Sesión 133

Un modelo efectivo para la administración de incidentes de Seguridad de Información

Ricardo Morales González

17 de Octubre 2005

AT&T

- Alestra está en sociedad con AT&T en México a través del grupo ALFA, es uno de los líderes en México en servicios de larga distancia y de Banda Ancha.
- Se cuenta con una red de más de 5,700 KM de fibra óptica para proveer una gama de servicios IP y de voz así como acceso transparente a la red de AT&T "Intelligent Network".
- Algunos de los servicios más importantes que ofrece Alestra a millones de usuarios son: Digital Private Lines, Frame Relay, Internet Access, Email service, IP-VPNs, Domestic and international long distance, Calling Card Services , 800 Services , VoIP, Managed Services, Transparent LAN, LAN Access , Content Distribution , Wireless services, Hosting, etc.
- Alestra está organizada en tres unidades de negocio, Empresarial, Residencial e Internacional.
- Alestra cuenta con un área especializada en Seguridad de Información dado que la preservación de la misma en sus clientes es una de sus más altas prioridades.
- Los controles de Seguridad de Información se implementan en los servicios que vende a millares de usuarios.

Objetivos

1- Entender cuáles son las principales amenazas que ocasionan incidentes en materia de Seguridad de Información así como sus impactos en las organizaciones.

2- Conocer un modelo de administración de incidentes basado en estándares como COBIT, ITIL, BS7799, mejores prácticas, etc.

3- Mencionar cuáles son las bases para la formación de un equipo de respuesta a incidentes efectivo.

4- Explicar el proceso de comunicación de incidentes de Seguridad así como su normatividad necesaria

5- Explicar el proceso de atención de incidentes de Seguridad así como su normatividad necesaria

Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

1- Introducción

Los Ataques, sean criminales o no son imprevistos, son eventos que toman a la gente por sorpresa, son anomalías en el aspecto social, estos afectan las vidas de las víctimas."

Bruce Schneier,
Libro Secrets & Lies

1- Introducción

"If you know the enemy and know yourself,
you need not fear the result of a hundred battles.

If you know yourself but not the enemy,
for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself,
you will succumb in every battle."

Sun Tzu, "The Art of War"

1- Introducción

Definición:

Un Incidente de Seguridad de Información es un acontecimiento adverso que materializa una amenaza cuando una vulnerabilidad se explota, afectando uno o más activos de información el cual es reflejado en cualquiera de las características siguientes de la Información:

Confidencialidad, Integridad o Disponibilidad

1- Introducción

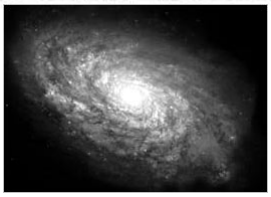
El 1 de Mayo de 2004, el gusano Sasser en una semana infectó a 18 millones de computadoras en el mundo, trajo a miles de negocios de rodillas y costó un estimado de 3,500 millones de Dólares.

Las empresas han invertido horas interminables y millones de dólares bajando nuevos parches, instalando software de Antivirus y Antispamm, etc.

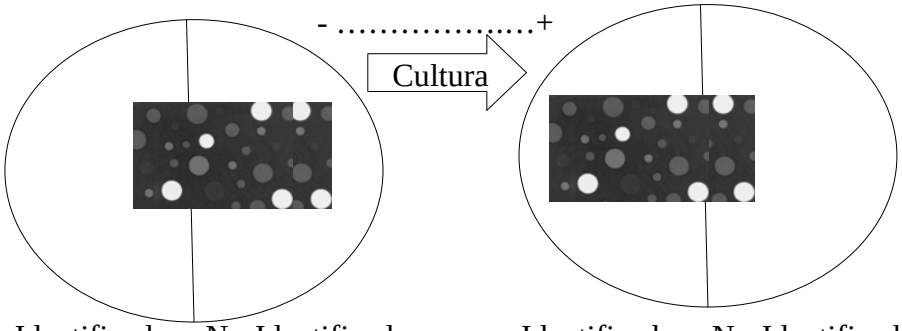
Más de una año despues, se ve que hay más spam, más virus, más “Phishing”, más gusanos y en general mas “hackeo”. Los “Hackers” y Cibercriminales son ahora más inteligentes, más rápidos y causan más daños que nunca.

1- Introducción

El Universo

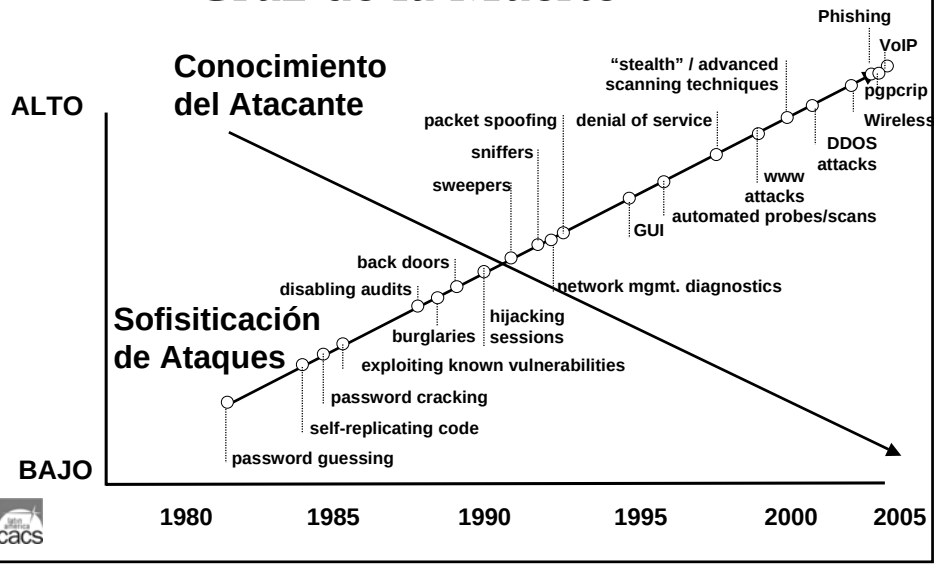


U Incidentes de Seguridad en las Organizaciones



1- Introducción

Cruz de la Muerte



1- Introducción

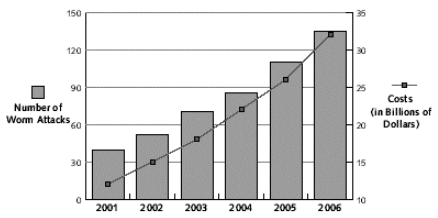
Vulnerabilidades

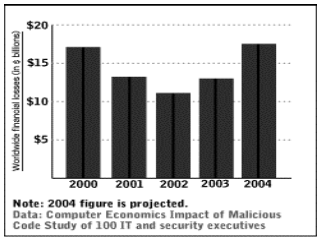
- Code Red Worm: $2.4B in 24 hours.
- Slammer Worm: $1B.
- Love Bug Virus: $8.7B in 15 hours.
- Denial of Service: $1.2B in 4 hours.
- Nimda Worm: $1.2 B.

Speed of Worm Propagation
Source: The Yankee Group, 2004

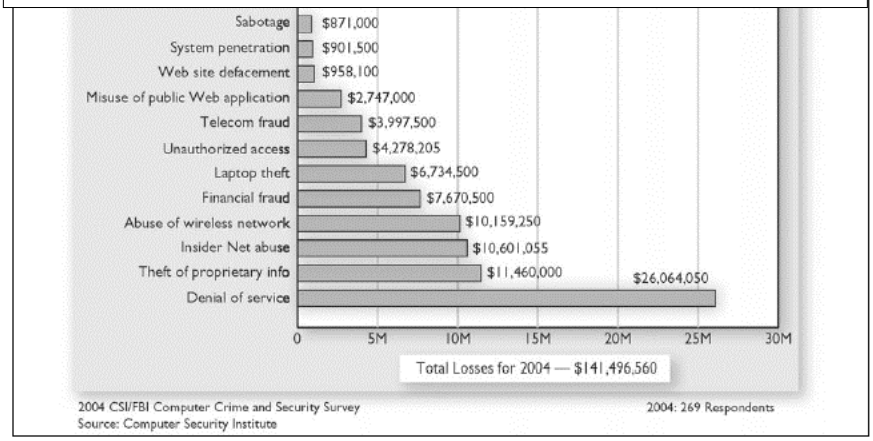
Worm	Day Zero	Infection Speed	Signature Available
Nimda	09/18/01	30 minutes	Day zero + 3 days
Slammer	01/25/03	10 minutes	Day zero + 1 day
Blaster	08/11/03	60 minutes	Day zero + 12 hours
Sasser	05/01/04	120 minutes	Day zero + 1 day

