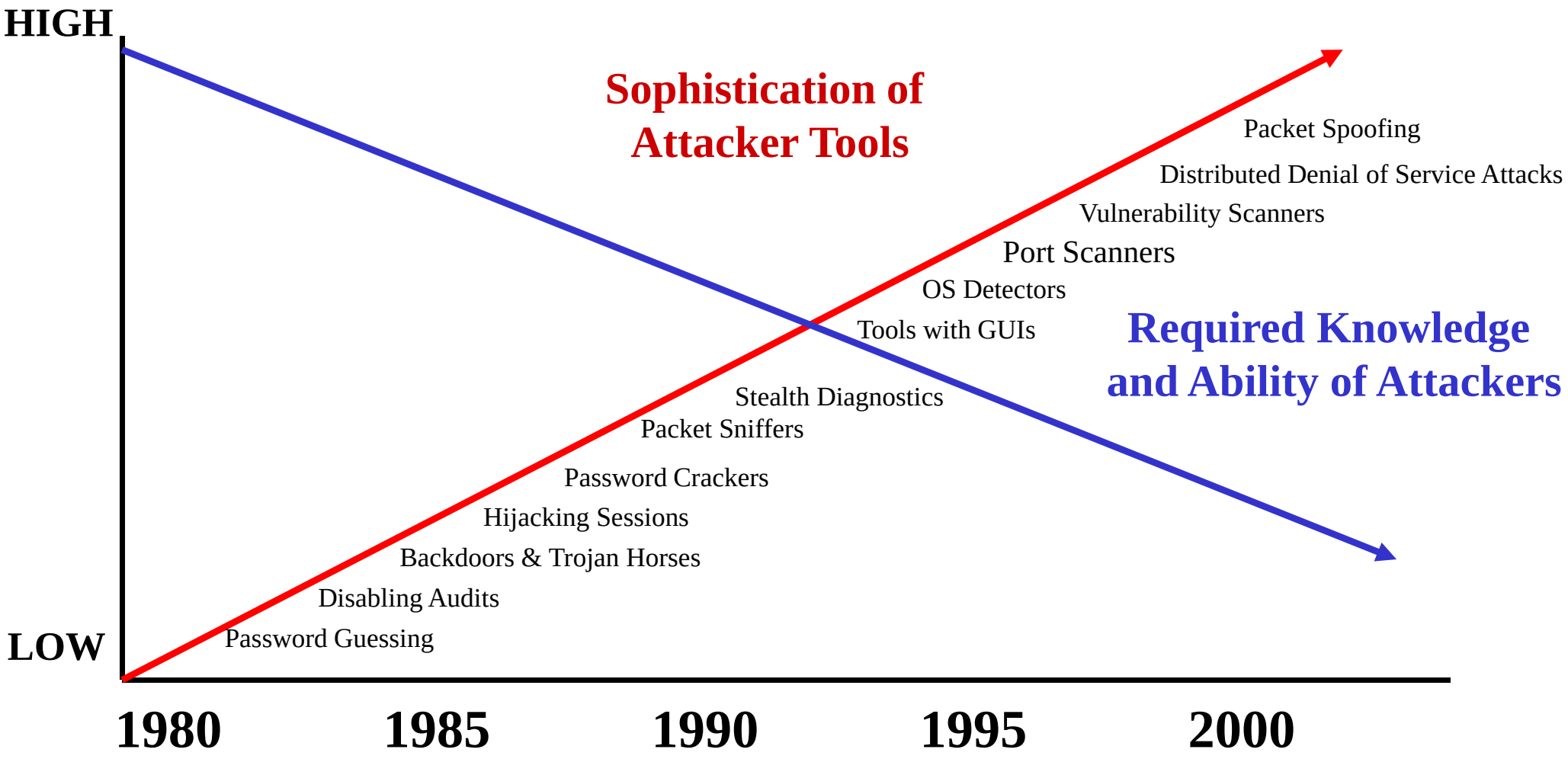
El Hacker: la nueva generación o los ¨Script-kidies¨

- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al *inframundo*.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy ¨cool¨.

Tecnológico de Monterrey

External Threats: Hacker Tool Explosion

Recent Web Search for "Hacker Tools" returned over 2100 hits



I get scanned dozens of times everyday. Less than 20% of those scans are US based

ISS User

Tecnológico de Monterrey

Los Lammers

- Individuo sin muchos conocimientos, aunque un poco más elevados que los mortales, pero claramente inferiores a los de un hacker.
- Se hacen pasar por hackers
- Termino bastante despectivo
- Se les reconoce por su costumbre de presumir en los chats de conocimientos, normalmente técnicas que aunque al conjunto de los usuarios puedan parecer asombrosas, son más viejas que el arca de Noé y su uso no implica conocimientos de alto nivel.

Tecnológico de Monterrey

Algunos intentos de sofisticación

- Escribir con k
  - “kasi” da pena al leerlos
- Escribir minúsculas y mayúsculas
  - EsTo TiPo De TiPoGrAfIa Ya No EsTa De MoDa Y yA nO sE uSa
- Lenguaje “elite”
  - sustituir letras por números
  - 3ST0 S3RI4 UN 3J3MPLO D3 DICH0 L3NGU4J3

Newbies

- Joven usuario que está comenzando y decide aprender siguiendo las reglas sin romper nada.
- No son peligrosos porque prefieren asesorarse y normalmente acaban siendo hackers
- En cierto modo un newbie es un “aprendiz” de un hacker.

Una madrecita Aprendiendo a “Hackear”.

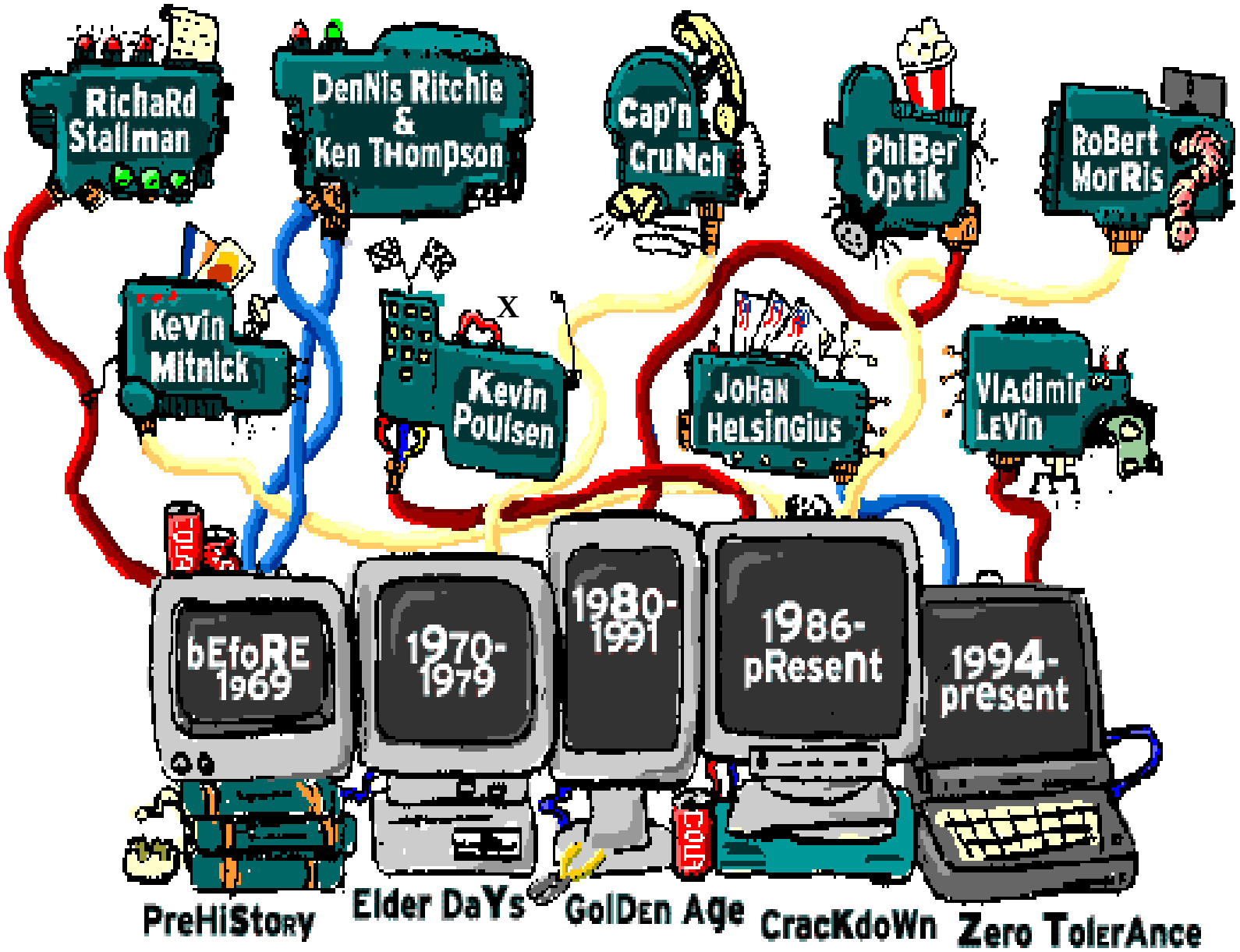
El Hacker: ¿cómo lo ven el resto de los usuarios?

