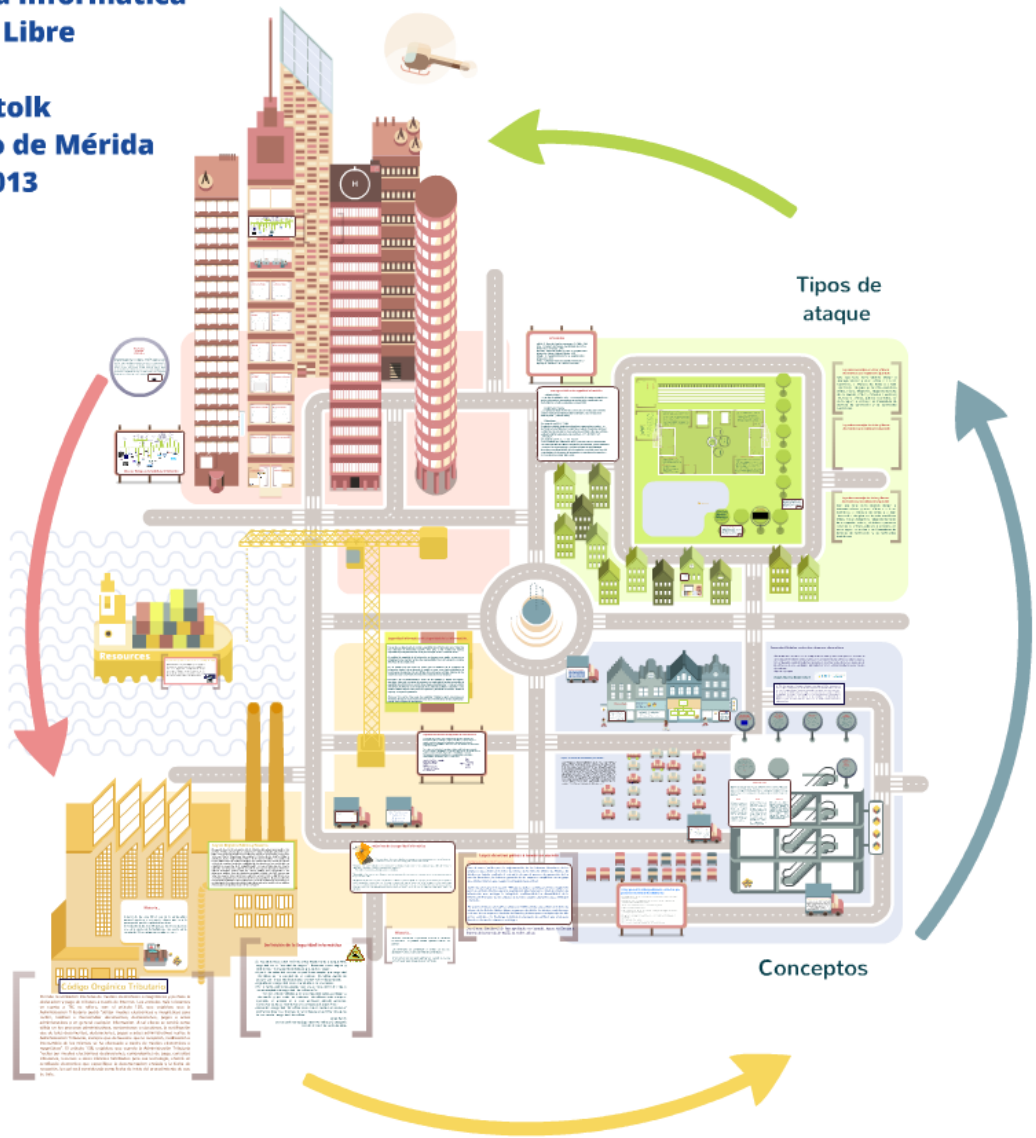
Técnicas de Seguridad Informática con Software Libre

Alejandra Stolk
Parque Tecnológico de Mérida
ESLARED 2013



Técnicas de Seguridad Informática con Software Libre

Alejandra Stolk
Parque Tecnológico de Mérida

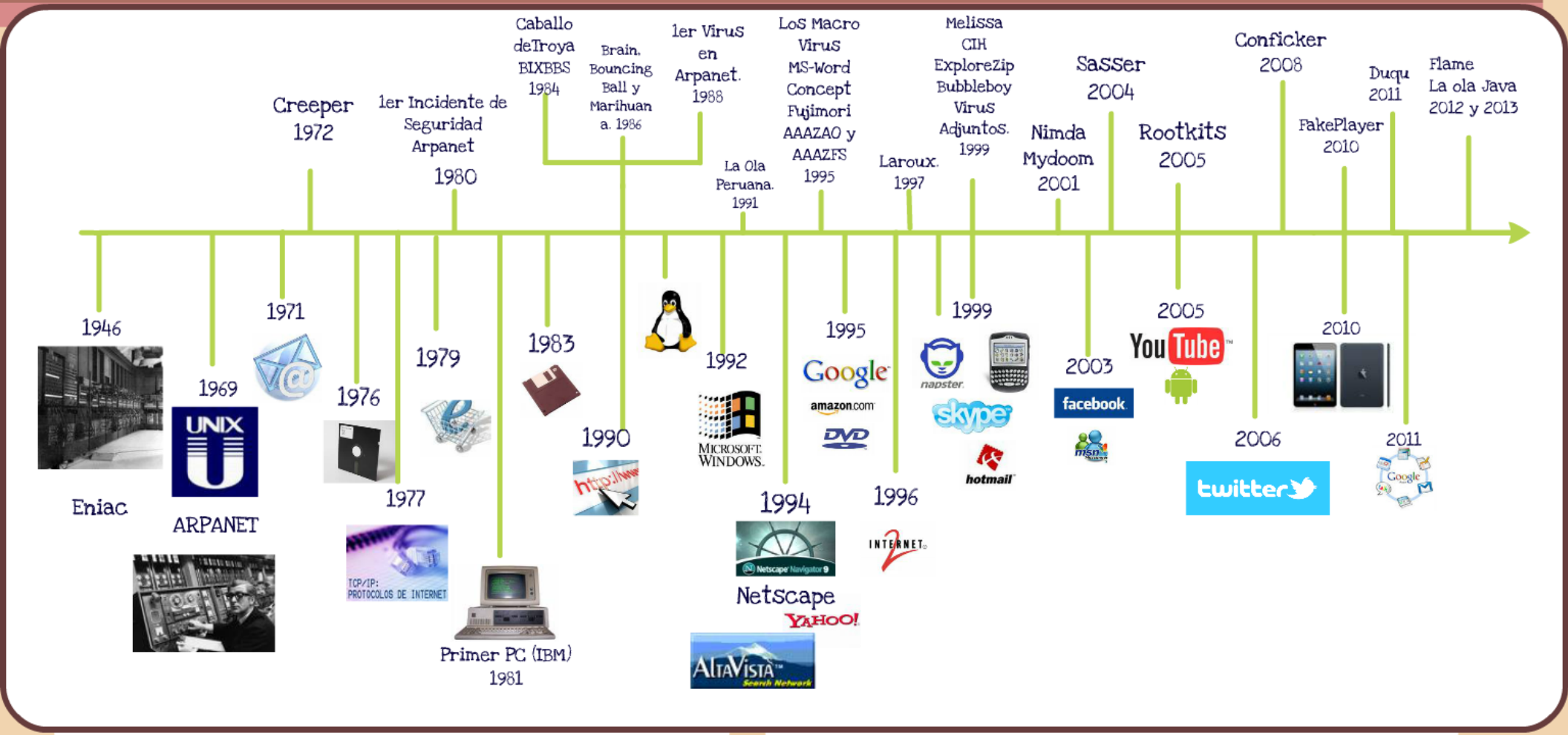
ESLARED 2013

Historia de la Seguridad Informática

Los primeros intentos en seguridad informática pueden ir tan temprano como la época de Julio Cesar y sus famosos mensajes cifrados. Sin embargo, las primeras técnicas de ocultamiento y resguardo de seguridad informática comenzaron durante la segunda guerra mundial con equipos como el enigma. Pero cuando realmente se hizo necesaria fue cuando las computadores se hicieron de propósito general y multiusuario, en ese momento el panorama de la seguridad de la información se tornó complejo.

n se tornó compl

El surgimiento equipos computacionales como el Eniac hizo que se desarrollaran aplicaciones muy diversas pero la más crítica de ellas era un sistema de defensa antimisiles, este sistema continuo desarrollándose y se transformó durante 10 años hasta llegar a un sistema distribuido con más de 50 empleados en 23 centros de operación. Es allí en dónde comienzan toda clase de amenazas de seguridad a la información manejada por diversas personas en un mismo centro de cómputo.



Linea de Tiempo del malware

Linea de Tiempo de la Seguridad Informática

1946 Eniac

1967 ISACA

1969 ARPANET

1971

1976 TCP/IP: PROTOCOLOS DE INTERNET

1977

1979

1981 Primer PC (IBM)

1983 IDS

1984 CFAA

1987 MKS Vir

1988 X.509 AntiVir

1989 Orange Book Users Code of Practice

1990 McAffe Norton

1990

1992 Microsoft Windows

1994 PIX CISSP

1994 Netscape

1995 BS7799

1995 Google amazon.com DVD

1996 Internet

1998 Snort Netfilter

1999 napster skype hotmail

2000 ISO27002

2001 CSIRT ECCouncil Ley Especial contra delitos informáticos

2002 SoX

2003 facebook

2005 ASA ISO 27005

2005 YouTube

2006 twitter

2007 antivirus para móviles

2009 ISO 3100

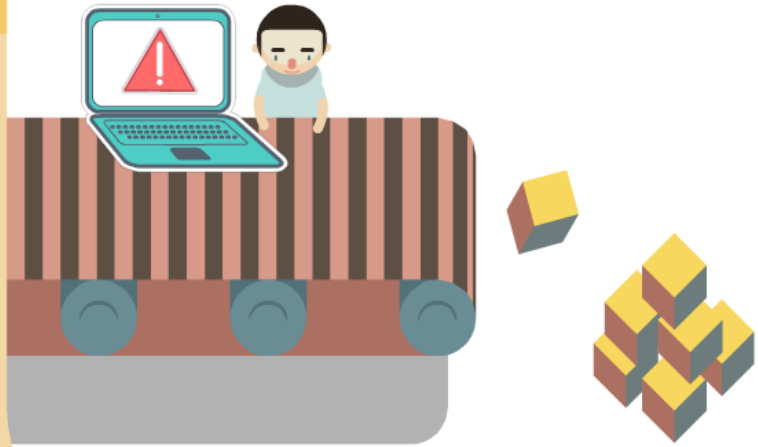
2010

2011 ISO 30300

2011

Historia...

- A partir de los años 80 el uso de la computadora personal comienza a ser común. Asoma por tanto la preocupación por la integridad de los datos.
- En la década de los años 90 aparecen los virus y gusanos y se toma conciencia del peligro que nos acecha como usuarios de PCs y equipos conectados a Internet.



Historia...

- Además, comienzan a proliferar ataques a sistemas informáticos. La palabra hacker aparece incluso en prensa.
- Las amenazas se generalizan a finales de los 90; aparecen nuevos gusanos y malware generalizado.
- En los años 00s los acontecimientos fuerzan a que se tome muy en serio la seguridad informática.

Definición de la Seguridad Informática

- Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es la "cualidad de seguro". Buscamos ahora seguro y obtenemos "libre y exento de todo peligro, daño o riesgo".
- A partir de estas definiciones no podríamos aceptar que seguridad informática es "la cualidad de un sistema informático exento de peligro", por lo que habrá que buscar una definición más apropiada.
- Algo básico: la seguridad no es un producto, sino un proceso.
- Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería:

  "Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico."
- Recuerde: la seguridad informática no es un bien medible, en cambio sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.

Jorge Ramió
Libro Electrónico de Seguridad Informática y Criptografía
Versión 4.1 de 1 de marzo de 2006

Seguridad Informática VS Seguridad de la Información.

Hoy en día se viene dando el cambio a seguridad de la información como traducción más adecuada de information security. Pero peso a ello todavía hay muchos especialistas que siguen llamando así al puro enfoque técnico comentado antes.

En realidad la seguridad de la información es bastante más amplia, ya que no es simplemente una cuestión técnica sino responsabilidad de la alta gerencia y cuadros directivos de una organización.

En tal sentido hay que tener en cuenta que el ambiente de la tecnología de información tiende a estar orientado al servicio y actuar como función habilitante de los procesos de negocios. En esto difiere de los procesos centrales mismos de una organización que constituyen el núcleo de los negocios de una empresa.