Worldwide Worm Epidemic
Source: The Yankee Group, 2004

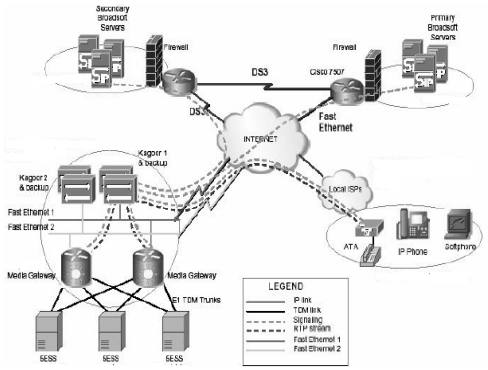




Pérdidas por tipos de incidentes



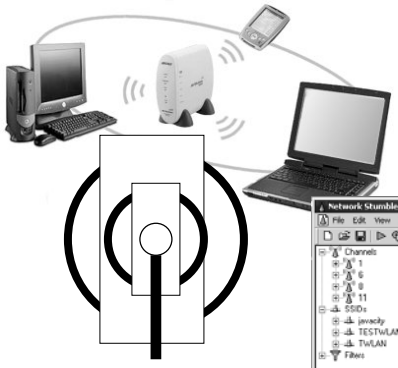
Amenazas en VoIP



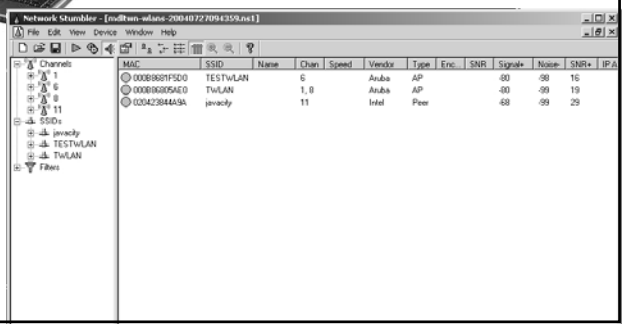
- Registration Hijacking, SIP
- Impersonating a Server, SIP
- Man in the middle, SIP
- Denial of Service
- Service Misuse
- Unauthorized modification
- Unauthorized access to ATA
- Hardware Failure
- Loss of Service
- Malicious Code
- Unauthorized privileges

1- Introducción

Amenazas en Wireless

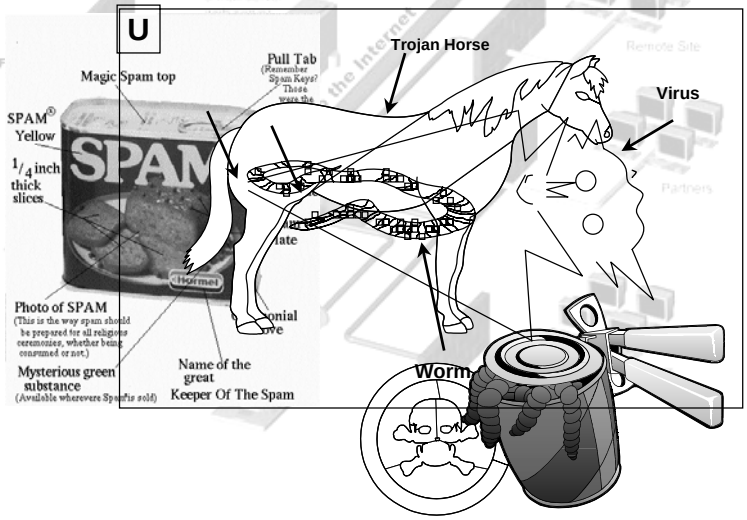


- SSID Finding
- MAC Address Modification
- WEP Cracking
- Access Points inside



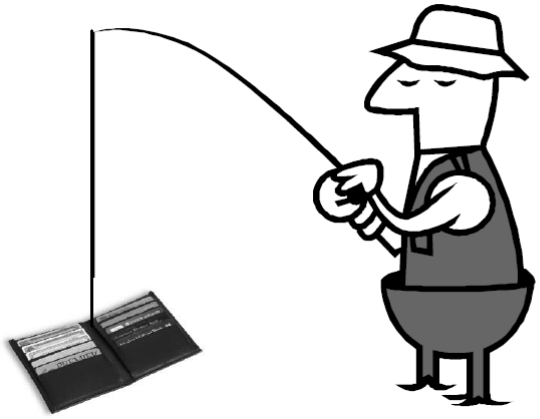
1- Introducción

e-Terror



1- Introducción

e-terror, *Phishing*



1- Introducción

e-terror, *Phishing*

Phishing Attack Example: eBay

SAMPLE EMAIL

The World's Online Marketplace®

Live Help

Dear valued customer

Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problems please **click here** and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

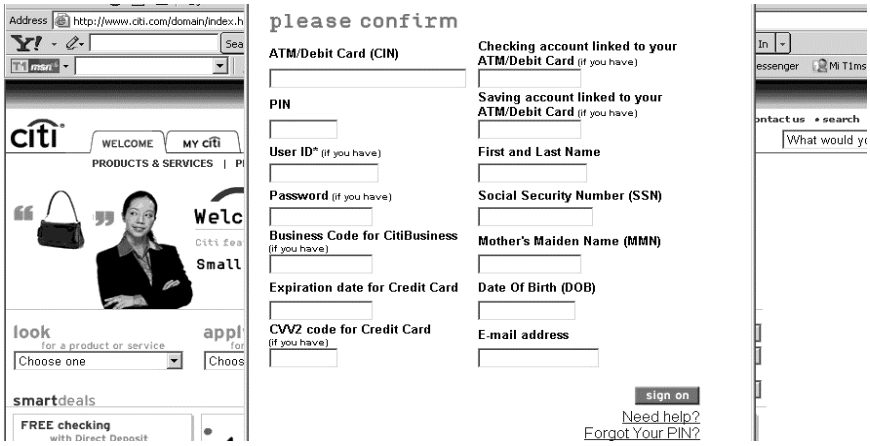
For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team. This is an automatic message.
Please do not reply.

1- Introducción

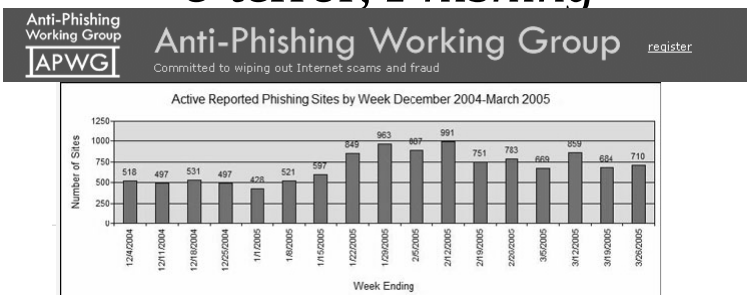
e-terror, *Phishing*



cacs

1- Introducción

e-terror, *Phishing*



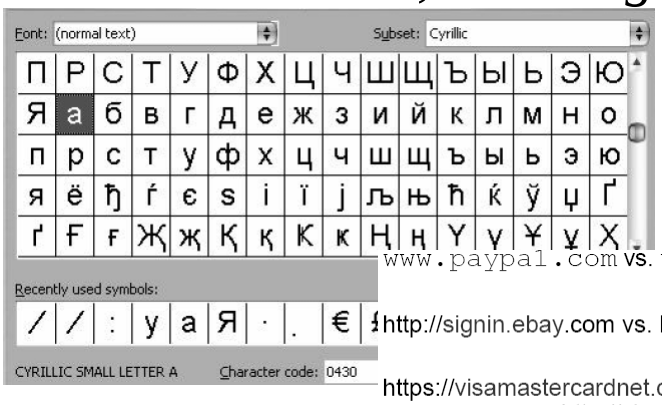
Recent Phishing Attacks:

Phish Alerts Courtesy Tumbleweed Communications' Message Protection Lab

- 10-05-05 - Paypal - 'Unauthorized Account Access'
- 09-05-05 - SouthTrust - 'Important Secuity Issue !!!'
- 03-05-05 - eBay - 'UpdateYour Account'
- 29-04-05 - Paypal- 'Update Account.'
- 27-04-05 - Marshall & Ilsley Bank- 'Security Update!'
- 25-04-05 - Citizens Bank - 'Citizens Bank Instant 5 USD reward survey'
- 22-04-05 - Ameritrade - 'Ameritrade Online Application'

cacs

e-terror, *Phishing*



www.paypal.com vs. www.paypal.com

http://signin.ebay.com vs. http://ebay.sign1n.com

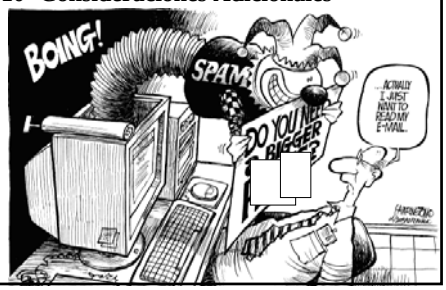
https://visamastercardnet.com/visamc/
http://visamcsecure.com/visamc/

Link as a Picture

cacs

Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

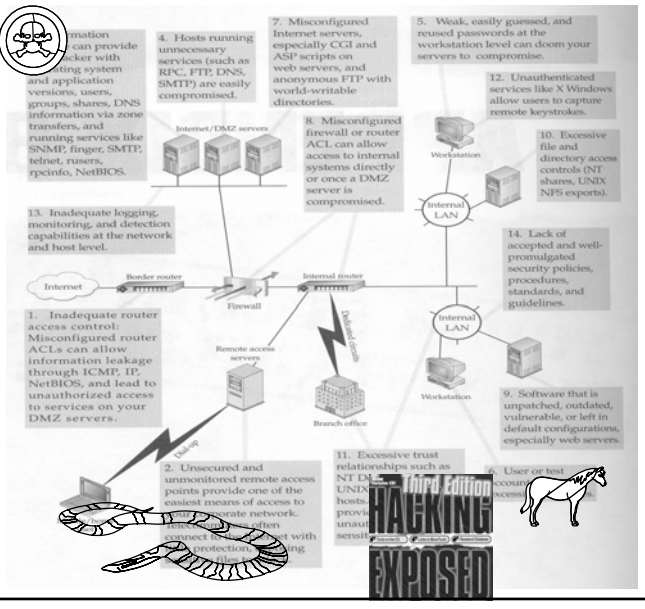


cacs

2-Problemática actual en materia de incidentes

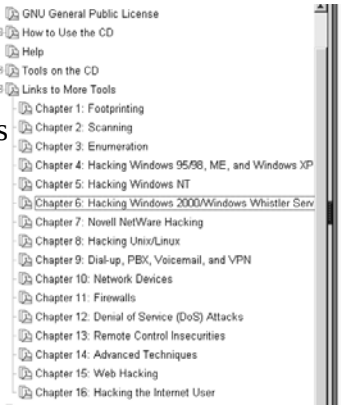
2- Problemática actual en materia de incidentes