- ¿Qué es eso?
- Eso pasa solo en las películas.
- Así como los de ¨The Net¨
- Yo soy hacker.
- Yo apenas sé como se usa una computadora.
- Bill Gates se va a encargar de ellos.

El hall de la fama de los hackers











www.discovery.com/area/technology/hackers/hackers.html

Tecnológico de Monterrey

¿Qué hicieron?

- Kevin Poulsen
  - En 1990 Poulsen tomo control de todas las líneas telefónicas que llegaban a la estación de radio de Los Angeles KII-FM para ganar un concurso.
- Johan Helsingius
  - Operaba el más famoso remailer anónimo a nivel mundial, llamado penet.fi, hasta que lo cerro en Septiembre de 1996
- Phiber Optik (Mark Abene)
  - Inspiro cientos a adolescentes en el país para “estudiar” los trabajos internos del sistema telefónico nacional de USA.
- Cap Crunch (John Draper)
  - Averiguo la forma de realizar llamadas telefónicas gratis usando un silbato de plástico que encontró en una caja de cereales

El hacker Kevin Mitnick

Tecnológico de Monterrey

Algunos otros

- Steve Wozniak
- Tsutomu Shimomura
- Linus Torvalds

¿Que motiva a un hacker?

- Hacktivists
- State sponsored
- Industrial Espionage

hacked - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites History

Address http://defaced.alldas.de/mirror/2001/10/28/webmaster-novel.com/ Go Links

[DEFACED]

[SECURITY TEST]

SERVER STATUS: VULNERABLE

BUG STATUS: NOT FIXED

SERVER FILEZ: INTACT

INDEX FILE: DEFACED

ADMIN TYPE: STUPID

< h4ck 1s n0t a cr1m3 >

[Steel Edge - Self Destruct - Kurt Vegetable - SuB-Z3r0 - Z3r0 C4LL - NeoByte]

Done Internet

Netscape

File Edit View Go Bookmarks Tools Window Help

http://www.chivas.com.mx/ Search

Mail AIM Home Radio Netscape Search Shop Bookmarks

::: Hacked By GiGoLoKo_ ® :::

gigoloko@alcoholicosanonimos.com

Document: Done (0.501 secs)

Arriba las Chivas!!!

Hacked by JhivD

jhivd@arribalaschivas.com

O único homem que não comete erros é o que nunca faz nada...
Não tenha medo de errar, contanto que não cometa duas vezes o mesmo erro.

A continuidade da vida
no planeta e a
sobrevivencia da
propria humanidade
depedem do
meio ambiente.
A preservação do
meio ambiente tem
que fazer parte do
cotidiano de todas as
pessoas.
Então,
todo dia deve ser
dia do meio ambiente

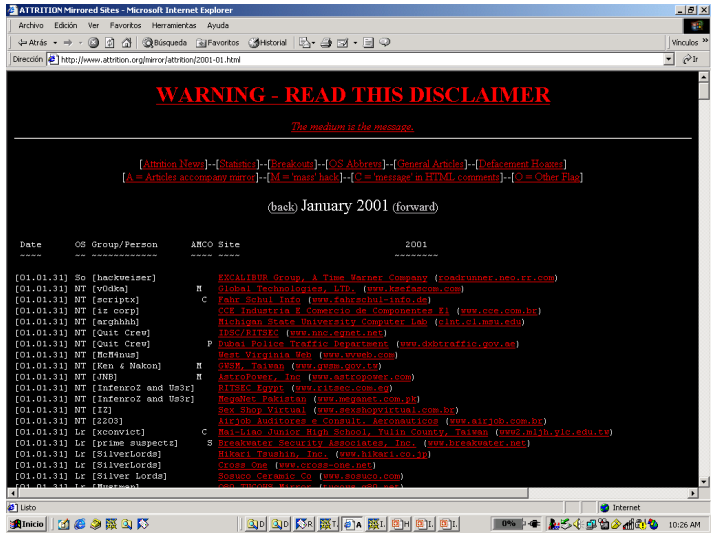
H.i.S
Fazendo sua parte

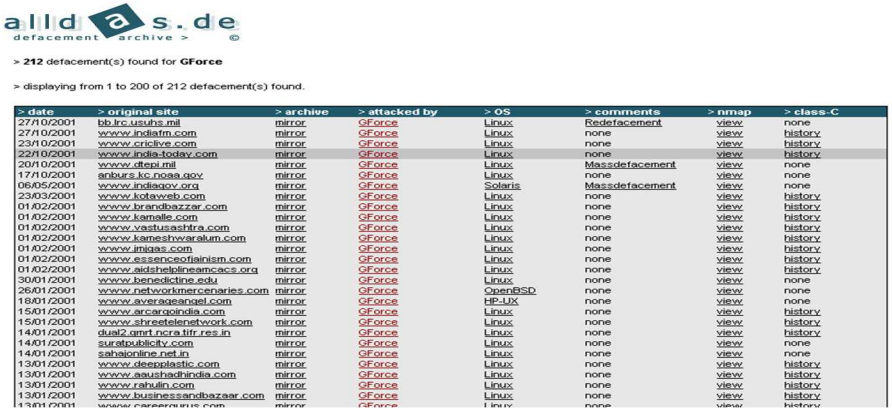
Thank: ModProb3, StaMaster, nandaF., ADMIM cool and GreenPeace
Fuck: American explorers of Brazillian florests

Tecnológico de Monterrey

Defaced pages

- Primero fue attrition
  - http://www.attrition.org
- Después fue alldas
  - http://defaced.alldas.de/
- Ahora es:
  - http://www.zone-h.org/defacements/onhold





> date	> original site	> archive	> attacked by	> OS	> comments	> nmap	> class-C
27/10/2001	bb.lrc.usuhs.mil	mirror	GForce	Linux	Redefacement	view	none
27/10/2001	www.indiafm.com	mirror	GForce	Linux	none	view	history
23/10/2001	www.criclive.com	mirror	GForce	Linux	none	view	history
22/10/2001	www.india-today.com	mirror	GForce	Linux	none	view	history
20/10/2001	www.dtepi.mil	mirror	GForce	Linux	Massdefacement	view	none
17/10/2001	anburs.kc.noaa.gov	mirror	GForce	Linux	none	view	none
06/05/2001	www.indiagov.org	mirror	GForce	Solaris	Massdefacement	view	none
23/03/2001	www.kotaweb.com	mirror	GForce	Linux	none	view	history
01/02/2001	www.brandbazzar.com	mirror	GForce	Linux	none	view	history
01/02/2001	www.kamalle.com	mirror	GForce	Linux	none	view	history
01/02/2001	www.vastusashtra.com	mirror	GForce	Linux	none	view	history
01/02/2001	www.kameshwaralum.com	mirror	GForce	Linux	none	view	history
01/02/2001	www.imigas.com	mirror	GForce	Linux	none	view	history
01/02/2001	www.essenceofiainism.com	mirror	GForce	Linux	none	view	history
01/02/2001	www.aidshelplineamcacs.org	mirror	GForce	Linux	none	view	history
30/01/2001	www.benedictine.edu	mirror	GForce	Linux	none	view	none
26/01/2001	www.networkmercenaries.com	mirror	GForce	OpenBSD	none	view	none
18/01/2001	www.averageangel.com	mirror	GForce	HP-UX	none	view	none
15/01/2001	www.arcargoindia.com	mirror	GForce	Linux	none	view	history
15/01/2001	www.shreetelenetwork.com	mirror	GForce	Linux	none	view	history
14/01/2001	dual2.gmrt.ncra.tifr.res.in	mirror	GForce	Linux	none	view	history
14/01/2001	suratpublicity.com	mirror	GForce	Linux	none	view	none
14/01/2001	sahajonline.net.in	mirror	GForce	Linux	none	view	none
13/01/2001	www.deepplastic.com	mirror	GForce	Linux	none	view	history
13/01/2001	www.aaushadhindia.com	mirror	GForce	Linux	none	view	history
13/01/2001	www.rahulin.com	mirror	GForce	Linux	none	view	history
13/01/2001	www.businessandbazaar.com	mirror	GForce	Linux	none	view	history