De hecho, sin el involucramiento activo de las unidades y líderes de negocio, ejecutivos, directorio y su grupo de asesores, no puede existir un plan sustentable de seguridad de la información, a partir de los riesgos determinados. Y todo esto dentro del sistema de dirección y control propio de un adecuado gobierno corporativo, como define la OECD (Organización para la Cooperación y Desarrollo Económico, OCDE en español) al corporate governance.

Ahora se trata, entre otras cosas, de considerar también la gente, los procesos y funciones de negocio, la protección de todos los activos/recursos de una organización. Donde toda la empresa es la impulsora.

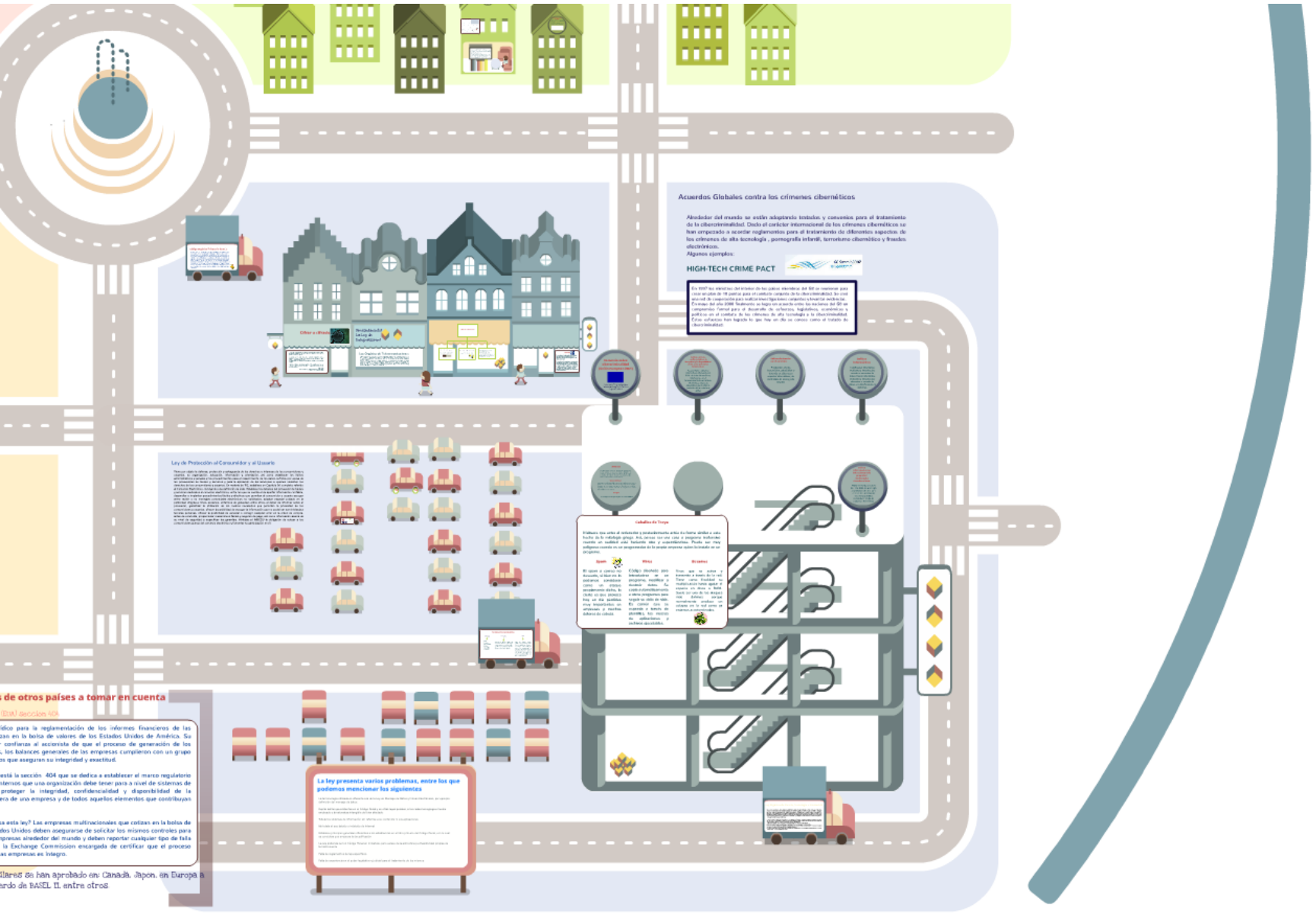
Seguridad Informática VS Seguridad de la Información

La extensión del concepto usual de seguridad informática al de seguridad de la información, implica un corrimiento y visión más amplia de un marco de riesgos de negocios respecto de la perspectiva tradicional de seguridad técnica, basada principalmente en vulnerabilidades. De acuerdo con lo visto anteriormente, tal extensión se da de dos maneras.

Por un lado, en el contexto de la seguridad de la información los riesgos de negocios incluyen no sólo las vulnerabilidades y un aspecto de las amenazas, sino el conjunto de los factores que determinan tales riesgos: activos, vulnerabilidades y amenazas.
Por otra parte, los riesgos de negocios que se consideran incluyen los riesgos organizacionales, operacionales, físicos y de sistemas ICT.

Ausencia de políticas, normas, procedimientos
Ausencia de control de cambios
Educación de usuarios
Conocimiento de la misión de la organización

Virus
Spam
Contraseñas
Ataques Ddos
Exploits
Iptables



Conceptos

Objetivos de la seguridad informática

*Confidencialidad: Los datos sólo deben ser conocidos y accedidos por quienes estén debidamente autorizados durante su almacenamiento, procesamiento o transmisión.

*Integridad: Los datos sólo pueden ser modificados y/o eliminados por quienes estén autorizados para ello y los sistemas y aplicaciones sólo deben ser operados por personal autorizado

Esto incluye: Autenticidad, No repudiación y Contabilidad

*Disponibilidad: Los sistemas que albergan datos e información deben garantizar su acceso, cuando así se requiera, por quienes tengan derecho a ello

*El objetivo del proceso de seguridad informática es obtener un nivel aceptable de seguridad, entendiéndose por aceptable un nivel de protección suficiente para que la mayoría de potenciales intrusos interesados en los equipos de nuestra organización fracasen en cualquier intento de ataque contra los mismos. Asimismo, se encarga de establecer los mecanismos para registrar cualquier evento fuera del comportamiento normal y tomar las medidas necesarias para restablecer las operaciones críticas a la normalidad.

Cifrar o cifrado

Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica o secreta, no será posible descifrarlo o recuperarlo.

No obstante, la RAE define cifrar como "Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar" ... también muy poco técnica .
En algunos países de Latinoamérica, por influencia del inglés, se usa la palabra encriptar.

Si bien se entiende, esta palabra todavía no existe y podría ser el acto de "introducir a alguien dentro de una cripta", ... algo bastante distinto a lo que deseamos expresar...

Jorge Ramió
Libro Electrónico de Seguridad Informática y Criptografía
Versión 4.1 de 1 de marzo de 2006

Próxim
La Ley
Infogor

Ley Or

Según la Paradoja d
nuevas tecnologías.
el sector de las tel
actualmente disfrut
En materia específic
la transferencia tec
propósito de asegu
objetivos, la ley exi
adecuada, a fin de l

Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica o secreta, no será posible descifrarlo o recuperarlo.

No obstante, la RAE define cifrar como "Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar" ... también muy poco técnica .
En algunos países de Latinoamérica, por influencia del inglés, se usa la palabra encriptar.

Si bien se entiende, esta palabra todavía no existe y podría ser el acto de "introducir a alguien dentro de una cripta", ... algo bastante distinto a lo que deseamos expresar...

Jorge Ramió
Libro Electrónico de Seguridad Informática y Criptografía
Versión 4.1 de 1 de marzo de 2006

No Repudio

Este término se ha introducido en los últimos años como una característica más de los elementos que conforman la seguridad en un sistema informático.

Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales de autenticación. Se habla entonces de No Repudio de Origen y No Repudio de Destino, forzando a que se cumplan todas las operaciones por ambas partes en una comunicación.

¿Qué es la información?

Desde el punto de vista de la ingeniería

Estudio de las características y estadísticas del lenguaje que nos permitirá su análisis desde un enfoque matemático, científico y técnico.

Desde el punto de vista de las empresas

Conjunto de datos propios que se gestionan y mensajes que se intercambian personas y/o máquinas dentro de una organización.

En las empresas se entenderá como:

- Todo el conjunto de datos y ficheros de la empresa.
- Todos los mensajes intercambiados.
- Todo el historial de clientes y proveedores.
- Todo el historial de productos.
- En definitiva, el know-how de la organización.

Si esta información se pierde o deteriora, le será muy difícil a la empresa recuperarse y seguir siendo competitiva. Por este motivo, es vital que se implanten unas políticas de seguridad y que, además, se haga un seguimiento de ellas.

Amenaza

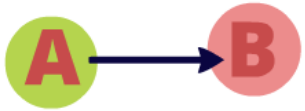
Cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. Ejemplos de amenazas son los ataques humanos, los desastres naturales, los errores humanos inadvertidos, fallas internas del hardware o el software, etc.

Vulnerabilidad

Consistirá en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.

Ataque

Es cualquier acción que explota una vulnerabilidad.

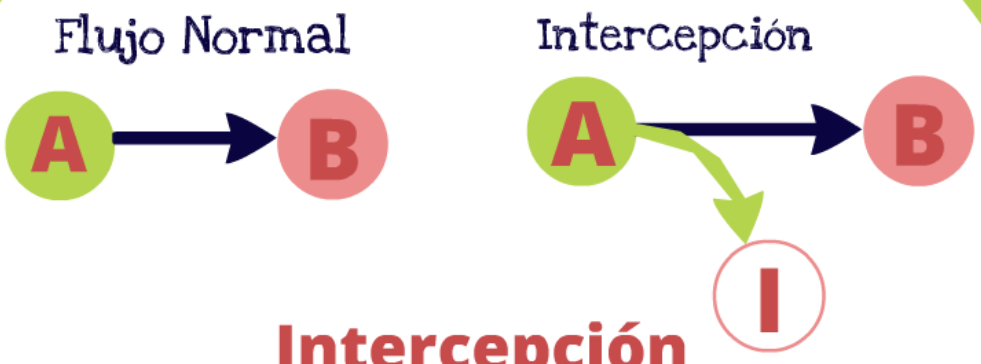


Flujo Normal

Interrupción

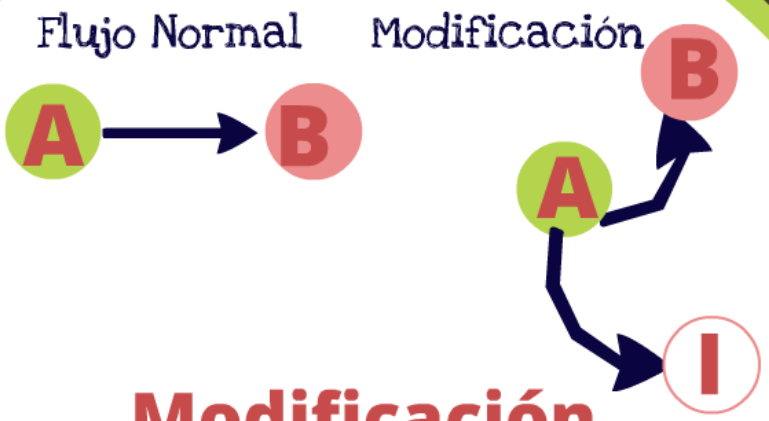
Interrupción

En el caso de una interrupción un activo del sistema se pierde, se hace no disponible o inutilizable. Un ejemplo de ello puede ser la destrucción maliciosa de un dispositivo de hardware o el borrado de un programa o archivo.



Intercepción

En el caso de una intercepción implica que alguien logre acceso no autorizado a un activo del sistema. Esta parte no autorizada puede ser una persona, programa, dispositivo, etc. Un ejemplo de ella puede ser el copiado de datos, la intervención de un canal de red.



Modificación

En el caso de que se realiza una intercepción y la parte no autorizada logra acceso a un activo del sistema y tiene la capacidad de manipularlo se trata de una amenaza por modificación.

Fabricación

La parte no autorizada que accede al sistema también puede crear objetos falsos en un sistema. Ejemplo de ello son la inserción de transacciones en un sistema o BD, fabricación de paquetes de datos, etc.

Algunos ejemplos...

Caballos de Troya

Malware que entra al ordenador y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa.