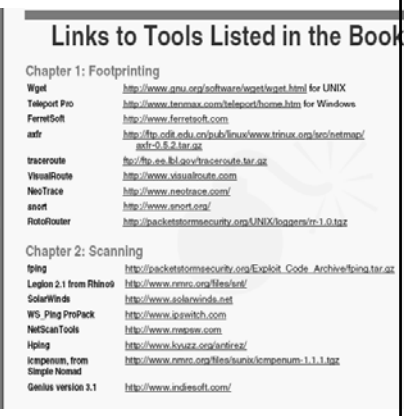
•Hackers conocen muy bien las vulnerabilidades



2- Problemática actual en materia de incidentes

•Hackers conocen muy bien las vulnerabilidades





2- Problemática actual en materia de incidentes

PASSWORD DATABASE

http://www.phenoelit.de/dpl/dpl.html

The Default Accounts Database is a collection of accounts and passwords that are, by default, the initial passwords for specific accounts on a given computer system. Sometimes these passwords are installed out-of-box, sometimes they are automatically installed by software, and sometimes they are installed by consultants that are brought in to perform services. This list should be used as a resource for computer security consultants interested in testing the security configuration of equipment.

B

Manufacturer	Product	Revision	Protocol	User ID	Password	Access Level	Comment
Bay Networks	Router		Telnet	Manager	(none)	Admin	
Bay Networks	Router		Telnet	User	(none)	User	
Bay Networks	SuperStack II		Telnet	security	security	Admin	
Bay Networks	Switch	350T	Telnet	n/a	NetICs	Admin	
Microsoft	Windows NT		Multi	(null)	(none)	User	Redbutton Hole
Microsoft	Windows NT		Multi	Administrator	Administrator	Admin	
UNIX	Generic		Multi	adm	adm	Admin	
UNIX	Generic		Multi	adm	(none)	Admin	
UNIX	Generic		Multi	admin	admin	User	
Cisco	CiscoWorks 2000			admin	cisco	Admin	
Cisco	CiscoWorks 2000			guest	(none)	User	
Cisco	ConfigMaker			cmaker	cmaker	Admin	
Cisco	IOS		Multi	cisco	cisco		
Cisco	IOS		Multi	enable	cisco		IOS technically has no default pw

2- Problemática actual en materia de incidentes

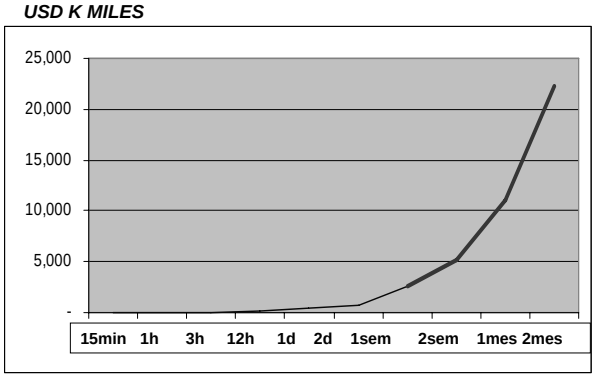
Confidencialidad, Integridad y Disponibilidad

Los incidentes pueden atacar directamente a las diversas características de la Seguridad de Información

C	I	D
	Banca	Carriers
Militar		
	Hospitales	
	Gobierno	
	Medios	

2- Problemática actual en materia de incidentes

Como pueden impactar incidentes de Seguridad en aspectos financieros



En la *Gráfica de Impactos financieros vs indisponibilidad* en el servicio XYZ, se muestra la pérdida en el ingreso considerando un evento de afectación total del servicio

2- Problemática actual en materia de incidentes

Como pueden impactar incidentes de Seguridad en aspectos legales y regulatorios

- SOX, Financial Information
- Mexico, Federal telecommunications law, 49 article (Confidentiality)
- HIPAA (The Health Insurance Portability and Accountability Act of 1996)
- NAFTA, article 1721, Confidential Information

2- Problemática actual en materia de incidentes

Como pueden impactar incidentes de Seguridad en aspectos de imagen

Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

3- Adversarios y taxonomía de incidentes

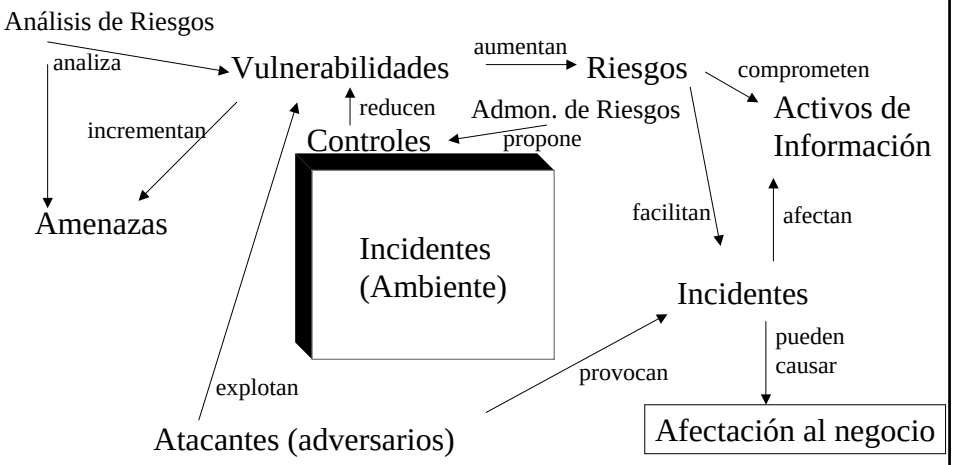
3- Adversarios y taxonomía de incidentes

Riesgo.
La posibilidad que una particular amenaza impactará en forma adversa a los activos de información por medio explotar determinadas vulnerabilidades

Amenaza.
Cualquier circunstancia o evento con un potencial impacto adverso a los activos de información

Vulnerabilidad.
Una debilidad en un activo de información que puede ser explotada causando un potencial impacto adverso

3- Adversarios y taxonomía de incidentes



Riesgo = Vulnerabilidad * Impacto

3- Adversarios y taxonomía de incidentes

Amenazas comunes relacionadas de Seguridad de Información (ejemplos)

- Errores
- Mal uso
- Accidentes
- Código malicioso
- Eventos de la naturaleza
- Accesos / cambios no autorizados
- Fraudes
- Robos
- Falla de equipo/ software
- Pérdida de Servicios

3- Adversarios y taxonomía de incidentes

Vulnerabilidades comunes relacionadas de Seguridad de Información (ejemplos)

- Software defectuoso
- Equipo mal configurado
- Políticas no reforzadas en tecnologías
- Pobre diseño de red
- Staff insuficiente
- Contraseñas débiles
- Tecnología no probada
- Comunicaciones no protegidas
- Falta de redundancia
- Sistemas operativos no actualizados

3- Adversarios y taxonomía de incidentes

Adversarios:

- Hackers
- Criminales solitarios
- Personal interno
- Espionaje industrial
- Prensa
- Crimen Organizado
- Policía
- Terroristas
- Organizaciones de Inteligencia
- “Infowarriors”

Bruce Schneier,
Libro Secrets & Lies

3- Adversarios y taxonomía de incidentes

Impactos causados por incidentes de Seguridad de Información (ejemplos)

- Pérdida económica
- Falla de cumplir con Legislación
- Pérdida de Reputación
- Reducción en el valor percibido por los clientes
- Poner en peligro a empleados o clientes
- Pérdida de confianza (!)
- Pérdida de oportunidades de negocios
- Reducción de eficiencia operacional
- Interrupción de actividades de negocios

3- Adversarios y taxonomía de incidentes

Clasificación de Ataques en materia de Seguridad de Información

- Visión de seguridad de red
- Visión por nivel de actividad maliciosa (Activos / Pasivos)

3- Adversarios y taxonomía de incidentes

- Visión de Seguridad de red

Diferentes tipos de vulnerabilidades, ataques y amenazas están relacionadas con diferentes niveles de las redes.

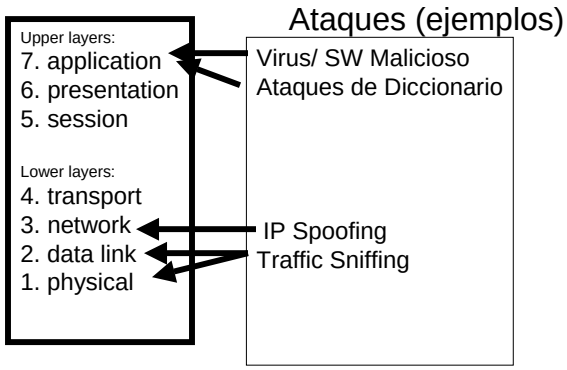
Con este enfoque nos permite entrar a más detalle en la tecnología de un ambiente complejo en cada una de las tecnologías relacionadas a las diversas capas del modelo OSI.