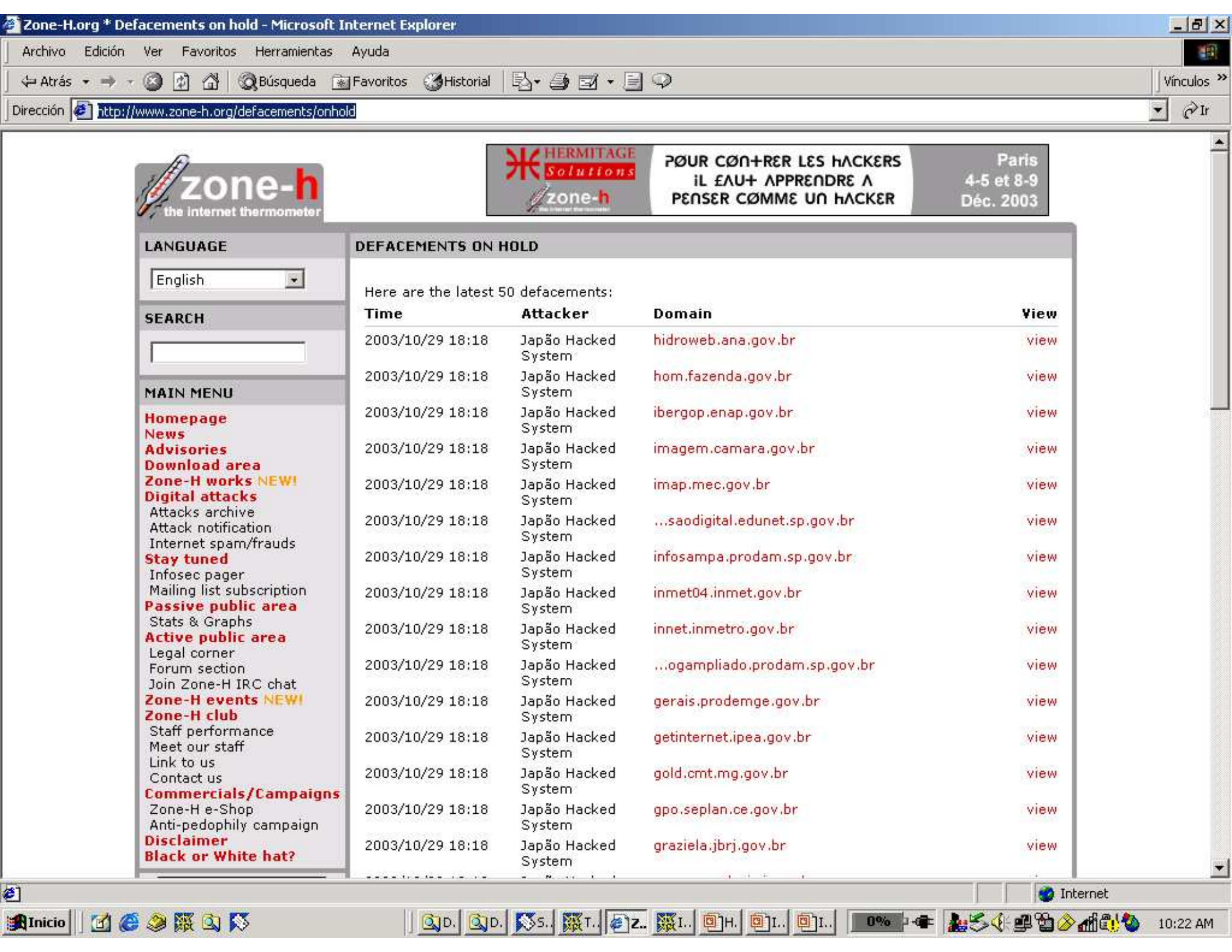
Tecnológico de Monterrey

Attrition Decision

One of the most predominant sections of Attrition has been the defacement mirror. What began as a small collection of web site defacement mirrors soon turned into a near 24/7 chore of keeping it up to date. In the last month, we have experienced single days of mirroring over 100 defaced web sites, over three times the total for 1995 and 1996 combined. With the rapid increase in web defacement activity, there are times when it requires one of us to take mirrors for four or five hours straight to catch up. Add to that the scripts and utilities needed to keep the mirror updated, statistics generated, mail lists maintained, and the time required for basic functionality is immense. A "hobby" is supposed to be enjoyable. Maintaining the mirror is becoming a thankless chore.

During this time, we have struggled to keep up various other sections of Attrition that have been a core part of the site. As the mirror grew and began to consume more resources, the other sections have found themselves on the backburner and rarely updated. In essence, what was once a hobby site run in spare time for fun has turned into a beleaguring second job. A job that comes with more headache, complaints, criticisms, slander and attacks than productive output or reward. In two years we have turned away countless computer security work that could have been fulfilled by a number of us. The abuse and ignorance we deal with from defacers and defacement victims is staggering, and some of that abuse spills over into actual attacks. Attrition has been taken down more than once by massive denial of service attacks which have inconvenienced our generous upstream provider, hundreds of other colo customers, and thousands of dialup customers, making our job even more difficult.

With that, the mirror will no longer be maintained. We've served our time.


Zone-H.org * Defacements on hold - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Historial
Vínculos
Dirección http://www.zone-h.org/defacements/onhold
Ir
zone-h
the internet thermometer
HERMITAGE Solutions
zone-h
PØUR CØN+RER LES hACKERS
iL £AU+ APPRENDRE A
PENSER CØMME UN hACKER
Paris
4-5 et 8-9
Déc. 2003
LANGUAGE
English
SEARCH
MAIN MENU
Homepage
News
Advisories
Download area
Zone-H works NEW!
Digital attacks
Attacks archive
Attack notification
Internet spam/frauds
Stay tuned
Infosec pager
Mailing list subscription
Passive public area
Stats & Graphs
Active public area
Legal corner
Forum section
Join Zone-H IRC chat
Zone-H events NEW!
Zone-H club
Staff performance
Meet our staff
Link to us
Contact us
Commercials/Campaigns
Zone-H e-Shop
Anti-pedophily campaign
Disclaimer
Black or White hat?
DEFACEMENTS ON HOLD
Here are the latest 50 defacements:
Time Attacker Domain View
2003/10/29 18:18 Japão Hacked System hidroweb.ana.gov.br view
2003/10/29 18:18 Japão Hacked System hom.fazenda.gov.br view
2003/10/29 18:18 Japão Hacked System ibergop.enap.gov.br view
2003/10/29 18:18 Japão Hacked System imagem.camara.gov.br view
2003/10/29 18:18 Japão Hacked System imap.mec.gov.br view
2003/10/29 18:18 Japão Hacked System ...saodigital.edunet.sp.gov.br view
2003/10/29 18:18 Japão Hacked System infosampa.prodam.sp.gov.br view
2003/10/29 18:18 Japão Hacked System inmet04.inmet.gov.br view
2003/10/29 18:18 Japão Hacked System innet.inmetro.gov.br view
2003/10/29 18:18 Japão Hacked System ...ogampliado.prodam.sp.gov.br view
2003/10/29 18:18 Japão Hacked System gerais.prodemge.gov.br view
2003/10/29 18:18 Japão Hacked System getinternet.ipea.gov.br view
2003/10/29 18:18 Japão Hacked System gold.cmt.mg.gov.br view
2003/10/29 18:18 Japão Hacked System gpo.seplan.ce.gov.br view
2003/10/29 18:18 Japão Hacked System graziela.jbrj.gov.br view
Internet
Inicio
0%
10:22 AM

Un ejemplo de conversación

#25 por ThA_CroW 21/9/2003

kiuvo banda? ya deberian de dejarse de lameradas y ponerse a trabajar ya ke se supone ke pagar tanta lana por este evento ke segun yo pienso ke deberia de ser gratis o ke? no ke muy hackers?

#14 por SoylaIradeDios 18/9/2003

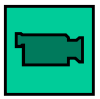
los de hackersoft y hakim.ws si son hackers la mayoria, y organizan sus reuniones sin cobrar para enseñar sus conocimientos en hack por eso preguntaba si iban a dar alguna ponencia como representantes de la escene en mexico, ellos si han hackeado servers importantes

#32 por ArPhAnEt_X 24/9/2003

pus komo ya dijo napa...no kreo ke esto sea kompetencia y al igual ke el yo tambien llevo amigos ke kieren aprender... lo ke dice la ira de dios pues kreo ke no todos en hackersoft sabemos mucho o por lo menos yo... pero lo ke si tenemos en hackersoft, es ganas de avanzar, aprender y kompartir todo esto con mas gente y esto es a lo ke muchos les hace falta y no estankarce kon lo ke ya esta deskubierto, sino deskubrir mas y enseñar a mas dejando el elitismo a un lado.