Spam

El spam o correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y muchos dolores de cabeza.

Virus

Código diseñado para introducirse en un programa, modificar o destruir datos. Se copia automáticamente a otros programas para seguir su ciclo de vida. Es común que se expanda a través de plantillas, las macros de aplicaciones y archivos ejecutables.

Gusanos

Virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red como ya estamos acostumbrados.

Amenazas más características...

Hardware

Agua
Fuego
Electricidad
Polvo
Cigarrillos
Comida.

Software

Además de algunos típicos del hardware, borrados accidentales o intencionados, estática, fallos de líneas de programa, bombas lógicas, robo, copias ilegales.

Datos

Tiene los mismos puntos débiles que el software. Pero hay dos problemas añadidos: no tienen valor intrínseco pero sí su interpretación y, por otra parte, habrá datos de carácter personal y privado que podrían convertirse en datos de carácter público: hay leyes que lo protegen.

Conceptos Básicos de Seguridad Informática

- Evidencia digital

Es un tipo de evidencia física. Esta construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.(Casey 2000)

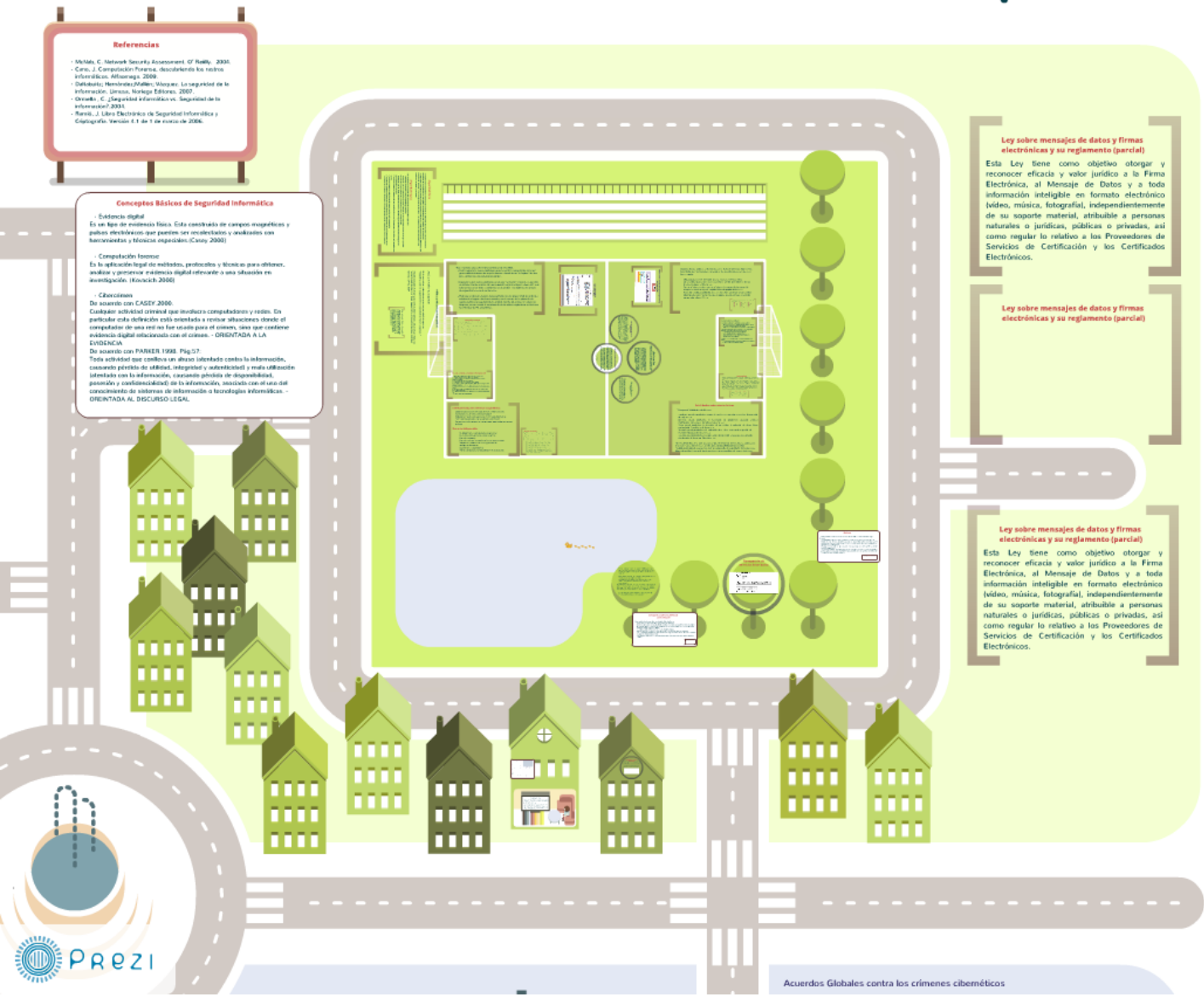
- Computación forense

Es la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar evidencia digital relevante a una situación en investigación. (Kovacich 2000)

- Cibercrimen

De acuerdo con CASEY.2000.
Cualquier actividad criminal que involucra computadores y redes. En particular esta definición está orientada a revisar situaciones donde el computador de una red no fue usado para el crimen, sino que contiene evidencia digital relacionada con el crimen. - ORIENTADA A LA EVIDENCIA
De acuerdo con PARKER.1998. Pág.57:
Toda actividad que conlleva un abuso (atentado contra la información, causando pérdida de utilidad, integridad y autenticidad) y mala utilización (atentado con la información, causando pérdida de disponibilidad, posesión y confidencialidad) de la información, asociada con el uso del conocimiento de sistemas de información o tecnologías informáticas. - OREINTADA AL DISCURSO LEGAL

Tipos de ataque



Denegación de servicio

Podríamos definir los ataques DOS (Denegation Of Service) como la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.

Existen tres tipos básicos de denegación de servicio:

- Consumo de recursos: El atacante intenta consumir los recursos del servidor hasta agotarlos: ancho de banda, tiempo de cpu, memoria, disco duro...
- Destrucción o alteración de la configuración: Se intenta modificar la información de la máquina. Este tipo de ataques necesitan de técnicas más sofisticadas.
- Destrucción o alteración física de los equipos: Se intenta denegar el servicio destruyendo físicamente el servidor o algunos de sus componentes, cortando el cable de conexión, o el cable de la red eléctrica.

Los sistemas de DOS más utilizados:

Mail Bombing: El primer sistema de denegación de servicio fue el denominado mail bombing, consistente en el envío masivo de mensajes a una máquina hasta saturar el servicio.

Smurfing: Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de ping. Esta trama lleva como dirección de origen la dirección IP de la víctima (usando IP Spoofing) y como dirección de destino la dirección broadcast de la red atacada. De esta forma todos los equipos de la red contestan a la víctima de tal modo que pueden llegar a saturar su ancho de banda.

SYN Flood: El sistema atacante utiliza una IP inexistente y envia multitud de tramas SYN de sincronización a la víctima. Como la víctima no puede contestar al peticionario (porque su IP es inexistente) las peticiones llenan la cola de tal manera que las solicitudes reales no puedan ser atendidas.

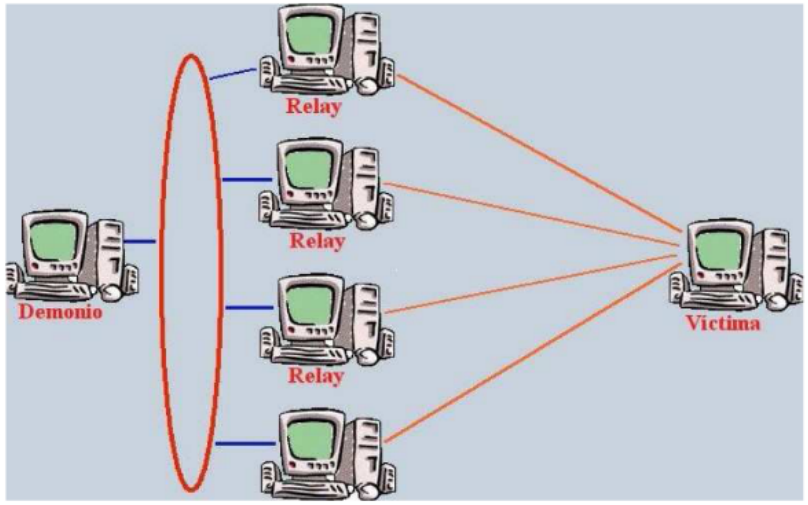


Fig. 1 Smurfing

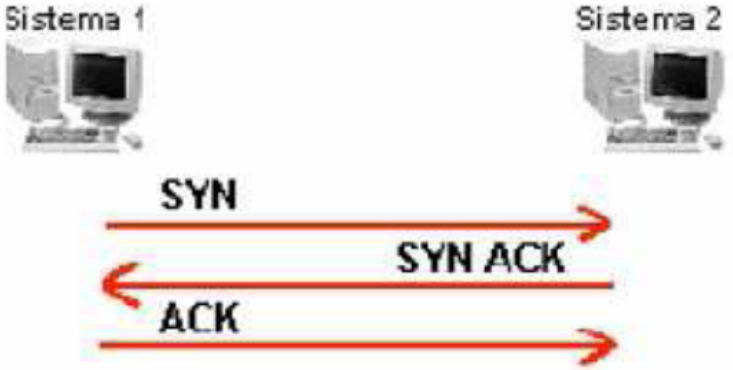
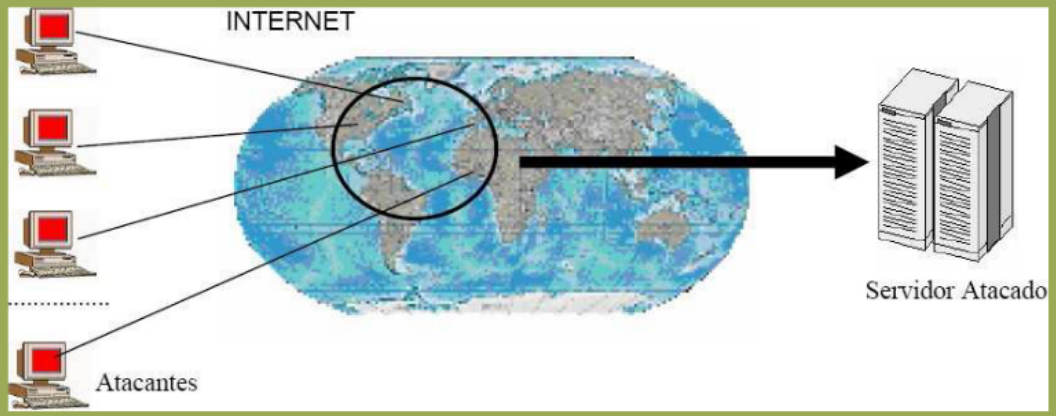


Fig. 2 Syn Flood

Denegación de Servicios Distribuida

Podemos definir el ataque DDOS como un ataque de denegación de servicio (DOS) dónde existen múltiples focos distribuidos y sincronizados que focalizan su ataque en un mismo destino.

Es decir, el ataque DDOS es una ampliación del concepto DOS sumándole la capacidad de acceso simultáneo y desde cualquier punto del mundo que ofrece Internet.



Existen diferentes tipos de ataques DDOS pero todos tienen en común un gran consumo de ancho de banda. Aquí está el gran peligro de este tipo de ataques que tienen dos vertientes:

- Denegación del servicio: Es su objetivo principal, hacer que un sistema no pueda cumplir su cometido.
- Saturación de la red: Debido a que los paquetes de estos ataques comparten las mismas rutas que el resto de comunicaciones.