Upper layers:
7. application
6. presentation
5. session

Lower layers:
4. transport
3. network
2. data link
1. physical

3- Adversarios y taxonomía de incidentes

•Visión de Seguridad de red



3- Adversarios y taxonomía de incidentes

•Visión por nivel de actividad maliciosa

Ataques Pasivos (ejemplos)

- Análisis de Red
- Intercepción
- Análisis de tráfico

3- Adversarios y taxonomía de incidentes

•Visión por nivel de actividad maliciosa

Ataques Activos (ejemplos)

- Brute Force
- Masquerading
- Packet Reply
- Message Modification
- Unauthorized Access
- Denial of service
- Dial-in Penetration
- E-mail bombing
- E-mail spoofing

3- Adversarios y taxonomía de incidentes

Metodología típica de una intrusión de un Hacker

1.	"Scan" de especificas direcciones IP	Ataques Pasivos
2.	Seleccionar objetivos "vivos"	
3.	Ejecutar un "Scan" de puertos	
4.	Seleccionar puertos con posibles vulnerabilidades	
5.	Analizar detalles de configuración de puertos	
6.	Buscar las vulnerabilidades en base a paso anterior	
7.	Si vulnerabilidades existen se buscan los códigos de explotación de las vulnerabilidades	
8.	Ejecutar código de explotación contra objetivos	Ataques Activos
9.	Login, instalar "rootkit" y otros programas	
10.	Esconder huellas y alterar bitácoras del sistema	
11.	Modificar utilerías del sistema	
12.	Logout	

Impacto al negocio

-

+

Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

4- Modelo de administración de incidentes

4- Modelo de administración de incidentes

Definición de respuesta a incidentes

Respuesta a incidentes es un término generalizado que se refiere a la respuesta por una persona o una organización a una violación o a un ataque.

Una reacción organizada y cuidadosa a un incidente puede significar la diferencia entre la recuperación completa y el desastre total.

Esta disciplina tiene que ser:
Costo-efectiva, orientada a negocio, eficiente, repetible y predecible

4- Modelo de administración de incidentes

Objetivos del proceso de respuestas a incidentes

- Restaurar y mantener las actividades normales del negocio
- Incrementar la defensa y supervivencia contra incidentes futuros
- Identificar rápidamente y recuperarse de un incidente
- Continuamente monitorear y verificar la integridad de los activos
- Prevenir incidentes futuros similares
- Investigar sobre potenciales amenazas antes que se materialicen
- Educar a la organización para alinearse al proceso

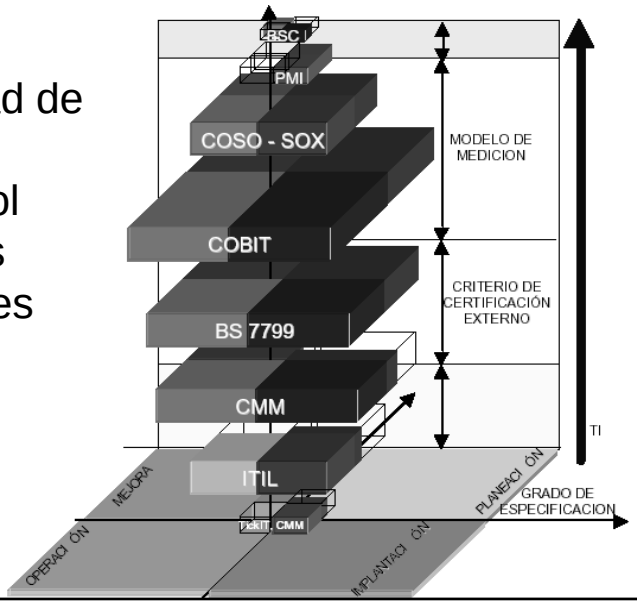
4- Modelo de administración de incidentes

Metas del proceso de respuestas a incidentes

- Minimizar la interrupción del negocio
- Proveer reportes precisos y recomendaciones útiles
- Minimizar exposiciones y compromisos de la información
- Proteger la reputación de la organización y sus activos
- Elevar el nivel de concientización de la alta administración sobre la importancia de un equipo de respuesta a incidentes y su rol crítico que juega para salvagauardar la continuidad e integridad de la organización

4- Modelo de administración de incidentes

Diversidad de Objetivos de Control , diversos estándares



4- Modelo de administración de incidentes

DS5 Delivery & Support
Ensure Systems Security

COBIT

DETAILED CONTROL OBJECTIVES *continued*

5.8 **Data Classification**
CONTROL OBJECTIVE
Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived

5.11 **Incident Handling**
CONTROL OBJECTIVE
Management should establish a computer security incident handling capability to address security incidents by providing a centralised platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

cacs

4- Modelo de administración de incidentes

ITIL (IT Infrastructure Library)

#5- Incident Management

Meta:
Restaurar la operación normal del servicio tan rápido como sea posible minimizando los impactos adversos sobre las operaciones del negocio

cacs

4- Modelo de administración de incidentes

BRITISH STANDARD | BS 7799-2:2002

A.6 Personnel security

A.6.3 ***Responding to security incidents and malfunctions*** *Control objective:* To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.			**6.3**
Controls			
A.6.3.1	*Reporting security incidents*	Security incidents shall be reported through appropriate management channels as quickly as possible.	**6.3.1**
A.6.3.2	*Reporting security weaknesses*	Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services.	**6.3.2**
A.6.3.3	*Reporting software malfunctions*	Procedures shall be established for reporting software malfunctions.	**6.3.3**
A.6.3.4	*Learning from incidents*	Mechanisms shall be put in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.	**6.3.4**
A.6.3.5	*Disciplinary process*	The violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process.	**6.3.5**

cacs

4- Modelo de administración de incidentes

PCAOB y COBIT

Sarbanes Oxley

		PCAOB IT General Control Heading			
	Cobit Control Objective	**Program Development**	**Program Changes**	**Computer Operations**	**Access to Program and Data**
AI2	Acquire or develop application Software	✓	✓	✓	✓
AI3	Acquire technology Infraestucture	✓	✓	✓	
AI4	Develop and maintain policies and procedures	✓	✓	✓	✓
AI5	Install and test application software and technology infraestucture	✓	✓	✓	✓
AI6	Manage changes		✓		✓
DSI	Define and manage service levels	✓	✓	✓	✓
DS2	Manage third-party services	✓	✓	✓	✓
DS5	Ensure system security			✓	✓
DS9	Manage the configuration			✓	✓
DS10	Manage problems and incidents			✓	
DS11	Manage data			✓	✓
DS13	Manage operations			✓	✓

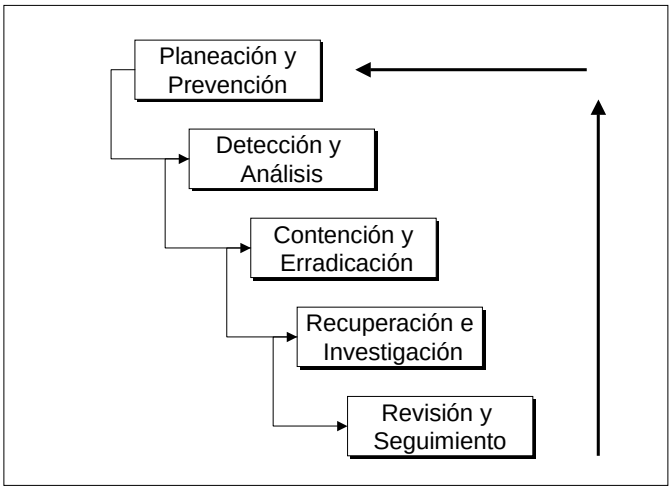
cacs

4- Modelo de administración de incidentes

Modelo de Administración de incidentes

4- Modelo de administración de incidentes

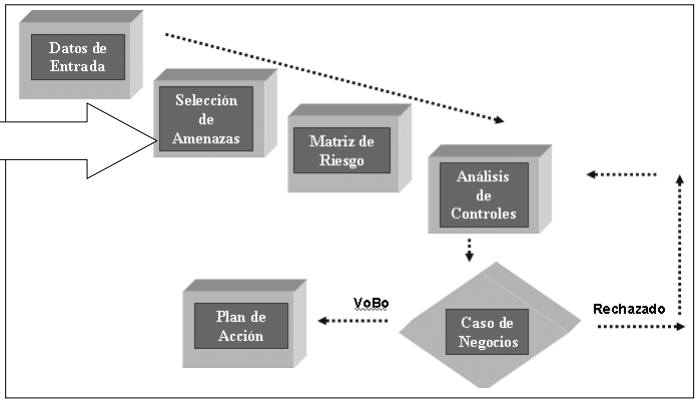
Proceso de respuesta a incidentes



4- Modelo de administración de incidentes

La información de incidentes es fundamental
como suministro de entrada al Análisis de Riesgos

Modelo de Análisis de Riesgos de TI



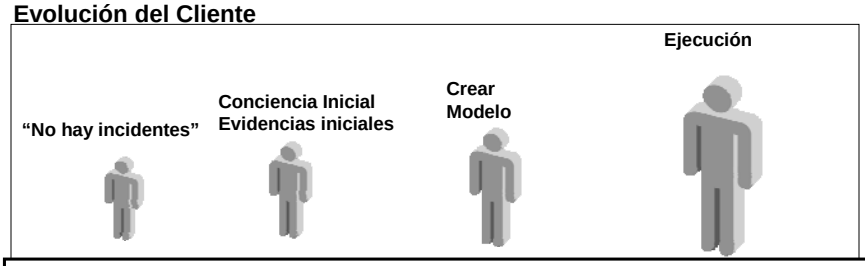
4- Modelo de administración de incidentes

Due Diligence/ Due Care

Conducta del Cliente

Due Diligence	Due Care

Evolución del Cliente



Due Care, implica razonable cuidado y competencia, no infalibilidad o extraordinario rendimiento, si hay fallas para lograr los mínimos estándares puede ser considerado esto como negligencia y llevar a la pérdida de activos, vidas y casos legales.

Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

5- Normatividad necesaria

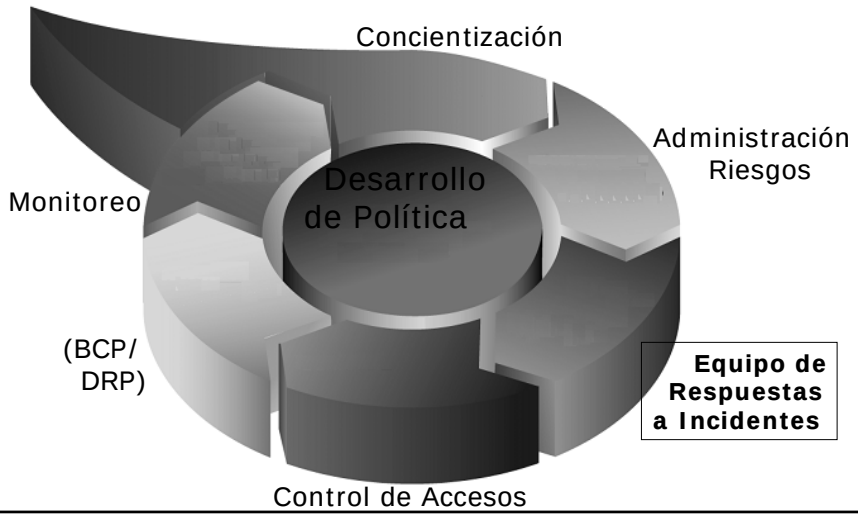
5- Normatividad necesaria

La Alta Administración debe:

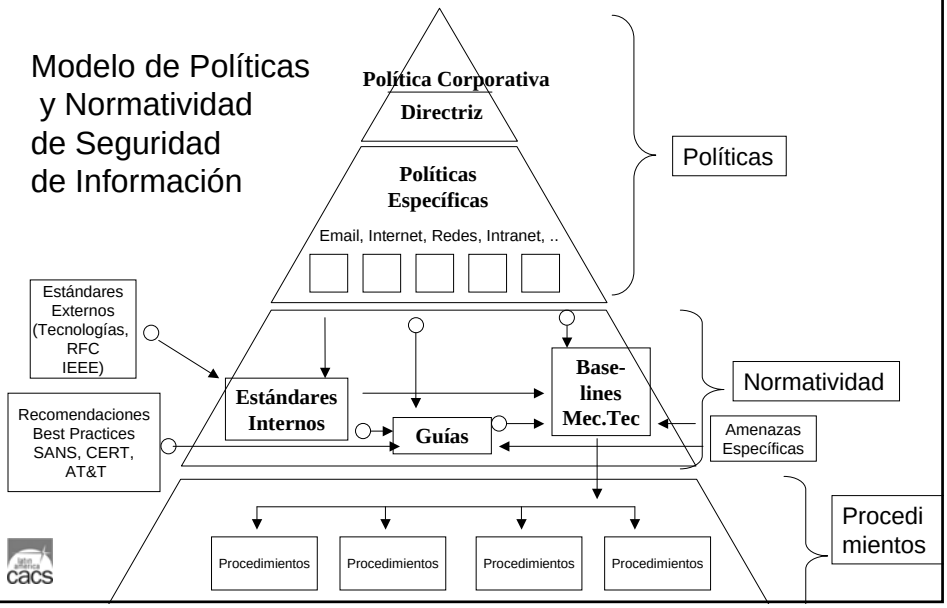
- Proveer todo el soporte y autorización a los equipos de respuestas a incidentes
- Decidir la prioridad corporativa respecto a los incidentes entre estas opciones:
  - Proteger y olvidar
  - Perseguir a los atacantes

5- Normatividad necesaria

Procesos estratégicos de Seguridad de Información



5- Normatividad necesaria



5- Normatividad necesaria

Política Corporativa, objetivos relativos a incidentes (ejemplo)

Reporte de incidentes.- Todo incidente que amenace la seguridad del personal, de la información propia y de otros en custodia, de las instalaciones y, en general, de todo aquello que constituye la propiedad de la empresa, deberá ser reportado a la Dirección de Seguridad de Información o de Recursos Humanos según aplique.

cacs

5- Normatividad necesaria

Directriz relativa a incidentes (ejemplo)

Respuesta ante incidentes y malfuncionamientos.- Todo incidente que afecte la seguridad de la información, deberá ser reportado siguiendo los procedimientos establecidos por el Comité de Seguridad de la Información, tan rápido como sea posible.

Todos los empleados y terceros deberán ser capacitados en los procesos para reportar los diferentes tipos de incidentes (transgresiones de seguridad de la información, amenazas, vulnerabilidades, malfuncionamientos, etc.) que pudieran tener un impacto en la seguridad de activos de información de la empresa. A ellos se les deberá requerir el reportar cualquier incidente observado o bajo sospecha tan pronto como sea posible, al Coordinador de la Seguridad de la Información de la Dirección Funcional que corresponda y/o al *Director de Seguridad de la Información.*

Es la responsabilidad de cada empleado conocer las directrices y procedimientos de seguridad y acatarlas; así como reportar cualquier cuestión que afecte los activos de información, a los respectivos Coordinadores de las Direcciones Funcionales y al *Director de Seguridad de la Información.*

cacs

5- Normatividad necesaria

Normas específicas (ejemplos)

- Repositorio de incidentes
- Asignación de Severidades
- Descripciones de puesto
- Proceso de comunicación de incidentes
- Proceso de respuesta a incidentes
- Capacitación
- Roles
- Filosofía de Perseguir / Responder

cacs

5- Normatividad necesaria

Normas específicas (ejemplos)

Nivel de Severidad de incidentes

Nivel 1-Incidente que afecta a sistema crítico, intrusión en sistema no crítico con comunicación con un sistema crítico, afectación al negocio

Nivel 2- Incidente que afecta a Sistema No Crítico , preparación de ataque a sistema crítico

Nivel 3- Preparación de ataque a sistema no crítico

Nivel 4- Mal uso de un activo de información o violación de política interna

Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

6- Roles

Organizaciones que deben de ser incluidos en el Equipo de Respuesta a Incidentes (ejemplos)

- Seguridad de Información
- Legal
- Relaciones Públicas
- Recursos Humanos
- Administradores de Sistemas
- Administradores de Red
- Desarrolladores de Sistemas
- Administradores de Bases de Datos

6- Roles

Cruz de Malta

Conocimiento

P
e
r
s
o
n
a

X

Organización

6- Roles

Cruz de Malta

- Arquitectura y Desarrollo de Sistemas
- Automatización de Oficinas Sistemas
- Desarrollo Tecnológico en Internet
- Sistemas Corporativos
- Red Sistemas
- Sistemas CRM y Facturación
- Soporte de Sistemas
- Data Center
- Ingeniería
- RRHH
- Legal
- Comunicación
- Finanzas
- Seguridad de Información
- etc.

X

Organización

6- Roles

Cruz de Malta

- Correo Corporativo
- PBX
- Firewall
- Herramienta de Detección de Intrusos
- Aplicaciones Corporativa: Siebel / Arbor
- Sistemas y Aplicaciones Corporativos
- Application Servers (JRUN, JDBC, TomCat, iPlanet)
- Lenguajes:PERL, C, C++, java, shell UNIX
- Lenguajes: XML; HTML, Power Builder
- Servidores Web (IIS, Apache, Zeus)
- Sistema Operativo: Windows 98, XP
- Sistema Operativo: Windows 2K, NT
- Sistemas Operativos: Solaris
- Sistemas Operativos: HPUX
- Base de Datos: SQL
- Base de Datos: Oracle, Sybase

Conocimiento

X

6- Roles

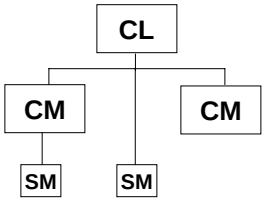
Cruz de Malta

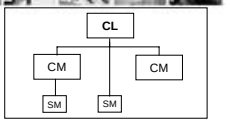
1= Primario,
2= Secundario,
3= Soporte

											3			3		**6**	Firewall
							2							3		**4**	Herramienta de Detección de Intrusos
						2							1			**3**	Aplicaciones Corporativa: Siebel / Arbor
												2			1	**3**	Sistemas y Aplicaciones Corporativos
					2						3			3		**4**	Aplicaciones de Red, Servicios y Protocolos relacionados:SMTP, HTTP, FTP, TELNET, LDAP, SMNP, DNS
					2				1							**2**	Application Servers (JRUN, JDBC, TomCat, iPlanet)
											3					**4**	Redes Públicas de Datos: Internet, IP VPN ; Protocolos de Red (MPLS, ICPM, TCP, UDP) y de Ruteo (Interior, Exterior)
			3													**3**	Redes Públicas de Datos para Protocolos ATM, Frame Relay
				2						1						**4**	Redes de Voz: ISDN, PSTN , IN, VoIP
					2				1							**3**	Lenguajes:PERL, C, C++, java, shell UNIX
					2				1							**3**	Lenguajes: XML; HTML, Power Builder
					1				2							**3**	Servidores Web (IIS, Apache, Zeus)
								2								**3**	Sistema Operativo: Windows 98, XP
								2								**3**	Sistema Operativo: Windows 2K, NT
							1									**3**	Sistemas: Operativos: IRIX
3							2									**4**	Sistemas Operativos: Solaris
3							2									**4**	Sistemas Operativos: HPUX
							2									**3**	Sistemas Operativos: Linux
1															3	**3**	Base de Datos: SQL
1															3	**3**	Base de Datos: Oracle, Sybase
1	1	1	3	2	1	2	1	2	1	1	3	2	1	3	1		**Conocimiento**
															Ruben Beltrán	TOTAL	**Persona**
																	Organización
																0	Arquitectura y Desarrollo de Sistemas(K. Rodríguez)
								X								**3**	Automatización de Oficinas (G. Welsh)
																1	Internet Data Center (I. Guzmán)
										X						**1**	Ingeniería
					X											**4**	O&M (Datos, Servidores)
			X								X			X		**7**	Planeación de Tecnología & Desarrollo de Servicios
									X							**2**	Sistemas Desarrollo Tecnológico en Internet (Alejandro Leal)
												X			X	**2**	Sistemas Corporativos (Elba González)
	X	X														**2**	Red Sistemas (Manuel Revelles)
						X							X			**2**	Sistemas CRM y Facturación (Gabriel Muñoz)
X																**1**	Soporte de Sistemas (Alberto Torres)
							X									**4**	Tier Datos
				X												**2**	Tier Voz