Tecnológico de Monterrey

Otros términos relacionados

- Wracker
  - programas shareware o freeware
- Carding
  - reventar o emular tarjetas de crédito
  - Copy-hackers o Copy-crakers
  - skimming 
- Wares
  - intercambio programas comerciales pirateados
- Sneaker
  - espía informático por excelencia

Tecnológico de Monterrey

Más términos relacionados

- Snuffer
  - variante sneaker, limitado a averiguar claves de acceso a sistemas y descubre errores y agujeros en programas
- Corsarios
  - ya no se habla, ya no existen en ningún país
  - comprobar efectividad programas de una empresa y sobre todo los de la competencia
- Bucaneros
  - sin tener conocimientos especiales, recogen programas pirateados y los revenden para enriquecerse con ello
- Rider
  - estaba en alguna de las categorías anteriores pero actualmente trabaja en el campo legal

Tecnológico de Monterrey

Algunos grupos

- Chaos Computer Club
  - www.ccc.de
- Cult of the Dead Cow
  - www.cultdeadcow.com
- DC2600.org
  - www.2600.com/
- AntiOffline removing the Dot in Dot.com
  - www.antioffline.com/
- The Ghetto Hackers (rootfu)
  - http://www.ghettohackers.net/
- DARK CLAW
- LoD
- ¿Y en México?
  - Raza Mexicana (www.raza-mexicana.org)
  - Aztlan Klan
  - Cucaracha Hackers Team

Re: Hostsentry configuration

From: drumstik (*root@127.0.0.1*)
Date: 05/30/02

- **Next message:** andrei: ""stealth" and "closed" a shown on grc / port 5001"
- **Previous message:** andrei: "Re: Firestarter Address Translation"
- **In reply to:** Diggy: "Hostsentry configuration"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]

From: drumstik
Date: Thu, 30 May 2002 21:16:17 GMT

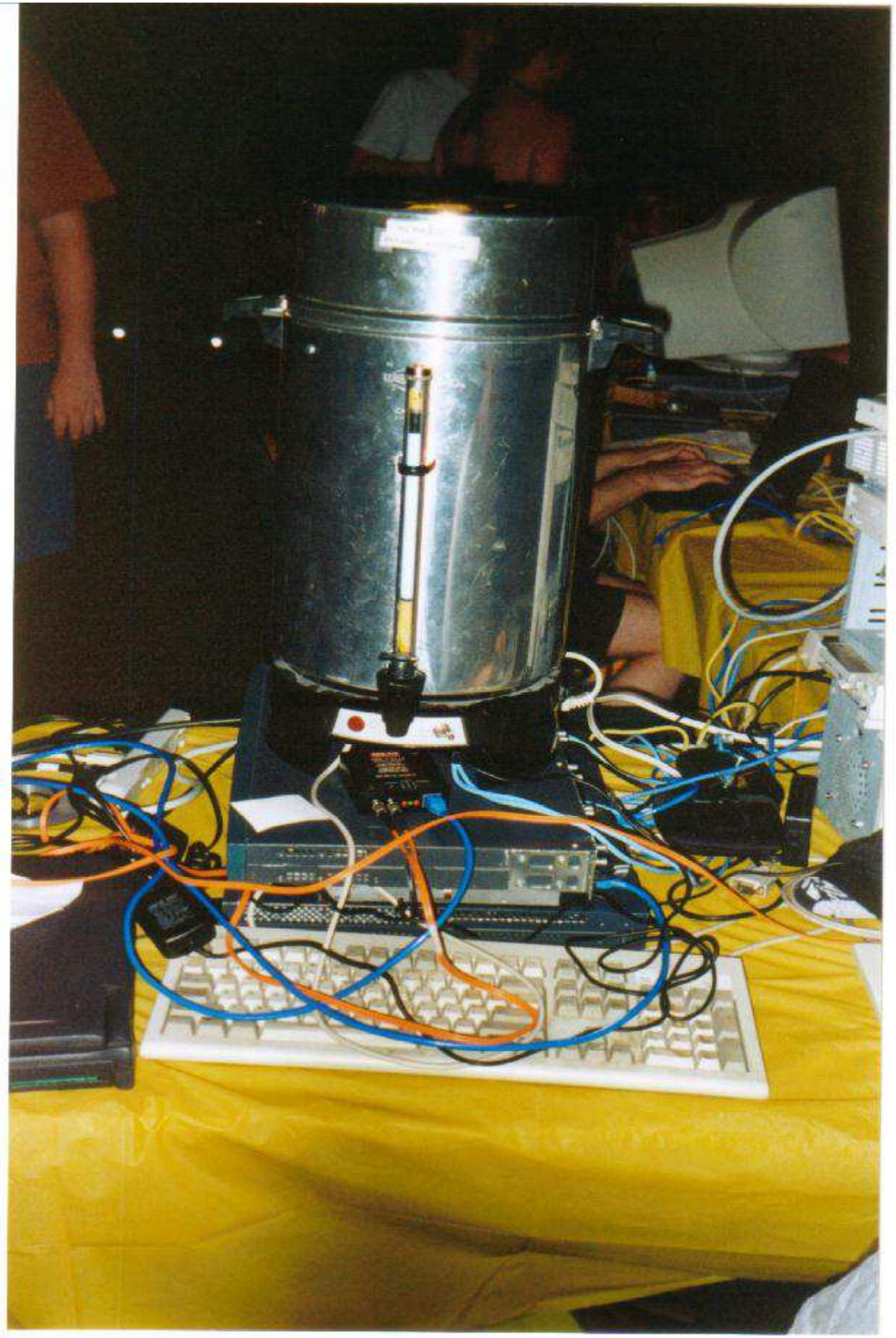
On Thu, 30 May 2002 13:58:18 -0400, Diggy wrote:

> *Does anyone know how to configure Psionic Hostsentry? Does it even need*
> *to be configured? How do you use it to spot anamolies?*

www.google.com
rtfm

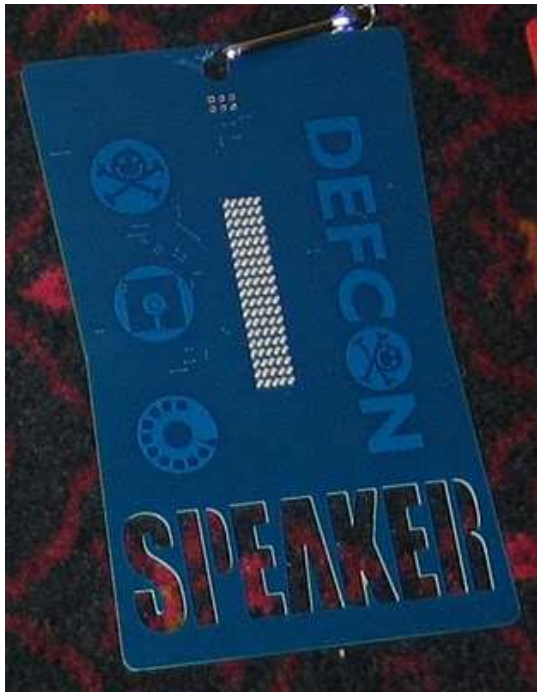
--
drumstik
www.ameriphreak.com
http://phreaks.freeshell.org/files/valuhackAdv.exe
http://valuhack.sourceforge.net


FUCK WORK



Tecnológico de Monterrey

Originalidad



¿Y cómo diferenciar a los buenos de los malos?

- Recomendaciones de terceros
- Prestigio de las compañías
- Certificaciones / títulos academicos

Tecnológico de Monterrey

Títulos y certificaciones

- Títulos académicos
  - Licenciatura
  - Maestría
  - Doctorado
- Certificaciones
  - CISSP
  - SSCP
  - CISA
  - CISM
  - CISMP
  - SCP
  - BS7799-LA

Tecnológico de Monterrey

Las opciones académicas

- Diplomados
  - ITESM-CEM
  - UNAM
  - y otros
- Cursos aislados en programas de maestría y licenciatura
- Licenciatura
  - Tec Milenio: Ingeniero en Seguridad Computacional
  - Universidad de Nuelvo Leon_
- Maestrías en seguridad informatica
  - CESNAV
  - UNITEC
  - ESIME Culhuacán
- Varias universidades americanas y europeas ofrecen maestrías en el área de seguridad informática.

Tecnológico de Monterrey

Universidades relacionadas

- University of Sheffield
  - http://www.shef.ac.uk
- Ecole Ingenieur Télécom Paris - ENST Ecole nationale
  - Mastere Sécurité des systèmes informatiques et des réseaux
  - http://www.enst.fr/3e-cycle-msc-masteres/masteres/ssir.php
- University Purdue
  - Center for Education and Research in Information Assurance and Security, or CERIAS
  - http://www.cerias.purdue.edu/
- The George Washington University
  - Master of Arts in the arts in the field of Criminal Justice Computer Fraud Investigation
  - http://www.gwu.edu

Tecnológico de Monterrey

Otras dos más...