El crecimiento del número de nodos conectados y la mejora del ancho de banda hacen que existan cada vez más atacantes potenciales. Se puede dar el caso de cientos de atacantes coordinados pero este fenómeno no se da en la realidad:

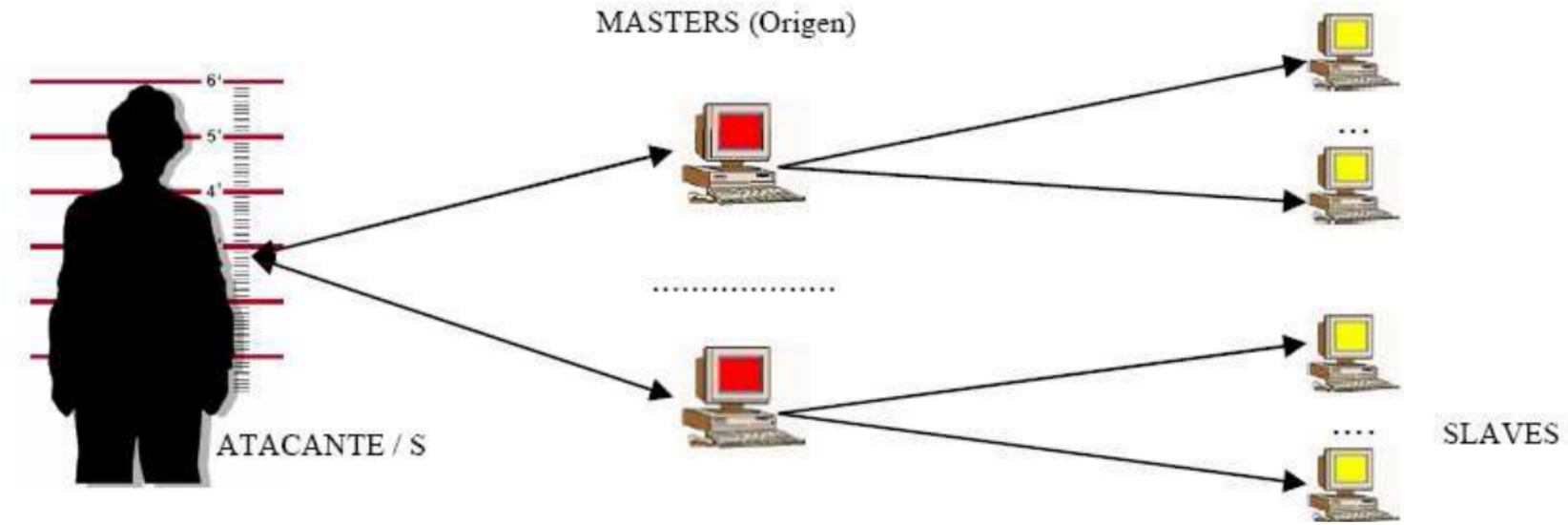
- Es muy arriesgado para un atacante usar su propio equipo.
- Es muy difícil coordinar a muchos atacantes.

Denegación de Servicios distribuida
¿Cómo lo hacen?

Uno o varios hackers buscan sistemas vulnerables. Esto es fácil ya que:

- Cada vez hay más nodos conectados permanentemente a internet.
- Muchos equipos carecen de las actualizaciones críticas de sus sistemas operativos o éstos son antiguos.
- El desconocimiento de muchos de los usuarios hace que no sean conscientes de que sus equipos están infectados por algún programa malicioso.
- Se realiza un ataque sobre esos nodos y se les instala el programa.
- Estos son los nodos "masters", es decir, los que tienen una conexión directa con el atacante.
- A su vez el programa instalado en estos nodos busca un segundo nivel de nodos ("slaves") que serán los encargados de realizar el ataque final.
- Los atacantes dan la orden de manera sincronizada para que todos los nodos slave ataquen al sistema "victima".

La gran ventaja de este sistema es que permite mantener el anonimato de los atacantes ya que analizan el trafico de los nodos slave y cuando detectan que están siendo analizados cierran la conexión, posteriormente limpian cualquier prueba en el master y finalmente cierran su conexión con el master.



Denegación de Servicios Distribuida

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

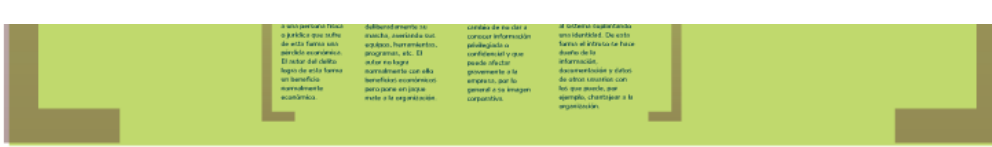
Total incidents reported (1988-2003): **319,992**

MyDoom

- El virus MyDoom ha sido uno de los más extendidos (1 millón de máquinas afectadas según F-Secure).
- Su propagación ha sido una de las más rápidas, en 4 segundos ya era una verdadera epidemia.
- Inicialmente este virus fue concebido para hacer un ataque DDoS sobre el servidor de SCO (www.sco.com), aunque existen teorías de que su verdadera intención era la recopilación de direcciones de e-mail para Spam.
- El ataque tuvo la SCO en jaque durante 1 semana hasta que SCO cambió su dominio (www.thescogroup.com).
- Su predecesor MyDoom.B no llegó a tener el mismo impacto ya sea por su menor propagación o por la capacidad de respuesta de su objetivo (www.microsoft.com), que cambió sus servidores solo 2 segundos después del inicio del ataque.

Blaster y Sasser

- Blaster ha sido uno de los últimos virus con gran expansión por la red.
- Su objetivo era un DDoS sobre los servidores de Microsoft. Especialmente contra el sitio www.windowsupdate.com
- Su infección se producía por una vulnerabilidad de Windows.
- Aunque el número de ordenadores infectados resulto ser bastante grande 1,2 millones, no provocó grandes problemas.
- El virus Sasser que, al igual que Blaster, aprovecha las vulnerabilidades de Windows para su distribución por la red. Sus consecuencias fueron menores que las de Blaster.



Debilidades más características

Triángulo de Debilidades del Sistema:

- Hardware: pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas, etc.
- Software: puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas al sistema, etc.
- Datos: puede producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.
- Memoria: puede producirse la introducción de un virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
- Usuarios: puede producirse la suplantación de identidad, el acceso no autorizado, visualización de datos confidenciales, etc.

*Es muy difícil diseñar un plan que contemple minimizar de forma eficiente todas estas amenazas, y que además se entienda y pase desapercibido por los usuarios.
*Debido al principio de acceso más fácil, el responsable de seguridad informática no se deberá descuidar ninguno de los cinco elementos susceptibles de ataque al sistema.

Delitos Informáticos

Cualquier comportamiento criminológico en el cual la computadora ha estado involucrada como material o como objeto de la acción criminal o como mero símbolo. (Carlos Sarzana, Mx)

Se conceptualiza en forma típica y atípica, entendiendo la primera como las conductas típicas, antijurídicas y culpables en que se tienen las computadoras como instrumento o fin, y por la segunda actitudes ilícitas en que se tienen a las computadoras como instrumento o fin. (Julio Tellez Valdés, Mx)

Toda acción dolosa que cause un perjuicio a personas naturales o jurídicas que puede producir o no un beneficio material para su autor, pudiendo o no perjudicar de manera directa o indirecta a la víctima, caracterizando dicha acción dolosa por la utilización de actividades o medios informáticos. (Orlando Solano B. Col.)

Fraude

Acto deliberado de manipulación de datos perjudicando a una persona física o jurídica que sufre de esta forma una pérdida económica. El autor del delito logra de esta forma un beneficio normalmente económico.

Sabotaje

Acción con la que se desea perjudicar a una empresa entorpeciendo deliberadamente su marcha, averiando sus equipos, herramientas, programas, etc. El autor no logra normalmente con ello beneficios económicos pero pone en jaque mate a la organización.

Chantaje

Acción que consiste en exigir una cantidad de dinero a cambio de no dar a conocer información privilegiada o confidencial y que puede afectar gravemente a la empresa, por lo general a su imagen corporativa.

Mascarada

Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad. De esta forma el intruso se hace dueño de la información, documentación y datos de otros usuarios con los que puede, por ejemplo, chantajear a la organización.

a la víctima, caracterizando dicha acción dolos
os informáticos. (Orlando Solano B. Col.)

Fraude

Acto deliberado de manipulación de datos perjudicando a una persona física o jurídica que sufre de esta forma una pérdida económica. El autor del delito logra de esta forma un beneficio normalmente económico.

Sabotaje

Acción con la que se desea perjudicar a una empresa entorpeciendo deliberadamente su marcha, averiando sus equipos, herramientas, programas, etc. El autor no logra normalmente con ello beneficios económicos pero pone en jaque mate a la organización.

Chantaje

Acción que consiste en exigir una cantidad de dinero a cambio de no dar a conocer información privilegiada o confidencial y que puede afectar gravemente a la empresa, por lo general a su imagen corporativa.

Mascarada

Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad. De esta forma el intruso se hace dueño de la información, documentación y datos de otros usuarios con los que puede, por ejemplo, chantajear a la organización.

Elementos Comunes a las definiciones

Revisando las definiciones se identifican elementos comunes:

- Sujeto actor o actores de la conducta dañosa que produce el hecho
- No es clara en todas las definiciones presentadas
- Algunas veces se deja por fuera de la definición o se asume implícita

Un medio adecuado para cometer el acto ilícito, o sea el dispositivo informático por medio del cual se lleva a cabo la acción.

- Se encuentra referenciado en todas las definiciones
- Se hace particular énfasis a medios informáticos
- En pocas definiciones se hace claridad sobre el lugar de la evidencias, dado el medio utilizado.

Un objeto, o sea, el bien que produce el beneficio ilícito para el o los autores

- Se consideran generalmente los objetos resultado de procesamiento de datos, los datos, la información resultado.

- Suponiendo que todos entendemos qué es un delito informático, algo no muy banal dado que muchos países no se ponen de acuerdo, parece ser que es un buen negocio:
  - Objeto pequeño: la información que se ataca está almacenada en contenedores pequeños: no es necesario un camión para robar un banco, llevarse las joyas, el dinero, etc.
  - Contacto físico: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del propio delincuente.
  - Alto valor: el objeto codiciado tiene un alto valor. Los datos (el contenido a robar) puede valer mucho más que el soporte que los almacena: servidor, computador, disco, CD, etc.

los almacena: servidor,

Son acciones que vulneran la confidencialidad, integridad y disponibilidad de la información.

Ataques a un sistema informático:

- Fraude
- Sabotaje
- Revelación
- Gusanos
- Malversación
- Espionaje
- Mascarada
- C. de Troya
- Robo
- Chantaje
- Virus
- Spam

Tres amenazas que se han incrementado en el año 2005:

- Cartas nigerianas: correo electrónico que comenta la necesidad de sacar una gran cantidad de dinero de un país africano a través de un "cómplice" de otro país, justificando una persecución política.

- Ingeniería social: correo electrónico en el que "se fuerza" al usuario a que abra un archivo adjunto, enlace, etc. que supuestamente le interesa o bien está muy relacionado con su trabajo, utilizando así el eslabón más débil de una cadena de seguridad como es el ser humano.

- Phishing: simulación, algunas veces perfecta, de una página Web de un banco solicitando el ingreso de claves secretas, con la excusa de la aplicación de nuevas políticas de seguridad de la entidad. Dentro del enlace a la noticia de Hispasec, se recomienda la visualización de los vídeos explicativos en flash con los altavoces del PC encendidos.

Administración de la Seguridad

La gerencia de la seguridad de la información involucra el control y verificación de procesos no sólo en el área de las TIC. Por ello se habla de varios niveles de gobierno:

Gobierno de las tecnologías de la información:

Leyes y acuerdos relativos a la seguridad de la información

En Venezuela

Artículos 108 y 110 de la Constitución Nacional:
Nuestra carta magna reconoce el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional, igualmente establece que el Estado garantizará servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información. Los centros educativos deben incorporar el conocimiento y aplicación de las nuevas tecnologías, de sus innovaciones, según los requisitos que establezca la ley.