Estructura del Equipo de Respuesta

- Core Leader (CL)
- Core Member (CM)
- Support Member (SM)



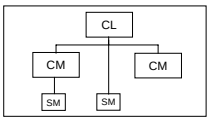


Core Leader

- Líder global en los incidentes
- Asigna severidades más altas de incidentes
- Interfase (Directores, CEO, CFO, InfoSec)
- Asegura que se siga la Política

6- Roles

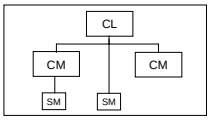
Core Member



- Interfase con Core Leader y demás miembros
- Interactúa con CL para tomar decisiones
- Facilita la identificación de causa raíz así como su fuente

6- Roles

Support Members



- Proveen experiencia técnica y profesional
- Dos categorías (Técnica y no Técnica)
- Proveen asesoría profesional (subject matter experts)para resolver incidentes donde se requiere especificas habilidades dependiendo de su función

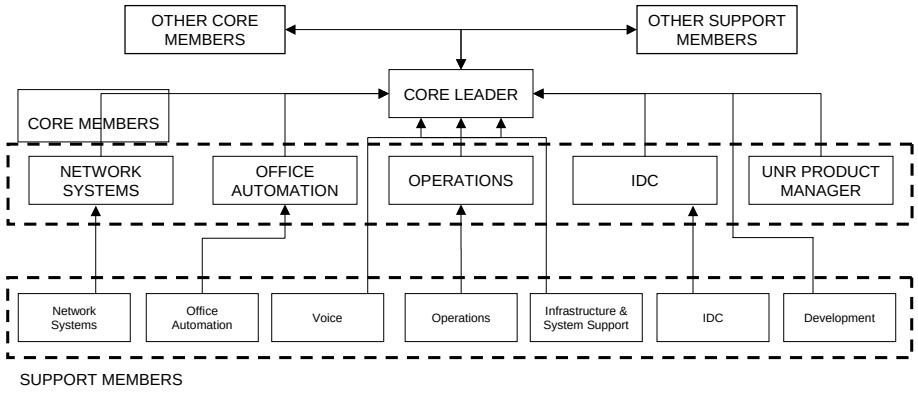
Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

7- Proceso de Comunicación de Incidentes

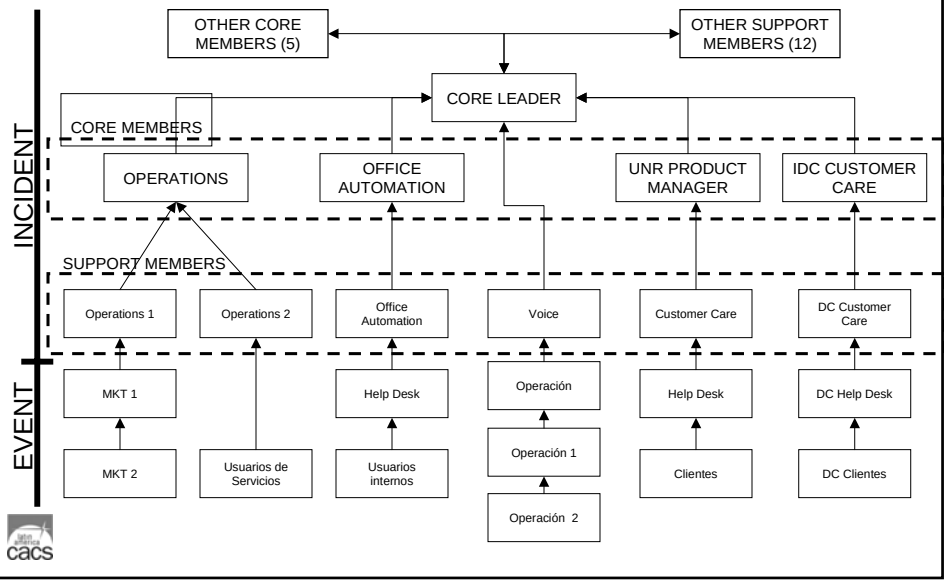
7- Proceso de Comunicación de Incidentes

Proceso de Alto Nivel



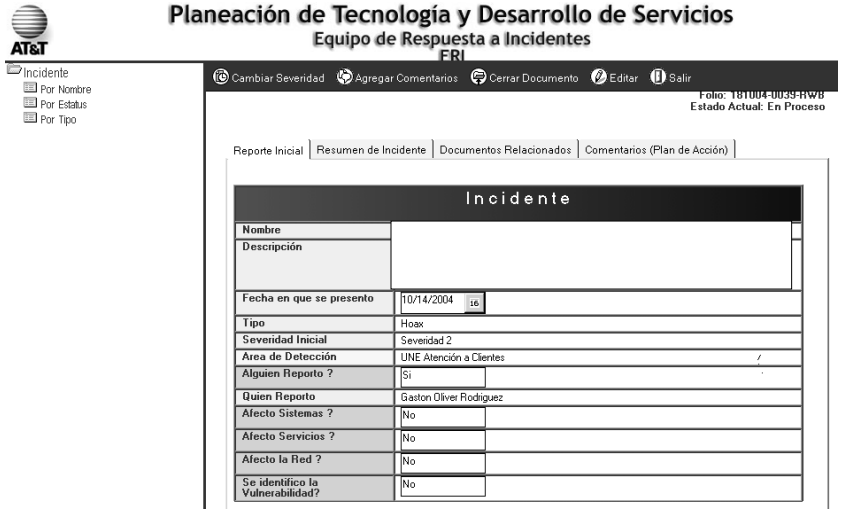
7- Proceso de Comunicación de Incidentes

Proceso detallado



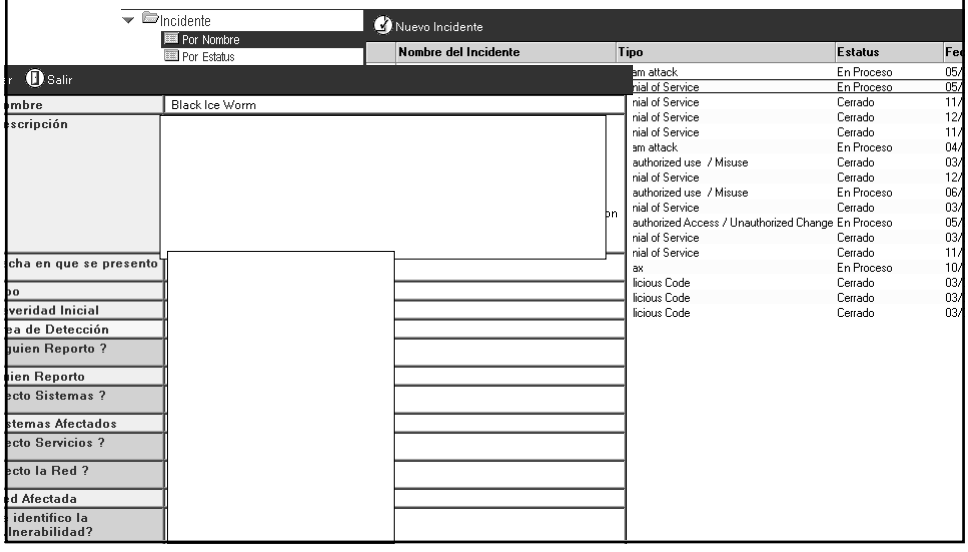
7- Proceso de Comunicación de Incidentes

Repositorio de incidentes



7- Proceso de Comunicación de Incidentes

Repositorio de incidentes



7- Proceso de Comunicación de Incidentes

INCIDENT IDENTIFICATION REGISTER

To be filled out during Detection & Analysis Phase

Date of Event: | INCIDENT #:

Person Initiating Documentation:

Name:
Phone Number:
Fax Number:
E-Mail:

Type of Incident:

Denial of Service	Espionage	Hoax
Malicious Code	Probe	Unauthorized Access
Unauthorized use	Other (explain)	

Location of Incident:

Address:
Building:
Room:

Additional Information:

How and when was the Incident Detected?