- Carnegie Mellon University.
  - Information Networking Institute (INI)
  - http://www.ini.cmu.edu/
  - Master of Science in Information Networking
  - Master of Science in Information Security Technology and Management
- Capitol College
  - Master of Science in Network Security
  - restricted by the United States Department of Commerce to U.S. citizens and permanent residents
  - http://www.capitol-college.edu/academics/grad/msns.html

Tecnológico de Monterrey

Certificaciones

- Requerimientos legales
  - Sarbanes Oxley (2002)
  - PCI: Mastercard y Visa (2007)
- ¿Qué puedo certificar?
  - Individuos
  - Organizaciones
  - Productos
- ¿Quién puede certificar?
  - (ISC)2
    - International Information Systems Security Certification Consortium
  - ISACA
    - Information Systems and Audit Control Association
  - British Standards Institute: BS
  - International Standards Organization : ISO

Tecnológico de Monterrey

Certificación de individuos

CISSP, SSCP, CISA, CISM, GIAC

Tecnológico de Monterrey

Certificación de individuos

- Las certificaciones en Seguridad tienen un rol cada día más importante en el proceso de selección y reclutamiento de individuos
- Cada certificación cuenta con un CBK
  - Cuerpo común de conocimientos

Tecnológico de Monterrey

Opciones certificación

- Más de 55 certificaciones en seguridad neutrales de productos
- Las mas demandadas
  - CISSP
  - SANS GIAC
  - CPP
- SANS GIAC la pionera en la creación de programas de certificaciones
  - cuenta con una gran variedad y están relacionadas entre sí a manera de carrera.

Hacia una jerarquía

primer nivel básico

CompTIA Security + | **SANS GSEC** | **SSCP de (ISC)2**

credenciales intermedias y de nivel Senior

SANS-GIAC | **CISSP de (ISC)2** | **CISM de ISACA**

restringen su acceso a solo individuos Most-Senior de la comunidad de la seguridad, simplemente porque requieren cinco a nueve años de experiencia profesional en el campo de seguridad.

CPP de ASIS | **PCI de ASIS** | **PSP de ASIS**

Tecnológico de Monterrey

CompTIA

- Asociación mundial de la industria de la computación, tanto en software como en hardware, con mas de 21,000 miembros en mas de 120 países
  - www.comptia.org
- Es la mas grande y única asociación global de este tipo
- Ha desarrollado once destrezas en Certificaciones en Tecnología Informática
  - cubren un amplio rango de disciplinas, ambientes operativos y niveles de destrezas

Certificaciones de la CompTIA

- A+ Entry-Level Computer Service
- CTT+ Certified Trainer
- Network+ Network Support and Administration
- CDIA+ Document Imaging and Management
- Server+ Server Hardware Technology
- i-Net+ Internet and Online Technologies
- Security+ Computer and Information Security
- Linux+ Linux Operating Systems
- HTI+ Home Technology Integration
- Project+ Project Management
- e-Biz+ e-Commerce

Tecnológico de Monterrey

CBK y examen

- CBK

Dominio	% examen
General Security Concepts	30%
Communication Security	20%
Infrastructure Security	20%
Basics of Cryptography	15%
Operational / Organizational Security	15%

- Examen
  - 100 preguntas
  - 90 minutos para responder
  - 764 en escala de 100-900 para pasar

Tecnológico de Monterrey

CISSP

- No es una asociación, es el título que ostenta el profesional certificado
  - Certified Information Systems Security Professional
- Ser CISSP es un privilegio que se debe ganar y mantener
- Otorgado por la $(ISC)^2$
  - International Information Systems Security Certification Consortium
  - Organismo independiente
  - Creado para realizar la certificación de profesionales en seguridad informática

Tecnológico de Monterrey

CBK del CISSP

- Access Control Systems & Methodology
- Telecommunications & Network Security
- Security Management Practices
- Applications & Systems Development Security
- Cryptography
- Security Architecture & Models
- Operations Security
- Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)
- Law, Investigations & Ethics
- Physical Security

Tecnológico de Monterrey

CISSP en México

- ALAPSI
  - Asociación Latinoamerica Profesionales Seguridad Informática
  - http://www.alapsi.org
- Dos/tres exámenes por año
- Cursos preparación examen
- Próximo examen: consultar página
- Número de certificados en México: 250/61,000

Tecnológico de Monterrey

El examen

- Formato
  - examen de opción múltiple
  - 250 preguntas
  - se cuenta hasta 6 horas para resolverrlo
- Aprobar examen con 700 puntos
- Enviar formato de adhesión/certificación (Endorsement Form) avalada por un CISSP o por otro profesional calificado
- Auditoría, si es seleccionado
- Calendarización
  - www.isc2.org

Tecnológico de Monterrey

SSCP

- Especialista Certificado de Seguridad de Sistemas
  - Systems Security Certified Practitioner
- Diseñada para personas que aplican los principios de seguridad de la información, procedimientos, estándares y guías de una organización.
  - proporcionar soporte de la infraestructura de la seguridad
  - security enforcer
  - la persona no solo entiende su posición, sino también tiene un conocimiento de experto de la seguridad informática, como funciona y como es aplicada

Tecnológico de Monterrey

CBK del SSCP

- Access Controls
- Administration
- Audit and Monitoring
- Risk, Response and Recovery
- Cryptography
- Data Communications
- Malicious Code/Malware

Tecnológico de Monterrey

CISA

- Certified Information Systems Auditor
- En un principio dominio exclusivo de auditores de IT
- Administrada por la ISACA (Information Systems Audit and Control Association & Foundation)
  - fundada en 1969
- Certificación CISA tiene desde 1978
- En 2002 se contaba con unos 28,000 personas con dicha certificación.
- Dominios coinciden con CISSP
  - más enfocado a los procedimientos del negocio que a la tecnología
- Varios CISSP optan por ganar su CISA

Tecnológico de Monterrey

Áreas CISA

- Management, planning and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management
- The IS audit process

Tecnológico de Monterrey

CISM

- ISACA acaba de diseñar la certificación CISM
  - Certified Information Security Manager
- Certificación reconoce el conocimiento y experiencia de un administrador de seguridad IT
- Debido a que es nuevo, pasa por un periodo de "apadrinamiento"
  - aquellos que puedan demostrar ocho años de experiencia en el área de seguridad informática puede obtener la certificación sin realizar examen alguno
  - periodo abierto hasta el 31 diciembre 2003
- Después periodo será necesario presentar examen.
- Primer examen será ofrecido en Junio 2004

Tecnológico de Monterrey

CBK del CISM

- Information Security Governance
- Risk Management
- Information Security Programme Management
- Information Security Management
- Response Management

Tecnológico de Monterrey

Global Information Assurance Certifications

- SANS Institute ofrece una serie de certificaciones bajo el programa GIAC
  - Global Information Assurance Certification
- Grupo de certificaciones técnicas y algunas administrativas
- La experiencia no es explicita o necesaria para obtenerla
  - orientado a la práctica de seguridad informática
- http://www.giac.org

Tecnológico de Monterrey

Certificaciones

- No hay un orden en particular
- Se recomienda empezar con los de nivel bajo e ir subiendo
- GIAC Certification
  - cursos 5-6 días
  - periodo de 6 meses para certificarse
  - color amarillo
- GIAC Certificates
  - cursos 1-2 días
  - 10 semanas
  - color verde

	Security Administration	Management	Operations	Legal	Audit
Level 3	GISF				
	SSP-MPA				
Level 4	GSEC	GFSP	GOEC	GBLC	GSAE
	GGSC-0100	GEIT		GCDS	G7799
	GGSC-0200	GHSC		GLFR	
	GGSC-0400	GEWF		GLIT	
		GCYW			
Level 5	GCFW	GCSC			GSNA
	GCIA	GSLC			
	GCIH				
	GCWN				
	GCUX				
	GCFA				
	GHTQ				
	GAWN				
	GWAS				
	GIPS				
Level 6	GNET				
	GREM				
	GSIP				

Las certificaciones

Security Administration

- Security Essentials Certification
- Certified Incident Handler
- Certified Intrusion Analyst
- Penetration Tester
- Certified Firewall Analyst
- Web Application Penetration Tester
- Certified Windows Security Administrator
- Assessing and Auditing Wireless Network
- Certified UNIX Security Administrator
- Information Security Fundamentals
- Certified Enterprise Defender
- Exploit Researcher and Advanced Penetration Tester

Forensics

- Certified Forensic Analyst
- Reverse Engineering Malware
- Certified Forensic Examiner

Management

- Security Leadership
- Information Security Professional
- Certified ISO-27000 Specialist
- Certified Project Manager

Software Security

- Secure Software Programmer-Java
- Certified Web Application Defender
- Secure Software Programmer-.NET

Audit

- Systems and Network Auditor

Legal

- Legal Issues in Information Technology and Security

Tecnológico de Monterrey

Otras certificaciones

- EC-Council
  - Grupo de certificaciones técnicas
- Offensive Security
  - http://www.offensive-security.com/
- Certificaciones de Productos
  - Symantec
  - Computer Associates
  - Checkpoint
  - McAfee
  - Juniper
  - Websense

Tecnológico de Monterrey

Certificaciones de organizaciones

ISO 17799 / BS 7799 / UNE 71502

Tecnológico de Monterrey

Certificación organizaciones

- Pregunta
  - ¿Si igual voy a hacer algo, porque no lo hago teniendo en cuenta las Normas, Metodologías y Legislaciones Internacionales aplicables?