Ley Especial Contra Delitos Informáticos

Crea el marco jurídico para el tratamiento de los crímenes informáticos. Se contemplan 4 tipos de delitos:

- Contra los sistemas que utilizan tecnologías de información
- Contra la Propiedad
- Contra la privacidad de las personas y de las comunicaciones
- Contra las niñas, niños y adolescentes
- Contra el orden económico

Ley sobre mensajes de datos y firmas electrónicas y su reglamento (parcial)

Esta Ley tiene como objetivo otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico (vídeo, música, fotografía), independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

La ley presenta varios problemas, entre los que podemos mencionar los siguientes

La terminología utilizada es diferente a la de la Ley de Mensaje de Datos y Firmas Electrónicas, por ejemplo: definición del mensaje de datos

Repite delitos ya existentes en el Código Penal y en otras leyes penales, a los cuales les agrega el medio empleado y la naturaleza intangible del bien afectado

Tutela los sistemas de información sin referirse a su contenido ni sus aplicaciones

No tutela el uso debido o indebido de Internet

Establece principios generales diferentes a los establecidos en el libro primero del Código Penal, con lo cual se considera que empeora la decodificación

La Ley pretende ser un Código Penal en miniatura, pero carece de la estructura y exhaustividad propias de tal instrumento

Falta de reglamentos de ley específicos

Falta de experiencia en el poder legislativo y judicial para el tratamiento de los mismos

Ley Orgánica de Ciencia, Tecnología e Innovación

Este Decreto-Ley tiene por objeto desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para la generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional. En materia específica de Tecnologías de Información y Comunicación

Se puede resaltar lo establecido en el artículo 22: "El Ministerio de Ciencia y Tecnología coordinará las actividades del Estado que, en el área de tecnologías de información, fueren programadas, asumirá competencias que en materia de informática, ejercía la Oficina Central de Estadística e Informática, así como las siguientes:
Actuar como organismo rector del Ejecutivo Nacional en materia de tecnologías de información.
Establecer políticas en torno a la generación de contenidos en la red, de los órganos y entes del Estado.
Establecer políticas orientadas a resguardar la inviolabilidad del carácter privado y confidencial de los datos electrónicos obtenidos en el ejercicio de las funciones de los organismos públicos.
Fomentar y desarrollar acciones conducentes a la adaptación y asimilación de las tecnologías de información por la sociedad.
Artículos 108 y 110 de la Constitución Nacional

Ley de Protección al Consumidor y al Usuario

Tiene por objeto la defensa, protección y salvaguarda de los derechos e intereses de los consumidores y usuarios, su organización, educación, información y orientación, así como establecer los ilícitos administrativos y penales y los procedimientos para el resarcimiento de los daños sufridos por causa de los proveedores de bienes y servicios y para la aplicación de las sanciones a quienes violenten los derechos de los consumidores y usuarios. En materia de TIC, establece un Capitulo (V) completo referido al Comercio Electrónico, incluyendo una definición de éste. Establece los deberes del proveedor de bienes y servicios dedicados al comercio electrónico, entre los que se cuenta el de aportar información confiable, desarrollar e implantar procedimientos fáciles y efectivos que permitan al consumidor o usuario escoger entre recibir o no mensajes comerciales electrónicos no solicitados, adoptar especial cuidado en la publicidad dirigida a niños, ancianos, enfermos de gravedad, entre otros, el deber de informar sobre el proveedor, garantizar la utilización de los medios necesarios que permitan la privacidad de los consumidores y usuarios, ofrecer la posibilidad de escoger la información que no podrá ser suministrada a terceras personas, ofrecer la posibilidad de cancelar o corregir cualquier error en la orden de compra, antes de concluirla, proporcionar mecanismos fáciles y seguros de pago, así como información acerca de su nivel de seguridad y especificar las garantías. Atribuye al INDECU la obligación de educar a los consumidores acerca del comercio electrónico y fomentar su participación en él.

Ley de Registro Público y Notario

El propósito de este Decreto-Ley ha sido la adaptación del ordenamiento jurídico a los cambios actuales, entre los que se encuentran la nuevas tecnologías informáticas para llegar a una automatización del sistema registral y notarial, así como unificar en un mismo texto normativo las disposiciones que regulen la actuación de los Registros Civiles y Subalternos, de los Registros Mercantiles y de las Notarías Públicas. Se considera de interés público el uso de medios tecnológicos en la función registral y notarial para que los trámites de recepción, inscripción y publicidad de los documentos sean practicados con celeridad, sin menoscabo de la seguridad jurídica. La Ley establece que los asientos registrales y la información registral emanada de los soportes electrónicos del sistema registral venezolano surtirán todos los efectos jurídicos que corresponden a los documentos públicos. Entre los principales postulados referidos a las TIC, tenemos que todos los soportes físicos del sistema registral y notarial actual se digitalizarán y se transferirán progresivamente a las bases de datos correspondientes. El proceso registral y notarial podrá ser llevado a cabo íntegramente a partir de un documento electrónico y se establece que la firma electrónica de los Registradores y Notarios tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa.

Código Orgánico Tributario

Permite la utilización intensiva de medios electrónicos o magnéticos y permite la declaración y pago de tributos a través de Internet. Los artículos más relevantes en cuanto a TIC se refiere, son: el artículo 125, que establece que la Administración Tributaria podrá "utilizar medios electrónicos o magnéticos para recibir, notificar e intercambiar documentos, declaraciones, pagos o actos administrativos y en general cualquier información. A tal efecto se tendrá como válida en los procesos administrativos, contenciosos o ejecutivos, la certificación que de tales documentos, declaraciones, pagos o actos administrativos realice la Administración Tributaria, siempre que demuestre que la recepción, notificación o intercambio de los mismos se ha efectuado a través de medios electrónicos o magnéticos". El artículo 138, establece que cuando la Administración Tributaria "reciba por medios electrónicos declaraciones, comprobantes de pago, consultas tributarias, recursos u otros trámites habilitados para esa tecnología, emitirá un certificado electrónico que especifique la documentación enviada y la fecha de recepción, la cual será considerada como fecha de inicio del procedimiento de que se trate.

Código Orgánico Tributario (cont.)

En todo caso, se prescindirá de la firma autógrafa del contribuyente o responsable () La Administración Tributaria establecerá los medios y procedimientos de autenticación electrónica de los contribuyentes o responsables" El artículo 162, numeral 3 del Código Orgánico Tributario, que establece: "Las notificaciones se practicarán, sin orden de prelación, en alguna de estas formas () 3. Por correspondencia postal efectuada mediante correo público o privado, por sistemas de comunicación telegráficos, facsimilares, electrónicos y similares siempre que se deje constancia en el expediente de su recepción. Cuando la notificación se realice mediante sistemas facsimilares o electrónicos, la Administración Tributaria convendrá con el contribuyente o responsable la definición del domicilio facsimilar o electrónico".

Ley Orgánica de Telecomunicaciones

Según la Paradoja de Hayles y sus "Capas de Desarrollo" (1.999) Sin infraestructuras previas, en definitiva, no hay acceso a las nuevas tecnologías. De aquí la importancia capital de este instrumento normativo que estableció la apertura y competencia en el sector de las telecomunicaciones en nuestro país y sentó las bases del desarrollo e inversión en la infraestructura que actualmente disfrutamos.

En materia específica de TIC podemos destacar algunos postulados de esta Ley; la promoción a la investigación, el desarrollo y la transferencia tecnológica en materia de telecomunicaciones y la utilización de nuevos servicios, redes y tecnologías con el propósito de asegurar el acceso en condiciones de igualdad a todas las personas. Para garantizar el cumplimento de sus objetivos, la ley exige a los distintos operadores la homologación y certificación de equipos, así como el uso de la tecnología adecuada, a fin de lograr el acceso universal a la comunicación.

Próximamente!

La Ley de Infogorbierno!

Acuerdos Globales contra los crímenes cibernéticos

Alrededor del mundo se están adoptando tratados y convenios para el tratamiento de la cibercriminalidad. Dado el carácter internacional de los crímenes cibernéticos se han empezado a acordar reglamentos para el tratamiento de diferentes aspectos de los crímenes de alta tecnología , pornografía infantil, terrorismo cibernético y fraudes electrónicos.
Algunos ejemplos:

HIGH-TECH CRIME PACT

En 1997 los ministros del interior de los países miembros del G8 se reunieron para crear un plan de 10 puntos para el combate conjunto de la cibercriminalidad. Se creó una red de cooperación para realizar investigaciones conjuntos y levantar evidencias.
En mayo del año 2000 finalmente se logra un acuerdo entre las naciones del G8 un compromiso formal para el desarrollo de esfuerzos, legislativos, económicos y políticos en el combate de los crímenes de alta tecnología y la cibercriminalidad. Estos esfuerzos han logrado lo que hoy en día se conoce como el tratado de cibercriminalidad.

Convenio sobre cibercriminalidad (Unión european 2001)

Define un criterio comun sobre: Infracciones contra delitos de la tecnología informática

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

Acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos, interferencia en el funcionamiento de un sistema informático, abuso de dispositivos que faciliten la comisión de los anteriores delitos

Delitos relacionados con el contenido

Producción, oferta, transmisión, adquisición o tenencia en sistemas o soportes informáticos, de contenidos de pornografía infantil.

Delitos informáticos

Falsificación informática mediante la introducción, borrado o supresión de datos, fraude informático mediante la introducción, alteración o borrado de datos, o la interferencia en sistemas.

los crímenes de alta tecnología , pornografía infantil, terrorismo ciber
electrónicos.
Algunos ejemplos:

HIGH-TECH CRIME PACT

En 1997 los ministros del interior de los países miembros del G8 se reunieron para crear un plan de 10 puntos para el combate conjunto de la cibercriminalidad. Se creó una red de cooperación para realizar investigaciones conjuntos y levantar evidencias.
En mayo del año 2000 finalmente se logra un acuerdo entre las naciones del G8 un compromiso formal para el desarrollo de esfuerzos, legislativos, económicos y políticos en el combate de los crímenes de alta tecnología y la cibercriminalidad. Estos esfuerzos han logrado lo que hoy en día se conoce como el tratado de cibercriminalidad.

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

Acceso ilícito a sistemas
cos, interceptación
datos informáticos,

Delitos relacionados con el contenido

Producción, oferta, transmisión, adquisición o tenencia en sistemas o soportes informáticos, de

**Delit
informá**

Falsificación i
mediante la in
borrado o sup
datos, fraude i

Convenio sobre cibercriminalidad (Unión european 2001)

Define un criterio común Sobre: Infracciones contra delitos de la siguiente índole:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

Acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos, interferencia en el funcionamiento de un sistema informático, abuso de dispositivos que faciliten la comisión de los anteriores delitos

Delitos relacionados con el contenido

Producción, oferta, transmisión, adquisición o tenencia en sistemas o soportes informáticos, de contenidos de pornografía infantil.

Delitos informáticos

Falsificación informática mediante la introducción, borrado o supresión de datos, fraude informático mediante la introducción, alteración o borrado de datos, o la interferencia en sistemas.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Posteriormente, en enero del año 2003, se promulgó un protocolo adicional para criminalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos

Leyes de otros países a tomar en cuenta

Sarbanes-Oxley (EUA) Sección 404

Crea el marco jurídico para la reglamentación de los informes financieros de las empresas que cotizan en la bolsa de valores de los Estados Unidos de América. Su objetivo es brindar confianza al accionista de que el proceso de generación de los estados financieros, los balances generales de las empresas cumplieron con un grupo de controles internos que aseguran su integridad y exactitud.

Dentro de esta ley está la sección 404 que se dedica a establecer el marco regulatorio para los controles internos que una organización debe tener para a nivel de sistemas de información para proteger la integridad, confidencialidad y disponibilidad de la información financiera de una empresa y de todos aquellos elementos que contribuyan a formarla.

Por qué nos interesa esta ley? Las empresas multinacionales que cotizan en la bolsa de valores de los Estados Unidos deben asegurarse de solicitar los mismos controles para cada una de sus empresas alrededor del mundo y deben reportar cualquier tipo de falla en los controles a la Exchange Commission encargada de certificar que el proceso llevado a cabo por las empresas es íntegro.

Leyes muy similares se han aprobado en: Canadá, Japón, en Europa a través del acuerdo de BASEL II, entre otros.

Administración de la Seguridad

La gerencia de la seguridad de la información involucra el control y verificación de procesos no sólo en el área de las TIC. Por ello se habla de varios niveles de gobierno:

Gobierno de las tecnologías de la información:

Es el sistema: normas, procedimientos, organización, infraestructura que gestiona y controla todas las tecnologías de la información de una organización

Gobierno de la empresa:

Es el sistema: normas, procedimientos, métodos, organización, procesos que dirige y controla una organización.

Gobierno de las tecnologías de la información es parte del gobierno de la empresa:

Información y conocimiento generado por uno o más sistemas de información que influyen en la dirección de una empresa e impactan en la actividad del negocio

Errores comunes cometidos a nivel gerencial

1. Suponer que los problemas desaparecerán si no se les hace caso
2. Autorizar soluciones reactivas o parches de corto plazo
3. No entender cuánto vale la información y qué tanto depende de ella la reputación corporativa
4. Depender principalmente de un cortafuegos
5. No lidiar con los aspectos operacionales de la seguridad
6. Hacer parches y no dar seguimiento para asegurarse que de los riesgos se han mitigado eficazmente
7. No entender la relación entre la seguridad y los problemas de funcionamiento de negocio
8. Entender los riesgos de la seguridad física pero no las consecuencias de una pobre seguridad informática
9. Designar personal a mantener la seguridad sin tener la capacidad apropiada para ello
10. Sentirse seguros al pasar una auditoria

A nivel gerencial, cómo enfrentar esos problemas

- Ubicar la seguridad informática al mismo nivel que otras actividades sustantivas de la organización
- Elaborar la misión de la seguridad informática claramente
- Promulgar las políticas que se derivan de la misión
- Determinar qué mecanismos se requieren para implementar esas políticas.