Assigned Severity Level:
Note: Highest level is Level 1, Lowest level is level 4

Level 1 | Explain Reason Why:

To be filled out during Containment & Eradication Phase

Isolate affected systems:

Was the system removed form network? Yes No

If NO what was the reason:

If YES time system(s) were disconnected:

Backup affected system(s):

Was system backup successful for all systems? Yes No

If NO, explain:

Name of person(s) completing backup(s):

Name:
Phone Number:
Fax Number:
E-Mail:

Name:
Phone Number:

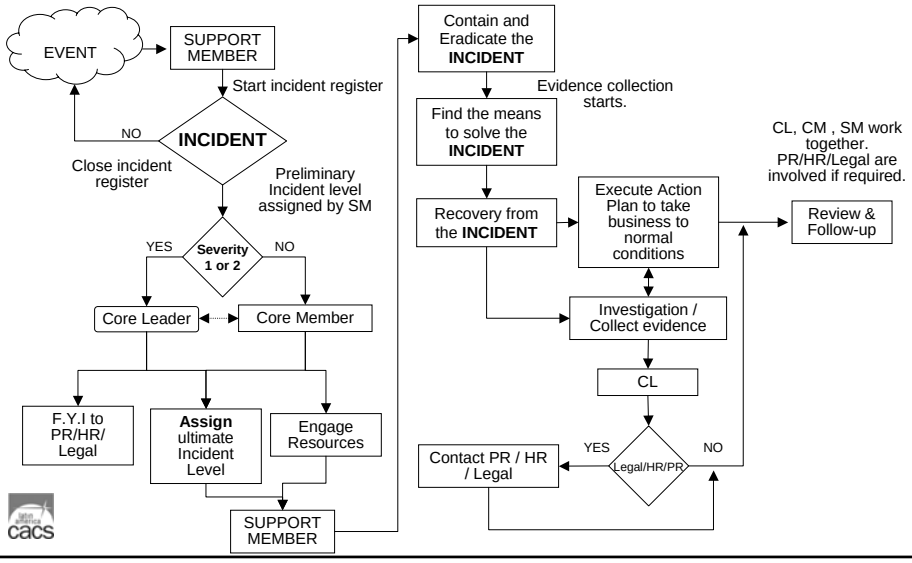
Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

8- Proceso de Atención a incidentes

8- Proceso de Atención a incidentes

Proceso de Respuesta a Incidentes (ejemplo)



8- Proceso de Atención a incidentes

Matriz de Procesos detallados de respuesta a incidentes (Muestra)

Incident / Areas of Knowledge	DoS / DDoS	Intrusions (Unauthorized Access / Unauthorized Changes)	Malicious Software (Virus / Worms)	Misuse (Unauthorized use or misuse of information processing facilities)	OS Vulnerability Exploit	Application Vulnerability Exploit
Network	X	X	N/A	X	N/A	N/A
Application	X	X	X	X	N/A	X
UNIX	N/A	X	X	X	X	N/A
Windows	N/A	X	X	X	X	N/A
Telecom	X	X	N/A	X	N/A	N/A

8- Proceso de Atención a incidentes

Matriz de Procesos detallados generales de respuesta a incidentes (Muestra)

CASE 1: DETECTION AND RESPONSE FOR DOS ON A NETWORK

CASE 2: DETECTION AND RESPONSE FOR INTRUSION (UNAUTHORIZED ACCESS/ UNAUTHORIZED CHANGES) ON NETWORK ELEMENT

CASE 3: DETECTION AND RESPONSE FOR MISUSE OF (UNAUTHORIZED USE OR MISUSE) OF PROCESSING FACILITIES ON NETWORK SYSTEM

CASE 4: DETECTION AND RESPONSE FOR DOS ON APPLICATION OR NETWORK SERVICES

CASE 5: DETECTION AND RESPONSE FOR INTRUSION (UNAUTHORIZED ACCESS/ UNAUTHORIZED CHANGES) ON APPLICATION

8- Proceso de Atención a incidentes

Matriz de Procesos detallados específicos de respuesta a incidentes (Muestra)

CASE 1: DETECTION AND RESPONSE FOR MISUSE (UNAUTHORIZED USE OR MISUSE OF PROCESSING FACILITIES ON E-MAIL SERVER)

CASE 2: DETECTION AND RESPONSE FOR INTRUSION (UNAUTHORIZED ACCESS/ UNAUTHORIZED CHANGES) ON UNIX SYSTEM

CASE 3: DETECTION AND RESPONSE FOR INTRUSION ON A WEB SERVER (UNAUTHORIZED ACCESS / UNAUTHORIZED CHANGES) (IIS).

CASE 4: DETECTION AND RESPONSE FOR MALICIOUS SOFTWARE (VIRUS/WORMS) ON A SQL2000 ON WINDOWS SYSTEM

CASE 5: DETECTION AND RESPONSE FOR DDOS ON A NETWORK (CISCO BORDER ROUTER) LIMITED TO BANDWIDTH EXHAUSTION DOS/DDOS ATTACKS.

8- Proceso de Atención a incidentes

Case 4: Detection and Response for malicious software (virus/Worms) on a SQL2000 on Windows System

8- Proceso de Atención a incidentes

Introduction

The Introduction section is to highlight other potential security issues that affect SQL2000. But, the overall document will concentrate on the Slammer worm.

A DENIAL OF SERVICE On SQL 2000

Let's suppose that the server is tightly locked down and we cannot do anything as an unprivileged user. If we are evil enough, we can resort to simply crashing the server. Remember that all users can create temporary stored procedures and tables. So we are authorized to execute the following statements.

create table #tmp (x varchar(8000))

exec('insert into #tmp select "X"')

while 1=1 exec('insert into #tmp select * from #tmp')

This will create a temporary table and will run an endless loop inserting values into the table. Temporary tables are created in the tempdb system database and, after some time, the tempdb database will grow until it consumes all system resources and causes the SQL Server instance to fail or crash.

8- Proceso de Atención a incidentes

Exploiting Openrowset

Trying to find another way to execute operating system commands, we try another known vulnerability.

SELECT * FROM OPENROWSET('Microsoft.Jet.OLEDB.4.0', 'C:\database.mdb';'ADMIN';'', 'select *, Shell("notepad") from customers')

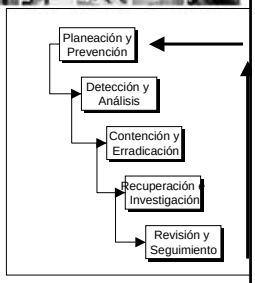
This doesn't work because the Jet sandbox blocks access to the Shell() function when it isn't executed from Microsoft Access. Let's try an older Jet OLEDB provider.

SELECT * FROM OPENROWSET('Microsoft.Jet.OLEDB.3.51', 'C:\database.mdb';'ADMIN';'', 'select *, Shell("notepad") from customers')

--database.mdb must be an MS Access 97 database

It works!!! This is because the Jet sandbox only blocks Jet 4.0 and we use an older version of Jet (3.51) that isn't blocked.

8- Proceso de Atención a incidentes

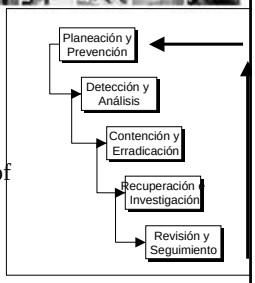


Planeación y prevención

The planning and prevention phase of an incidence response for detection and response for malicious software (virus/Worms) SQL2000 Windows System involves:

1. SQL2000 servers should have a baseline of all running processes, services and file system. Use Microsoft baseline security Analyzer.
2. Events, performance logs and alerts from systems, process and applications are properly configured and collected daily, securely stored, time stamped to a clock source and analyzed using a log analysis program and viewed daily by knowledgeable personnel. http://www.rhysome.com/ , http://www.gfi.com/lanselm/
3. …….

8- Proceso de Atención a incidentes



Detección y análisis

The ability to detect the SQL2000 slammer attack depends on prior planning and preparations, available tools and skills. The SQL2000 was a vast replicating worm with a network Denial of Service type signature.

1. Sudden massive network degradation. Router network links – ingress and egress were excessive. The pattern of traffic on the network was similar to a 'DoS' attack. If traffic patterns were being monitored and graphed – including segment 'top talker' and source and destination flows.

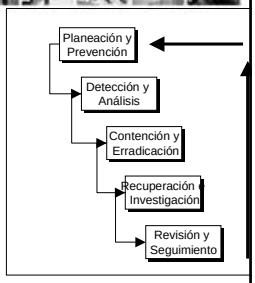
2. Internal local area network segments indicated excessive traffic.

3. Slow response from applications and services within the internal network and external networks. Services such as DHCP, DNS, email, etc were impacted if an infected SQL2000 computer was in that network segment.

4. ….

8- Proceso de Atención a incidentes

Contención y erradicación



The containment and eradication process strategy is formed based on the facts, gathered evidence, advisories, prior experience and the incidence level.

1. Document all steps including timelines. Documenting the steps and processes will be helpful later for prosecution and also 'lessons learned'.

2. Follow the Incidence Response process and procedure – contact the Core Leader and Core member prior to making any changes on the router(s)

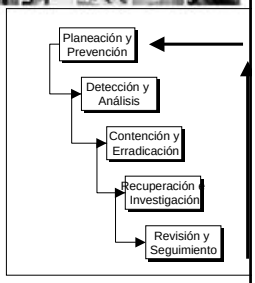
3. Create a clear and specific action plan on how to resolve the issue(s).

4. Disconnect the infected system from the network since the worm is fast spreading and network resource is severely impacted. The disconnection will prevent other systems from being infected.

5. …

8- Proceso de Atención a incidentes

Recuperación e investigación



1. Shut down systems

2. Reboot system – one at a time

3. Install solution based on advisories from CERT (www.cert.org), Microsoft (http://www.microsoft.com/security/), http://windowsupdate.microsoft.com/ and update anti-virus/worm software from product vendor.

4. Update IDS and firewall rules to detect worm

5. Disable the TCP library for MS SQL, this will disable port 1433 for those installations where the MS SQL server is installed on the same box as an IIS server.

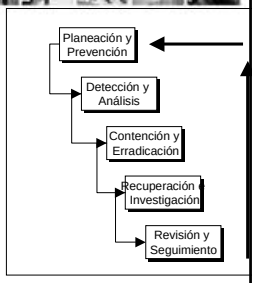
6. Review ALL installations of MS SQL and appropriately harden the installation. A guide for hardening MS SQL installations can be found at: http://www.sqlsecurity.com/

7. …..