Norma ISO 17799 / BS 7799 / UNE 71502

- Un conjunto de *controles* basados en las *mejores prácticas* en seguridad de la información
  - SGSI: Sistema de Gestión de la Seguridad de la Información
- Proceso metodológico basado en modelo PDCA
  - Plan, Do, Check, Act
- Estándar internacional que cubre todos los aspectos de la seguridad informática:
  - Equipos
  - Políticas de gestión
  - Recursos humanos
  - Aspectos jurídicos

Sistema de gestión de la seguridad de la información (SGSI).

- Se implanta mediante un proceso ordenado que consiste en establecer los mecanismos necesarios de seguridad de manera documentada y conocida por todos los miembros de la empresa.
- Implantación de un SGSI no garantiza la protección en su totalidad .
- ISO en su portal 27000
  - *Garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías*

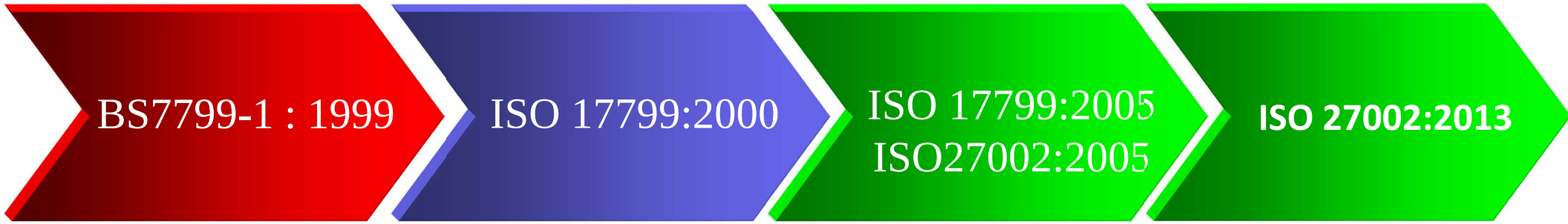
Tecnológico de Monterrey

BSI: British Standard Institute

Fecha	Alcance
1901	Nacimiento de la British Standard Institute (BSI)
1910	Creación del primer estándar
1926	Inicio del proceso de certificación de productos
1946	Creación de la ISO (Internacional Standard Organization) por parte del miembro de la BSI
1979	Primer estándar para los sistemas de gerencia (BS 5750)
1992	Elaboración del estándar sobre el medio ambiente
1999	Elaboración del estándar sobre seguridad de la información (BS 7799)

Tecnológico de Monterrey

Transición

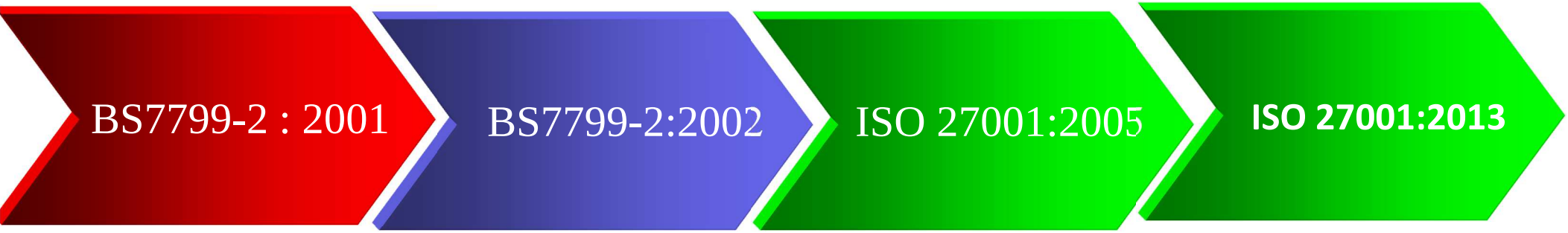


10 dominios
36 controles objetivo
127 controles específicos

10 dominios
36 controles objetivo
127 controles específicos

11 dominios
39 controles objetivo
133 controles específicos

14 dominios
35 controles objetivo
114 controles específicos



10 dominios
36 controles objetivo
127 controles específicos

10 dominios
36 controles objetivo
127 controles específicos

11 dominios
39 controles objetivo
133 controles específicos

14 dominios
35 controles objetivo
114 controles específicos

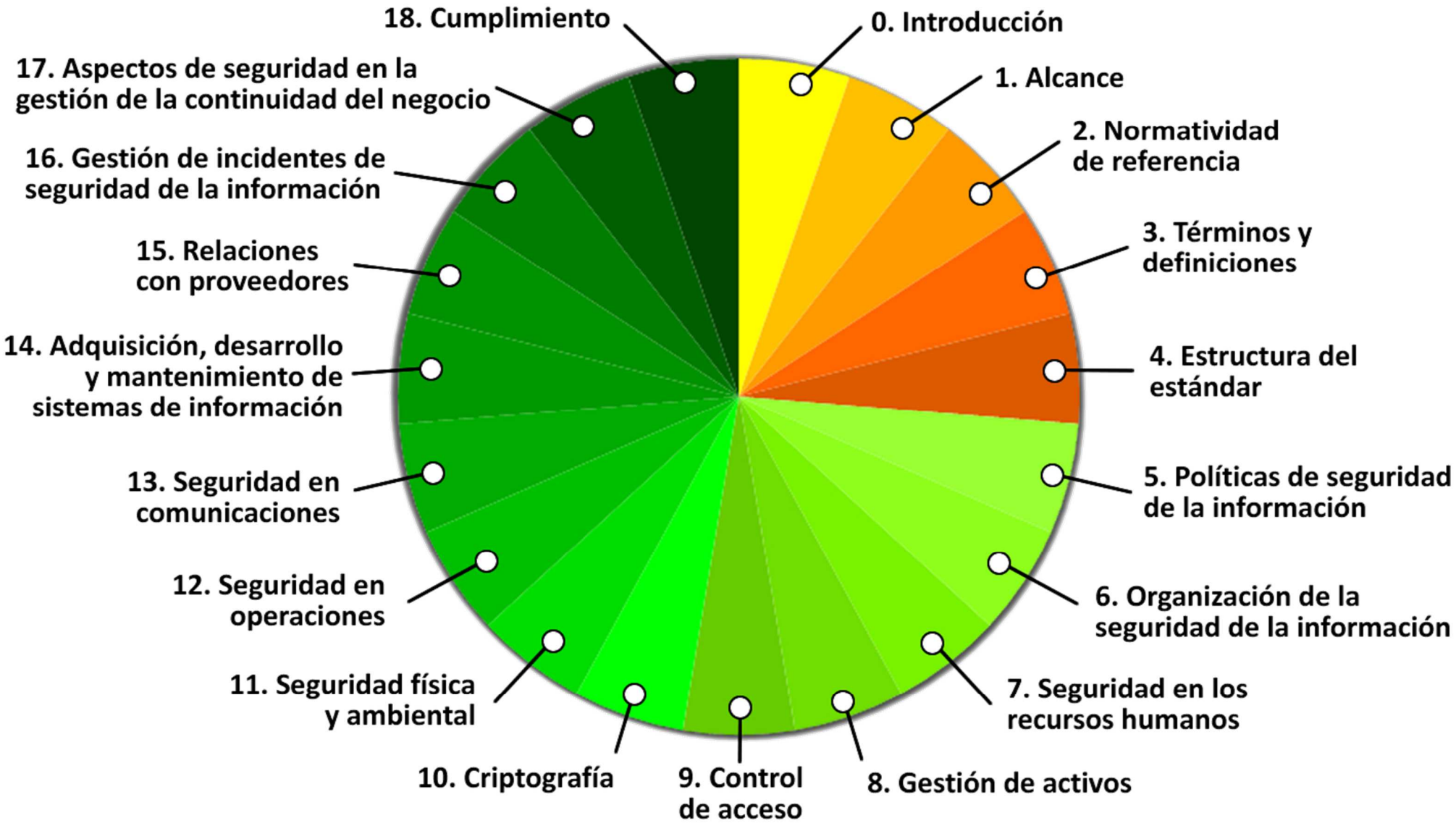
Tecnológico de Monterrey

Controles de la norma

ISO/IEC 27001:2013 especifica 114 controles agrupados en 14 grupos

A5	Information security policies
A6	How information security is organised
A7	Human resources security - controls that are applied before, during, or after employment.
A8	Asset management
A9	Access controls and managing user access
A10	Cryptographic technology
A11	Physical security of the organisation's sites and equipment
A12	Operational security
A13	Secure communications and data transfer
A14	Secure acquisition, development, and support of information systems
A15	Security for suppliers and third parties
A16	Incident management
A17	Business continuity/disaster recovery (to the extent that it affects information security)
A18	Compliance - with internal requirements, such as policies, and with external requirements, such as laws.