Elementos indispensables

- Establecimiento de la política de seguridad
- Auditoria de la seguridad de los sistemas
- Gestión de acceso
- Gestión de la configuración de los sistemas y redes
- Respaldos y acervos de datos y programas
- Manejo de incidentes
- Escalamiento de problemas
- Planes de respuesta y recuperación ante desastres

Arquitectura de Seguridad

La arquitectura de seguridad se refiere a los conceptos, principios, estructuras y estándares usados para diseñar, implementar, monitorizar y asegurar los sistemas operativos, los equipos, las redes y las aplicaciones. La arquitectura de seguridad define los controles usados para hacer cumplir los niveles de disponibilidad, integridad y confidencialidad.

Una arquitectura de seguridad completa abarca protección a varios niveles y contra amenazas accidentales e intencionales:

- Protección del recurso humano: Ante amenazas físicas y lógicas
- Protección de la infraestructura física: Ante amenazas físicas.
- Protección de la red: Ante ataques pasivos y activos.
- Protección de los servicios: Tanto internos como externos a la organización (evitar ataques desde dentro de la organización hacia servicios externos a laorganización).

Seguridad Física

El objetivo de la seguridad física es proporcionar un ambiente seguro para todos los activos e intereses de la organización, incluyendo las actividades del sistema de información.
La seguridad física proporciona protección para los edificios o cualquier estructura (vehículos) que hospede el sistema u otros componentes de redes. Los sistemas son caracterizados como estáticos, móviles o portátiles.

Seguridad Lógica

Los objetivos que se plantean para lograr la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Se disponga de pasos alternativos de emergencia para la transmisión de información.

Gerencia del riesgo

La gestión de riesgos es el proceso que comprende la identificación y medición de los riesgos de seguridad en los sistemas informáticos, así mismo, comprende la creación de estrategias que permiten controlar y minimizar dichos riesgos.

Entre las estrategias se incluyen:

- Transferir el riesgo,
- Evitar el riesgo,
- Reducir el efecto negativo del riesgo
- Aceptar parte o todas las consecuencias de un riesgo particular.

El objetivo primordial de dichas estrategias es reducir al mínimo los costos mientras se maximiza la reducción de los efectos negativos de los riesgos, dando como resultado un plan de seguridad adecuado a un sistema o ambiente específico

Análisis de riesgo

El análisis y evaluación de riesgos es el proceso de analizar el ambiente y las relaciones de los atributos relacionados con los riesgos.

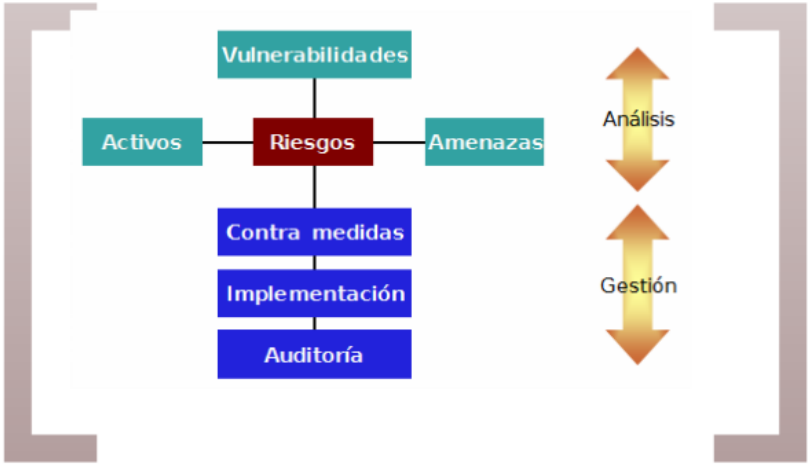
Este proceso debe identificar vulnerabilidades y asociarlas con los activos afectados. La fase incluye la identificación de riesgos, y de las medidas para reducir dichos riesgos, así como también determinar el impacto económico de aceptar los riesgo, evitar los riesgos o transferir los riesgo.

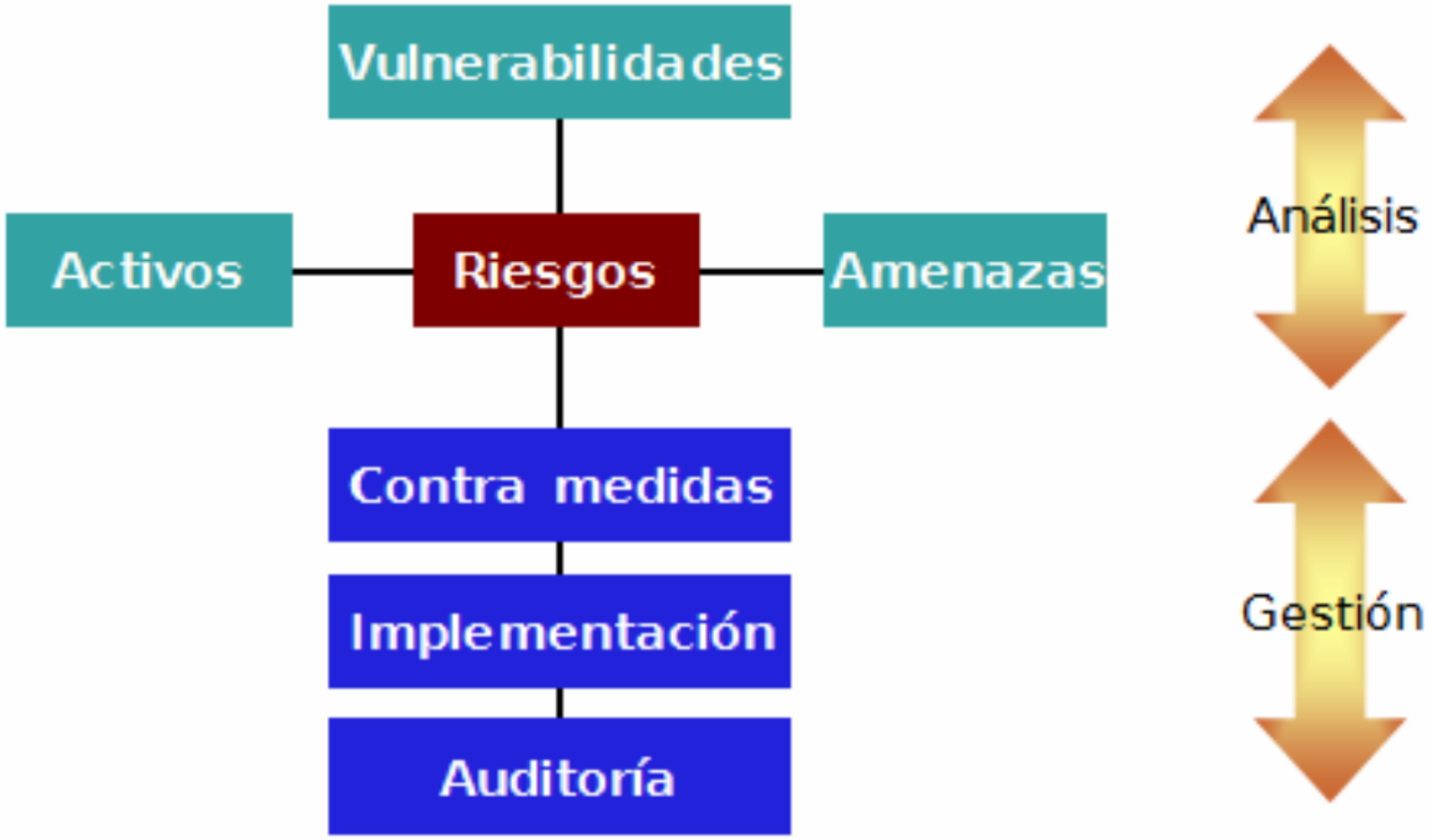
Riesgo = Amenaza x Impacto

CRAMM

Central Computer and Telecommunications Agency Risk Analysis and Management Method

Es una metodología cualitativa para el análisis y gestión de riesgos. Hoy en día ya existen herramientas automatizadas para llevar a cabo un análisis de riesgos utilizando la metodología CRAMM (www.cramm.com)




Vulnerabilidades
Activos
Riesgos
Amenazas
Contra medidas
Implementación
Auditoría
Análisis
Gestión

OCTAVE

Operationally Critical Threat, Asset and Vulnerability Evaluation

Es un estándar que permite evaluar las vulnerabilidades y amenazas que existen sobre los activos y operaciones críticas de una organización. Su metodología evalúa la tecnología en función de los riesgos operacionales y las prácticas de seguridad.

Esta metodología fue desarrollada para organizaciones grandes (+ 300 empleados) con jerarquías múltiples con la capacidad mantener una infraestructura de sistemas robusta.

OCTAVE

Esta metodología consta de 3 fases para evaluar los aspectos organizativos y tecnológicos para proveer una imagen de las necesidades de la organización en términos de seguridad.

Cada fase cuenta con talleres conducidos por equipos interdisciplinarios de entre 3 y 5 empleados de la empresa. En ellos se detallaran:

- Identificación de activos críticos y sus amenazas
- Identificación de vulnerabilidades tanto organizativas como tecnológicas que pueden exponer a la organización a las amenazas identificadas en la fase anterior
- Desarrollar una estrategia de protección y mitigación que refleje la misión de la organización y sus prioridades

Cada fase cuenta con talleres conducidos por equipos interdisciplinarios de entre 3 y 5 empleados de la empresa. En ellos se detallaran:

- Identificación de activos críticos y sus amenazas
- Identificación de vulnerabilidades tanto organizativas como tecnológicas que pueden exponer a la organización a las amenazas identificadas en la fase anterior
- Desarrollar una estrategia de protección y mitigación que refleje la misión de la organización y sus prioridades

Gerencia del riesgo

La gestión de riesgos es el proceso que comprende la identificación y medición de los riesgos de seguridad en los sistemas informáticos, así mismo, comprende la creación de estrategias que permiten controlar y minimizar dichos riesgos.

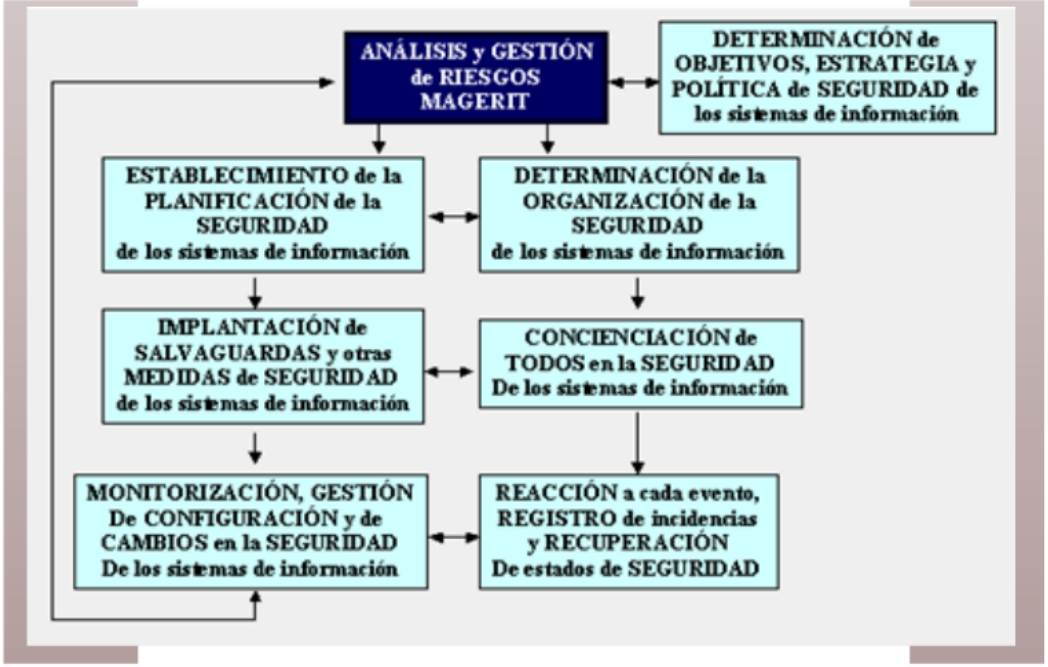
Entre las estrategias se incluyen:

- Transferir el riesgo,
- Evitar el riesgo,
- Reducir el efecto negativo del riesgo
- Aceptar parte o todas las consecuencias de un riesgo particular.