8- Proceso de Atención a incidentes

Revisión y seguimiento

Refer to the General Incident Response Process



Agenda

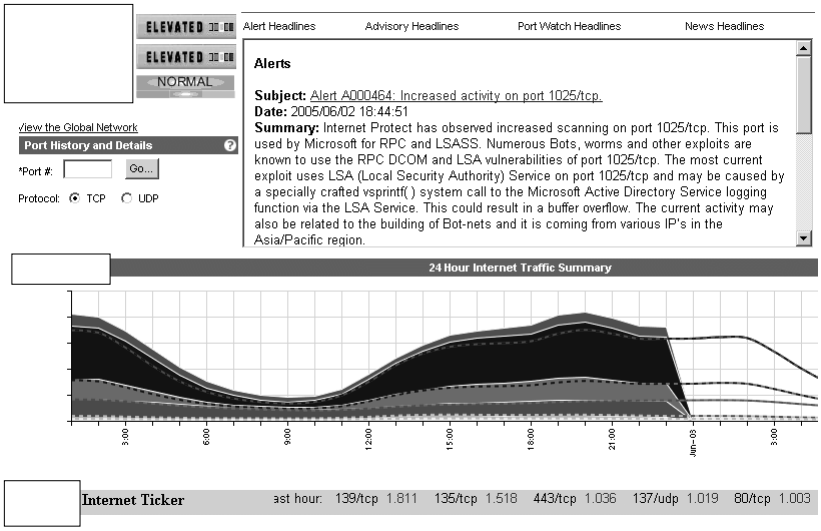
- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

9-Tecnologías relacionadas con la atención a incidentes

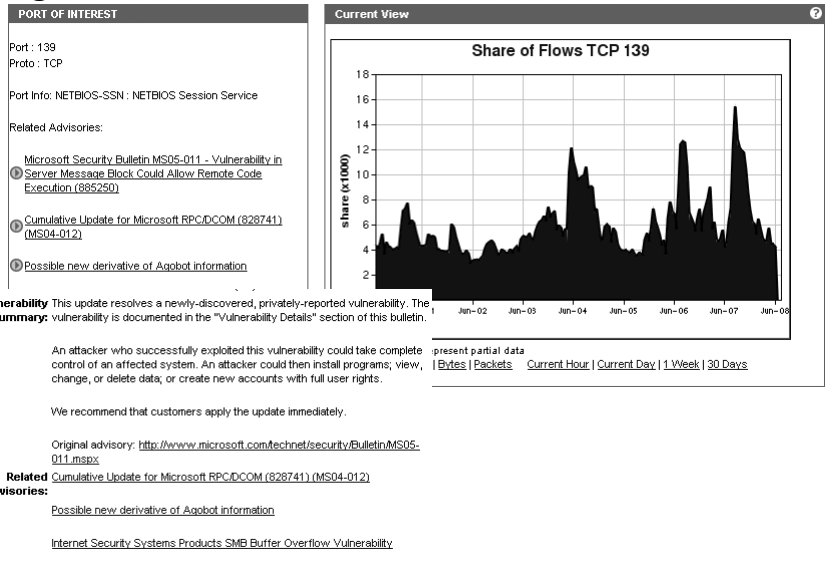
9-Tecnologías relacionadas con la atención a incidentes

- Intrusion Detection Systems (Network, Host)
- Intrusion Prevention Systems
- Honey Pots
- Integrity Checkers
- Firewalls
- Colectores
- Correlacionadores
- Parsers
- Agents (Vulnerabilities, policy enforcements)
- Forensics Kit
- Log Analyzers
- Hackers tools
-….

9-Tecnologías relacionadas con la atención a incidentes



9-Tecnologías relacionadas con la atención a incidentes



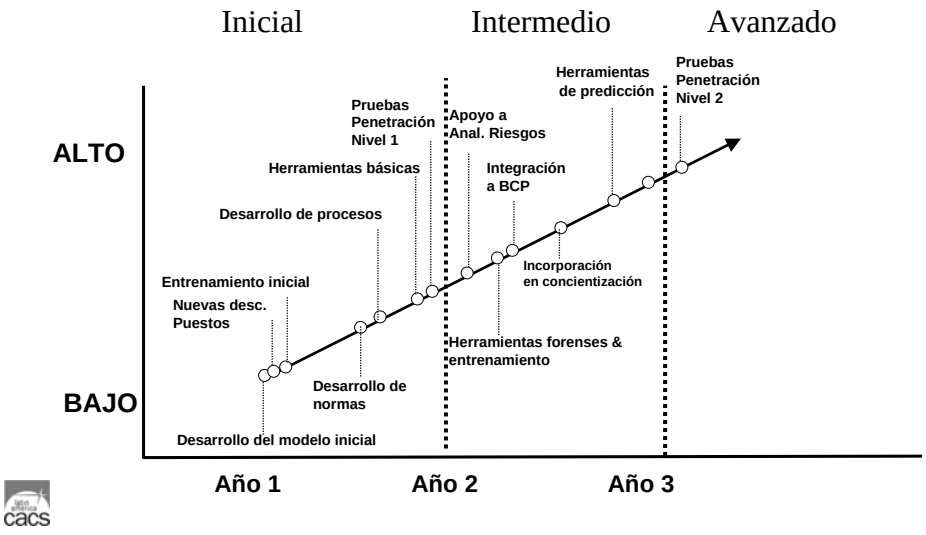
Agenda

- **1- Introducción**
- **2- Problemática actual en materia de incidentes**
- **3- Adversarios y Taxonomía de incidentes**
- **4- Modelo de administración de incidentes**
- **5- Normatividad necesaria**
- **6- Roles**
- **7- Proceso de Comunicación de Incidentes**
- **8- Proceso de Atención a Incidentes**
- **9- Tecnologías relacionadas con la atención a incidentes**
- **10- Consideraciones Adicionales**

10- Consideraciones Adicionales

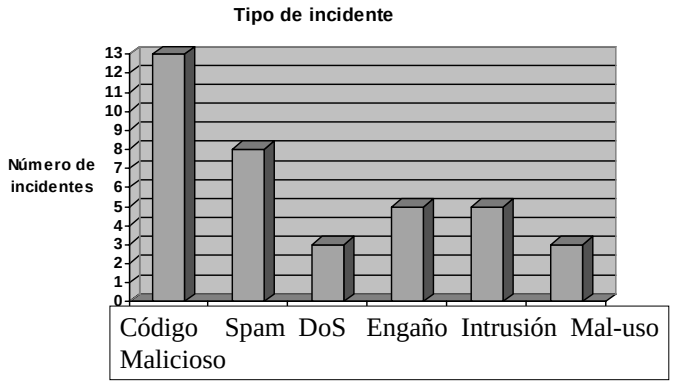
10- Consideraciones Adicionales

Nivel de Madurez de Atención a incidentes, Ciclo de desarrollo



10- Consideraciones Adicionales

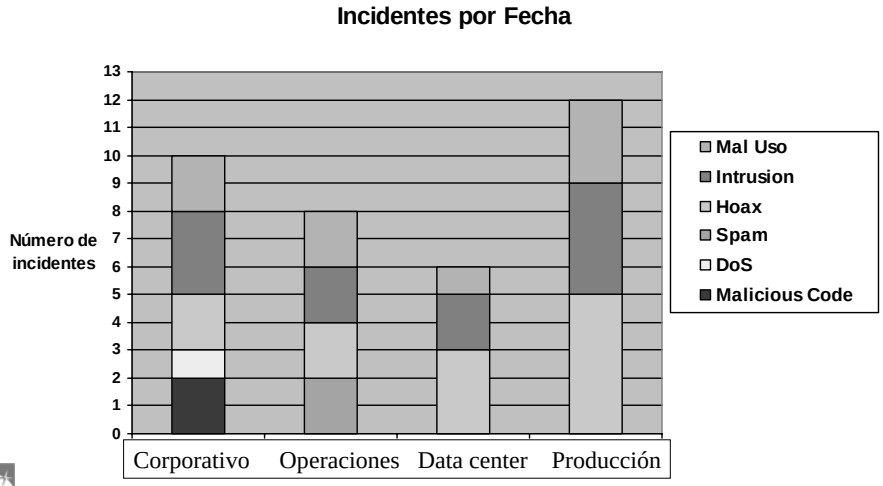
Métricas del Proceso



Información del 1 al 31 de Octubre 2005

10- Consideraciones Adicionales

Métricas del Proceso



Información del 1 al 31 de Octubre 2005

10- Consideraciones Adicionales

Métricas del Proceso

Severidad	Descripción / Incidente	Impacto de Incidente			
		Imagen	Legal	Clientes	Pérdida Financiera
1	Intrusión Servidor xyz	4	1	1	4
2	Gusano en Servidores de Correo Externo	1	1	1	1
2	Denegación Servicio al servidor Web de xxx	4	1	1	1
2	Sitio de Cliente Falsificado	2	1	1	3
3	Spam a lista de correo de xx.cc.cc.xom	2	1	3	1
3	Spam desde xyz	4	3	1	1
4	Virus *Mydoom*	1	1	1	5

Información del 1 al 31 de Octubre 2005

10- Consideraciones Adicionales

Procesos Operativos

Es necesario que las organizaciones refuercen sus procedimientos operativos (día a día) en el sentido de incorporar mejores prácticas en ellos (ITIL, COBIT, BS7799, etc.):

-Respaldos
-Control de accesos y privilegios
-Software malicioso
-Bitácoras
-Capacidad
- Etc.

10- Consideraciones Adicionales

Entrenamiento

Dos tipos de entrenamientos técnicos:

- Casos Generales
- Casos específicos

¡Gracias!

Ricardo Morales González
rmoralesg@alestra.com.mx