Estructura: 14 dominios, 35 objetivos de control y 114 controles



Tecnológico de Monterrey

Ejemplo controles

A.9 Access control

			BS ISO/IEC 17799:2000 numbering
A.9.1 ***Business requirement for access control*** *Control objective:* To control access to information.			**9.1**
Controls			
A.9.1.1	*Access control policy*	Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.	**9.1.1**
A.9.2 ***User access management*** *Control objective:* To ensure that access rights to information systems are appropriately authorized, allocated and maintained.			**9.2**
Controls			
A.9.2.1	*User registration*	There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.	**9.2.1**
A.9.2.2	*Privilege management*	The allocation and use of privileges shall be restricted and controlled.	**9.2.2**
A.9.2.3	*User password management*	The allocation of passwords shall be controlled through a formal management process.	**9.2.3**
A.9.2.4	*Review of user access rights*	Management shall conduct a formal process at regular intervals to review users' access rights.	**9.2.4**

Los estándares de la series ISO IEC 27000

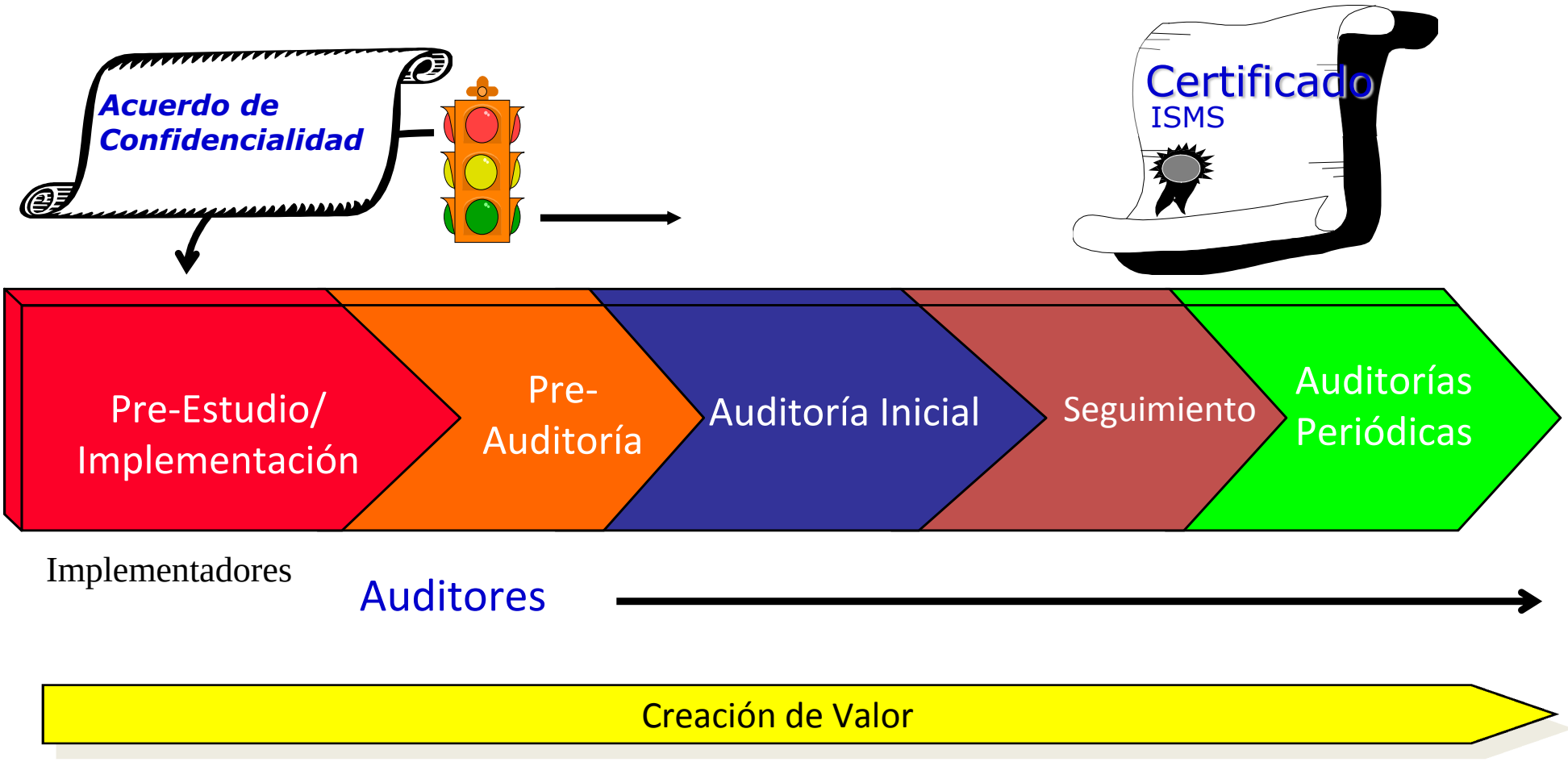
ISO/IEC	Descripción
27000	Vocabulario y definiciones
27001	Especificación de la estructura metodológica (basada en el BS7799-2:2002):2013
27002	Código de prácticas (basada en ISO17799:2005):2007
27003	Guía de implementación
27004	Métricas y medidas
27005	La Administración del Riesgo:2008-2011 (basado en BS 7799-3)
27006	Requerimientos para organismos de acreditación de Sistemas de Gestión de Seguridad de la Información: 2007

Tecnológico de Monterrey

A considerar

- Los certificados tienen una validez de 3 años.
- Se requieren auditorías de evaluación, que van desde los periódica de 6 hasta los 12 meses después de efectuada la primera auditoría.
- A partir publicación del estándar ISO 27001, BS7799 queda anulado.
- Solo se certificó en BS7799 hasta el 15 de Abril del 2006, a partir de esa fecha todas la auditorías se efectúan en base al ISO 27001.
- Las empresas certificadas tendrán un periodo de tiempo para la transición de la ISO27001:2005 a la 2013 de 2 años.
- Las empresas que están en vías de certificarse con la ISO27001:2005 lo podrán hacer pero tendrán que migrar a la ISO27001:2013 en el tiempo establecido.

El camino de la certificación



Integración con otras normas

BS 15000 is ISO 9001:2000 for IT and can be an extension of ISO 9001 scope

Tecnológico de Monterrey

La certificación de productos

TCSEC, ITSEC, CTCPEC, CC

Tecnológico de Monterrey

TCSEC certification

- Trusted Computer Systems Evaluation Criteria
- Pagina (Rainbow Series Library)
  - http://www.radium.ncsc.mil/tpep/library/rainbow/
- Documento publicado por el Departamento de Defensa de los Estados Unidos en 1983 (DOD 5200.28-STD) conocido también como el “Orange Book.”
  - actualizado en 1985