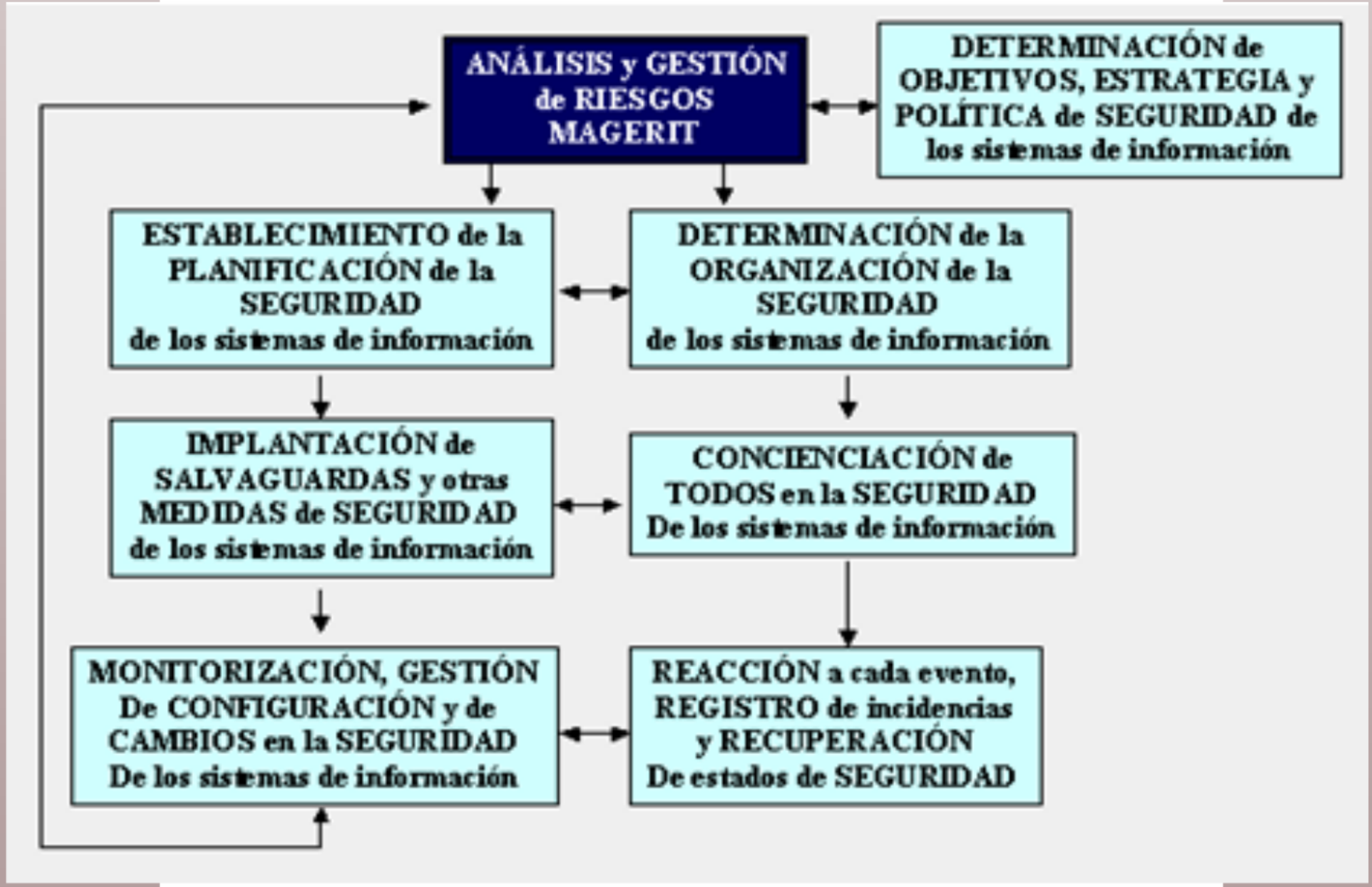
El objetivo primordial de dichas estrategias es reducir al mínimo los costos mientras se maximiza la reducción de los efectos negativos de los riesgos, dando como resultado un plan de seguridad adecuado a un sistema o ambiente específico

MAGERIT

Es una metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones publicas. Fue elaborado por el Consejo Superior de Informática del Estado Español. Su objetivo es investigas los riesgos inherentes a los sistemas de información y recomendar medidas para controlarlos.



los.


ANÁLISIS y GESTIÓN de RIESGOS MAGERIT
DETERMINACIÓN de OBJETIVOS, ESTRATEGIA y POLÍTICA de SEGURIDAD de los sistemas de información
ESTABLECIMIENTO de la PLANIFICACIÓN de la SEGURIDAD de los sistemas de información
DETERMINACIÓN de la ORGANIZACIÓN de la SEGURIDAD de los sistemas de información
IMPLANTACIÓN de SALVAGUARDAS y otras MEDIDAS de SEGURIDAD de los sistemas de información
CONCIENCIACIÓN de TODOS en la SEGURIDAD De los sistemas de información
MONITORIZACIÓN, GESTIÓN De CONFIGURACIÓN y de CAMBIOS en la SEGURIDAD De los sistemas de información
REACCIÓN a cada evento, REGISTRO de incidencias y RECUPERACIÓN De estados de SEGURIDAD

Clasificación del riesgo

La clasificación de bienes le proporciona a la organización una manera de determinar y manejar sus riesgos mas significativos, produciendo el nivel adecuado de seguridad.

Clasificar la información y los bienes de la organización basado en riesgos del negocio, valor de los datos y de los bienes, o algún otro criterio, tiene mucho sentido en los negocios.

No toda la información y los bienes tienen el mismo valor o uso o están sujeto a los mismos riesgos. Por lo tanto, los mecanismos de protección, procesos de recuperación, etc, son, o deberían ser, diferentes, con la respectiva diferencia de costos asociados con ellos.

Clasificación del riesgo

Una vez los riesgos han sido identificados y evaluados, todas las técnicas para manejar los riesgos pertenecen a una de estas principales categorías:

- Aceptar el riesgo
- Evitar el riesgo
- Reducir el riesgo
- Transferir el riesgo

De forma práctica

1. Realizamos un inventario de los bienes informáticos (Computadores, laptops, enrutadores, switchs, cortafuegos, cableado, servidores, sistema de enfriamiento, sistema eléctrico)

2. Realizamos un inventario del software utilizado en la empresa o institución

3. Luego se recomienda realizar equipos de trabajo interdisciplinario para la evaluación de las amenazas e impacto de cada bien

4. Una vez que conocemos todos los elementos se construye la matriz de riesgos en conjunto con el listado de amenazas y los inventarios

5. De acuerdo a la evaluación se decidirá: aceptar, evitar, reducir o transferir el riesgo

Listado de amenazas

Código	Amenaza	Código	Amenaza
A1	Replicación de Malware	A14	Falta de Administración de Incidentes
A2	Fugas de Información	A15	Errores de configuración (Administradores)
A3	Alteración de la Información	A16	Falta Mantenimiento General
A4	Destrucción de la Información	A17	Falta de Documentación de los procesos de Administración de dispositivos y del sistema
A5	Divulgación de la información	A18	Falta de actualizaciones (Sistema Operativo, Antivirus, Gestor de B.D)
A6	Vulnerabilidad de Sw. (Servicios y Aplicaciones)	A19	Daño físico de dispositivos
A7	Sw desactualizado (Servicios y Aplicaciones)	A20	Falta de Aplicación de Buenas Prácticas en el desarrollo in House
A8	Acceso no Autorizado	A21	Falta de Personal disponible
A9	Intercepción de Tráfico e Información	A22	Renuncia del Personal
A10	DoS	A23	Caída del canal WAN
A11	Falta Backup de Información	A24	Caída del canal Internet Personal
A12	Falta Backup de Configuración de Dispositivos	A25	Caída del canal Internet Estudiantes
A13	Falta de Administración de Logs	A26	Caída de la red LAN

Listado de salvaguardas

Código	Salvaguarda
S1	Cifrado
S2	Copias de Respaldo
S3	Controles de Acceso
S4	Registro de Actuaciones
S5	Detección de Intrusos (Monitorización)
S6	Hardening de Dispositivos y Aplicaciones
S7	Gestión y administración de claves
S8	Definición de Roles de Seguridad
S9	Administración de Continuidad del Negocio
S10	Auditoría Interna
S11	Antivirus Actualizado
S12	Análisis de Requerimientos
S13	Desarrollo bajo metodologías de calidad CMMI
S14	Actualización de Versiones
S15	Aplicación de Pruebas de Funcionamiento
S16	Mantenimiento de Equipos
S17	Definición exacta de Funciones
S18	Definición de Políticas de Seguridad
S19	Topologías Redundantes
S20	Documentación de los Procesos Administrativos y de Configuraciones
S21	IDS/IPS
S22	PKI
S23	ISDN
S24	Canal de Contingencia
S25	VPN