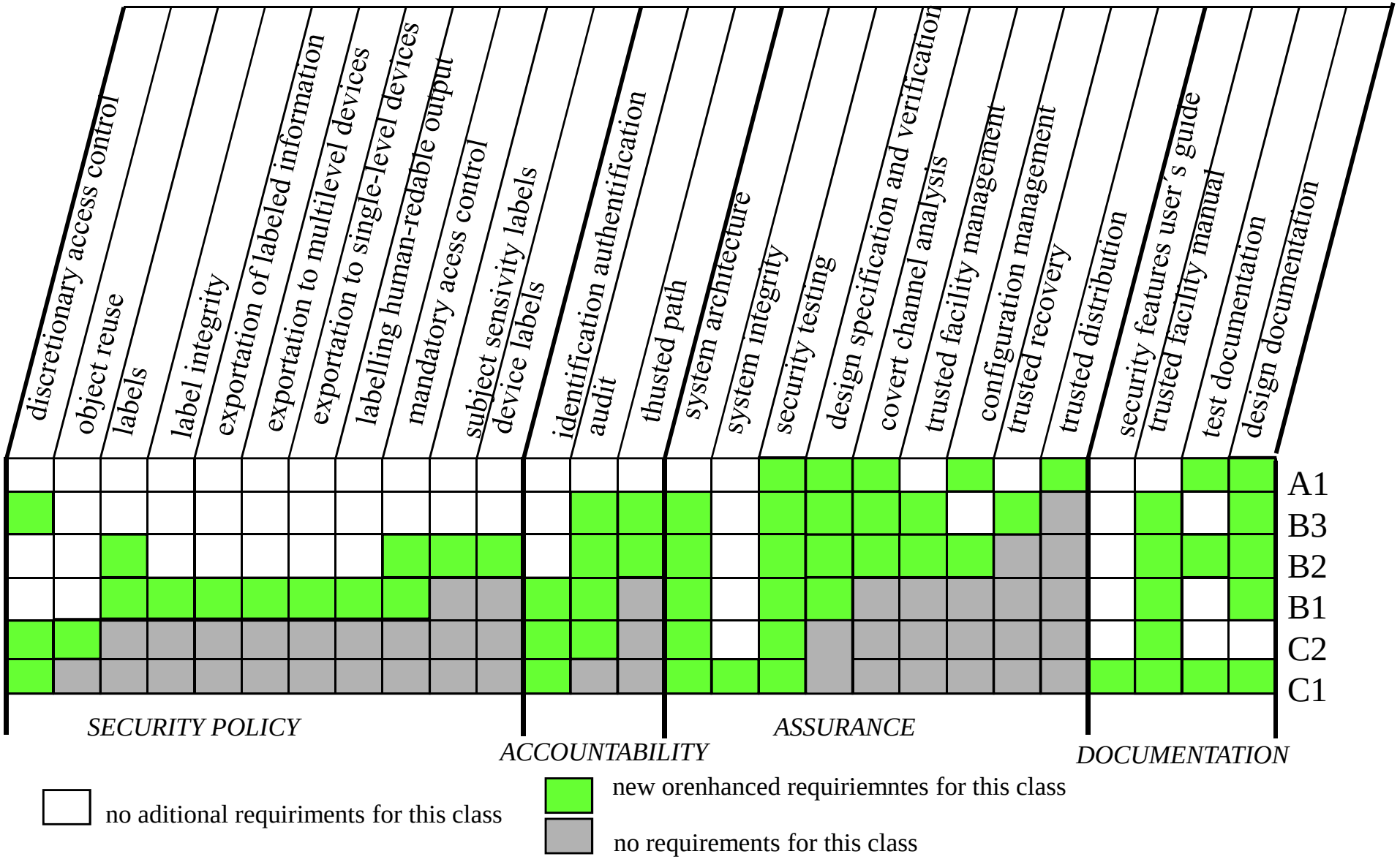
Tecnológico de Monterrey

Objetivos TCSEC

- Proporcionar una guía a los fabricantes de productos comerciales en relación a las características de seguridad que deben cumplir sus productos.
- Dotar al DoD de los Estados Unidos con una métrica para evaluar el grado de confiabilidad de los sistemas orientados a manejar información clasificada.
- Proporcionar una base a los usuarios finales para establecer requerimientos de seguridad en sus adquisiciones de productos.

Tecnológico de Monterrey

Criterios y niveles



Tecnológico de Monterrey

Los niveles

Nivel	Descripción	Comentarios
D	sistema no seguro	
C1	protección discrecional	DAC identificación + autenticación
C2	acceso controlado	auditoria de sistemas
B1	seguridad etiquetada	etiqueta + nivel seguridad jerárquico + categorías
B2	protección estructurada	etiqueta cada objeto de nivel superior por ser padre de un inferior
B3	dominios seguridad	monitor referencia que permite o niega peticiones acceso
A	protección verficada	uso métodos formales para asegurar todos los procesos

Tecnológico de Monterrey

Ejemplo SOs evaluados por la NSA bajo TCSEC (1996)

OS	Level	Cert. date	Notes
Trusted XENIX 3.0	B2	8.4.92	Unix OS. Trusted Information Systems.
Trusted XENIX 4.0	B2	17.9.93	Unix OS. Trusted Information Systems.
Harris CX/SX 6.2.1	B1	18.9.95	Unix OS. Networking is evaluated.
HP-UX BLS, 9.09+	B1	13.4.95	Unix OS. Standard HP-UX software can run on this system.
Trusted IRIX/B V4.0.5EPL	B1	6.2.95	Unix OS.
NT 3.5 Service Pk.3	C2	31.7.95	Proprietary OS. Microsoft. Networking and the Win16 subsystem are not evaluated.
Trusted Solaris V1.1	B1	7.10.94	CMW. Sun.
OpenVMS VAX V6.1	C2	14.7.95	Proprietary OS. DEC.
Digital Unix (OSF)	C2 ?		Unconfirmed.
Ultrix MLS+	B1	21.4.93	Proprietary OS. DEC.
AS/400 with OS/400 V2, R3, M0	C2	5.10.95	Proprietary OS. IBM.
NetWare 4 Server Component and Network System	C2	under eval.	Networking is being evaluated. Novell.
OS 1100/2200 Release SB4R7	B1	20.4..94	Proprietary OS. Unisys.
CA-ACF2 R6.1 with MVS/ESA	C2	14.7.95	Proprietary OS. Computer Associates & IBM.
CA-ACF2 R6.1 with CA MAC and MVS/ESA	B1	14.7.95	Proprietary OS. Computer Associates & IBM.

Algunos libros de la serie arcoiris

- Orange Book
  - DoD Trusted Computer System Evaluation Criteria
- Green Book
  - DoD Password Management Guideline,
- Light Yellow Book
  - Computer Security Requirements
- Yellow Book
  - Guidance for Applying the DoD TCSEC in Specific Environments,
- Light Yellow Book
  - Guidance for Applying the DoD TCSEC in Specific Environments
- Bright Blue Book
  - Trusted Product Evaluation - A Guide for Vendors
- Red Book
  - Trusted Network Interpretation

Tecnológico de Monterrey

Estandares creados a partir del TSSEC

- ITSEC
  - Information Technology Security Evaluation Criteria
  - http://www.cordis.lu/infosec/src/crit.htm
  - la versión europea
- CTCPEC
  - Canadian Trusted Computer Product Evaluation Criteria
  - ftp://ftp.cse.dnd.ca/pub/criteria/CTCPEC.ascii
  - la versión canadiense

Tecnológico de Monterrey

Common Criteria

- Estándar internacional ISO 15408
- Trabajo de varios países (14)
- Inspirado del TCSEC, ITSEC, CTCPEC
- Flexible
  - No cuenta con perfiles predeterminados.
  - Permite la adición de nuevos criterios.
- Parte de las necesidades de cada usuario/fabricante
  - No de las necesidades del DoD.
  - Cada nueva evaluación implica la creación de un modelo o marco de referencia (Security Target o ST).

Tecnológico de Monterrey

Objetivos CC

- Permitir a los usuarios el especificar sus requerimientos de seguridad,
- Permitir a los desarrolladores especificar los atributos de sus productos
- Permitir que los evaluadores determinen si los productos cumple con lo que estipulan.

Tecnológico de Monterrey

Tipos documentos CC

- El CC define un conjunto de requerimientos de seguridad
  - Dividido en requerimientos funcionales y de seguridad
- Dos tipos de documentos
  - Protection Profiles (PPs): documento creado por un usuario o comunidad de usuarios que identifica requerimientos de seguridad por parte del usuario
  - Security Targets (STs): documento creado por un desarrollador de sistema, que identifica las capacidades de un producto en partícular
    - Un ST puede indicar la implementación de cero o mas PPs

Tecnológico de Monterrey

Los niveles del CC (EAL)

- Usuario puede contar con una evaluación independiente que compruebe que el producto cumple con lo estipulado en el ST
  - Evaluación conocida como TOE - Target of Evaluation
- EAL: Evaluation Assurance Level
  - Numeradas del 1 al 7
  - EALs superiores requieren de un mayor esfuerzo de evaluación
  - los EAL de mayor valor garantizan más “seguridad”, pero su evaluación requiere de mayor tiempo y cuesta más dinero
  - EAL valor grande no significa “mejor seguridad”, solo estipula que seguridad proclamada fue extensamente validada

Tecnológico de Monterrey

Niveles Aseguramiento CC

Common Criteria	Descripción	Referencia TCSEC
EAL1	Probado funcionalmante	--
EAL2	Estructuralmente probado	C1
EAL3	Metodológicamente probado	C2
EAL4 (W2K, Solaris, HP-UX, AIX)	Metodológicamente diseñado, probado, y revisado	B1
EAL5	Semiformalmente diseñado y probado	B2
EAL6	Semiformalmente verificado (diseño) y probado	B3
EAL7	Formalmente verificado (diseño) y probado	A1

Tecnológico de Monterrey

Ejemplo productos clasificados

Producto	Nivel	Fecha
3Com© Embedded Firewall V1.5.1	EAL2	June 2003
IBM WebSphere Application Server V5.0.2.8	EAL2+	2 December 2004
Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886	EAL4+	October 2002
Borderware, V6.1.1 Firewall Serve	EAL4+	January 2000
Check Point VPN-1/FireWall-1© NG	EAL4	June 2002
Oracle8i Release 8.1.7.0.0	EAL4	EAL4
Red Hat Enterprise Linux 3	EAL2	February 2004
Symantec Manhunt Version 2.11	EAL3	December 2003

http://www.commoncriteriaportal.org/public/consumer/index.php?menu=4

Tecnológico de Monterrey

Actores, protagonistas y certificaciones

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://cryptomex.org