Valores para la probabilidad de ocurrencia y el impacto

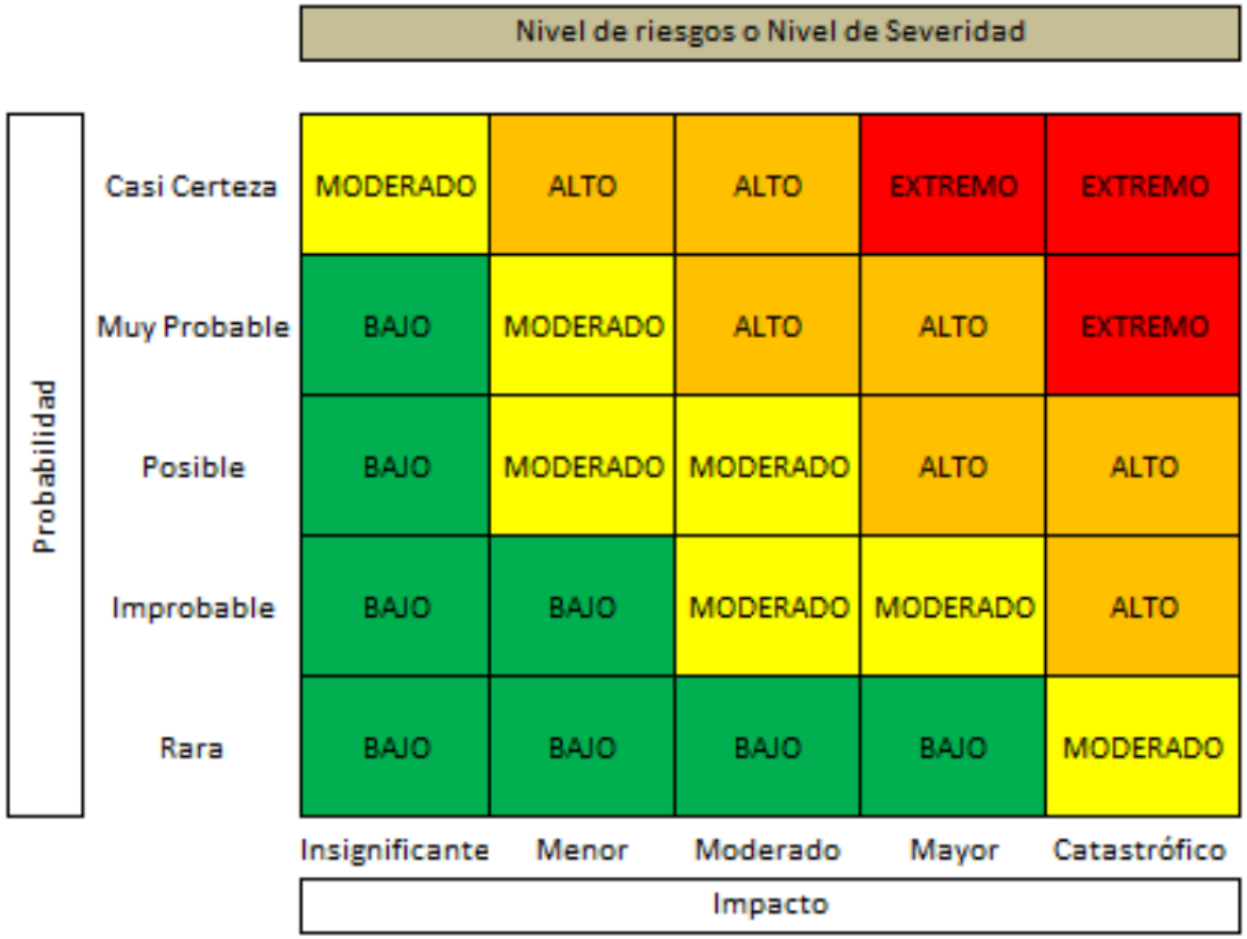
Probabilidad

Descriptor	Valor
Rara	1
Improbable	2
Posible	3
Muy Probable	4
Casi Certeza	5

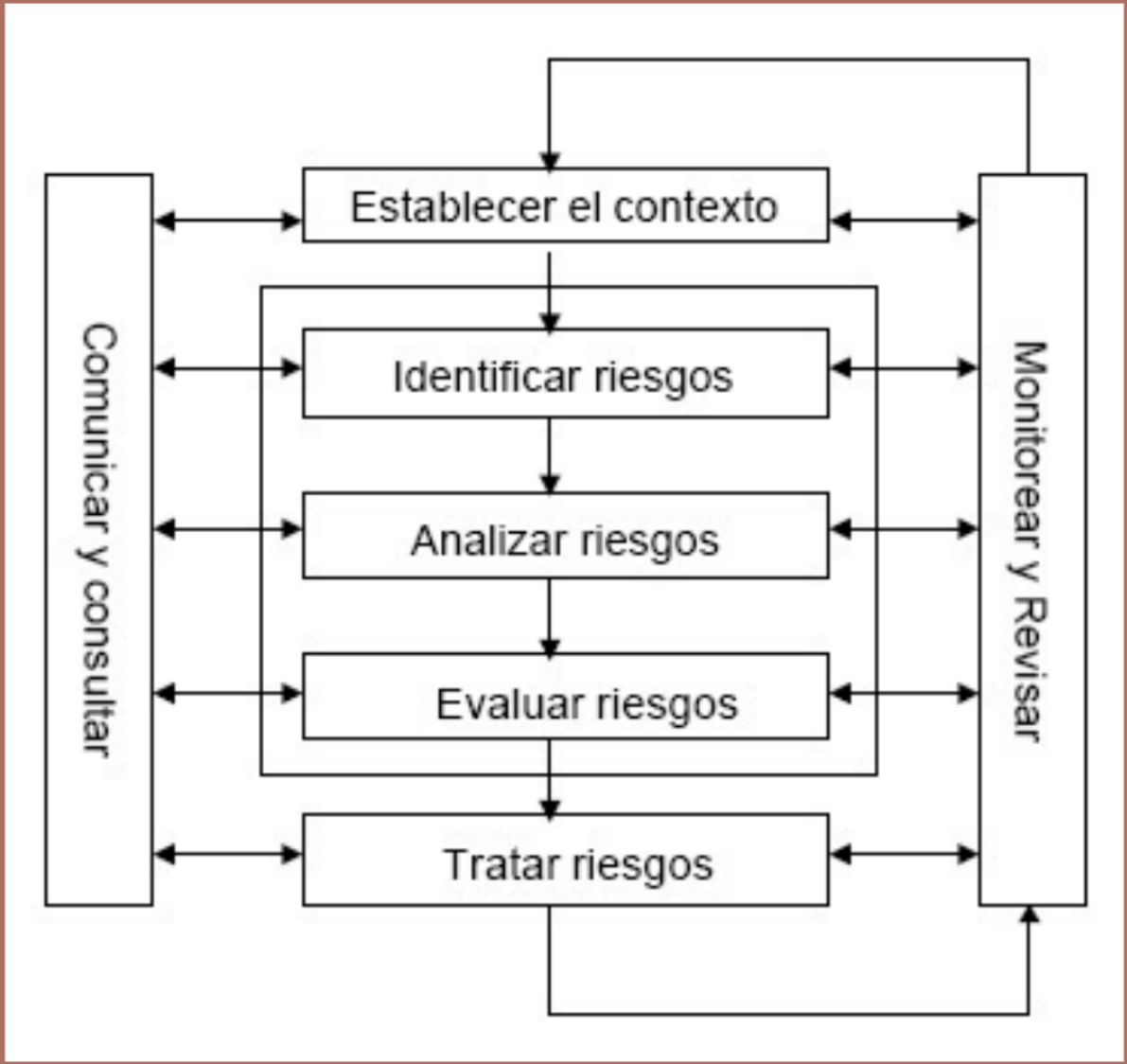
Impacto

Descriptor	Valor
Insignificante	1
Menor	2
Moderado	3
Mayor	4
Catastrófico	5

Cuando los unimos:



El proceso de gestión de riesgos



Política y Directrices de Seguridad

¿Qué es la Política de Seguridad?

Es la normativa y directrices que nos permitirán lograr un "Equilibrio entre la seguridad y la capacidad de hacer negocios."

SysAdminAudit, Networking and Security Institute. Information Systems Security Architecture: A Novel Approach to Layered Protection. Estados Unidos. SANS, 2004

¿Qué contiene la Política de seguridad?

"Declaración de la importancia de la información en la organizaciones, de tal manera que refleje las intenciones de la Alta Gerencia por cumplir con los objetivos de seguridad del negocio, de acuerdo a su misión y visión e incorporando además la legislación vigente en materia de seguridad aplicable al negocio"

¿Qué contiene la Política de seguridad?

"Declaración de la importancia de la información en la organizaciones, de tal manera que refleje las intenciones de la Alta Gerencia por cumplir con los objetivos de seguridad del negocio, de acuerdo a su misión y visión e incorporando además la legislación vigente en materia de seguridad aplicable al negocio"

as tareas
tadas la

S

¿Qué define la política de Seguridad?

"La política de SI define las pautas en el comportamiento de los actores respecto a la protección de uno de los activos importantes dentro de la organización, la información.

Se recomienda redactar la política de SI y sus directrices con un lenguaje apropiado que permita el fácil entendimiento a los usuarios."

JulyCalvo, Diego Parada, Angélica Flórez. Proyecto Metodología para la implementación del Modelo de Arquitectura de Seguridad de la Información (MASI), 2010.

¿Qué son las Directrices de Seguridad?

"Detallan los lineamientos estratégicos de la política de seguridad de la información."

¿Qué son las Normas de Seguridad?

"Las normas establecen la instrumentalización de los lineamientos definidos en la política y las directrices de seguridad de la información.
Clarifica qué se busca proteger (activos, procesos, personas, entre otros) y el nivel de protección que se quiere brindar, especificando de forma general los ítems o requisitos necesarios para dar cumplimiento a la política desde un punto de vista táctico."

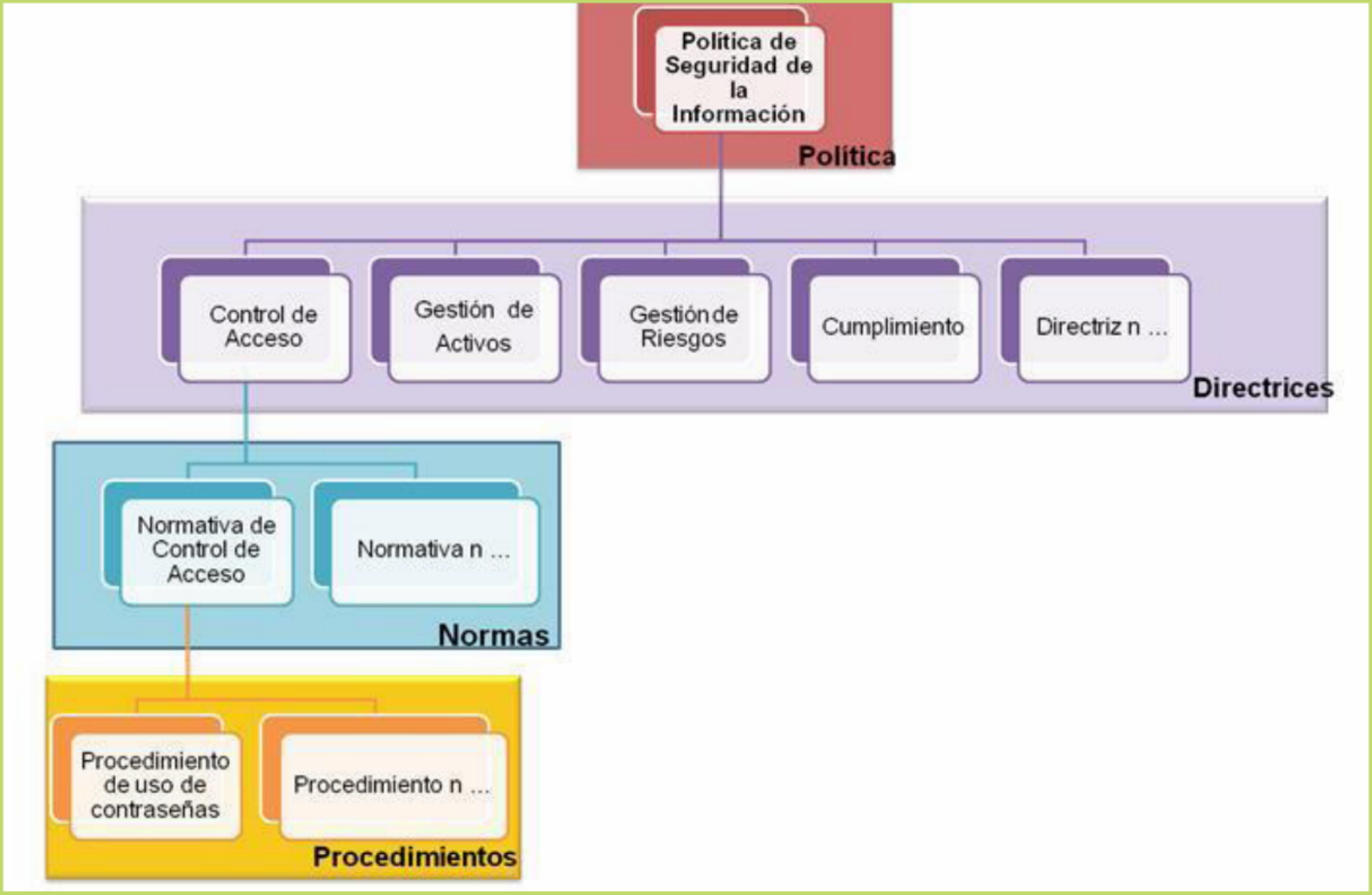
ntos

encuentran en

¿Qué son los procedimientos de Seguridad?

"Contienen el marco operativo y se encuentran en caminados en el cumplimiento de las normas de SI, por tal razón, en éstos se detallan cada una de las actividades basadas en buenas prácticas que deben ser desarrolladas por los actores.
También en los procedimientos se especifican las tareas que determinan el cómo deben ser ejecutadas la actividades y los responsables de su ejecución."

Estructura de la política de seguridad y su normativa



Un ejemplo!

ID	Título de la Directriz
	Cultura de Seguridad Informática
Dirigida a	Comunidad Universitaria
Objetivo	Involucrar a la comunidad universitaria en el mejoramiento de los esquemas de la Seguridad Informática en la Institución, mediante el cumplimento de reglas de comportamiento que faciliten el aseguramiento y protección de los recursos y servicios informáticos.

Normas

- Los usuarios deben firmar cláusulas de cumplimiento de las Políticas de Seguridad en los contratos laborales y académicos.
- El Departamento de Tecnologías debe realizar actividades de concienciación y capacitación a los usuarios respecto a la importancia y la forma de proteger la información manejada al interior de la Institución.
- El Departamento de Desarrollo del Personal debe reportar al Departamento de Tecnologías de la renuncia o despido de empleados, con el fin de retirar los permisos de acceso a los servicios.
- El manejo de la información en medio impreso es responsabilidad de cada dependencia, se debe tener en cuenta que:
  - Debe estar almacenada en un lugar seguro.
  - El manejo de la correspondencia debe guiarse bajo las técnicas de oficina vigentes.
  - La información deberá resguardarse en lugares de difícil acceso a terceros y protegidos de condiciones ambientales que puedan afectarle.
  - Por ningún motivo se debe dejar documentación e información relevante sobre los escritorios cuando la persona a cargo se ausente del sitio de trabajo.
- Todos los integrantes de la Institución deben propender por el cumplimiento de las directrices establecidas.

Desarrollada por	Departamento de Tecnologías y Seguridad de la Información
Revisada por	
Rige a partir de	Su fecha de publicación

Referencias

- McNab, C. Network Security Assessment. O' Reiilly. 2004.
- Cano, J. Computación Forense, descubriendo los rastros informáticos. Alfaomega. 2009.
- Daltabuitz; Hernández;Mallén; Vázquez. La seguridad de la información. Limusa, Noriega Editores. 2007.
- Ormella , C. ¿Seguridad informática vs. Seguridad de la información?.2004.
- Ramió, J. Libro Electrónico de Seguridad Informática y Criptografía. Versión 4.1 de 1 de marzo de 2006.