Seguridad Informática

Semana 01 – 02

Manuel Lagos

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
Real, Pontificia y Nacional
1677

Temario

- Perfil del estudiante de Seguridad Informática

- Conceptos básicos de la seguridad
- Objetivos de la seguridad informática
- Servicios de seguridad de la información
- Consecuencias de la falta de seguridad
- Principio de defensa en profundidad
- SGSI
- Análisis y gestión de riesgos.

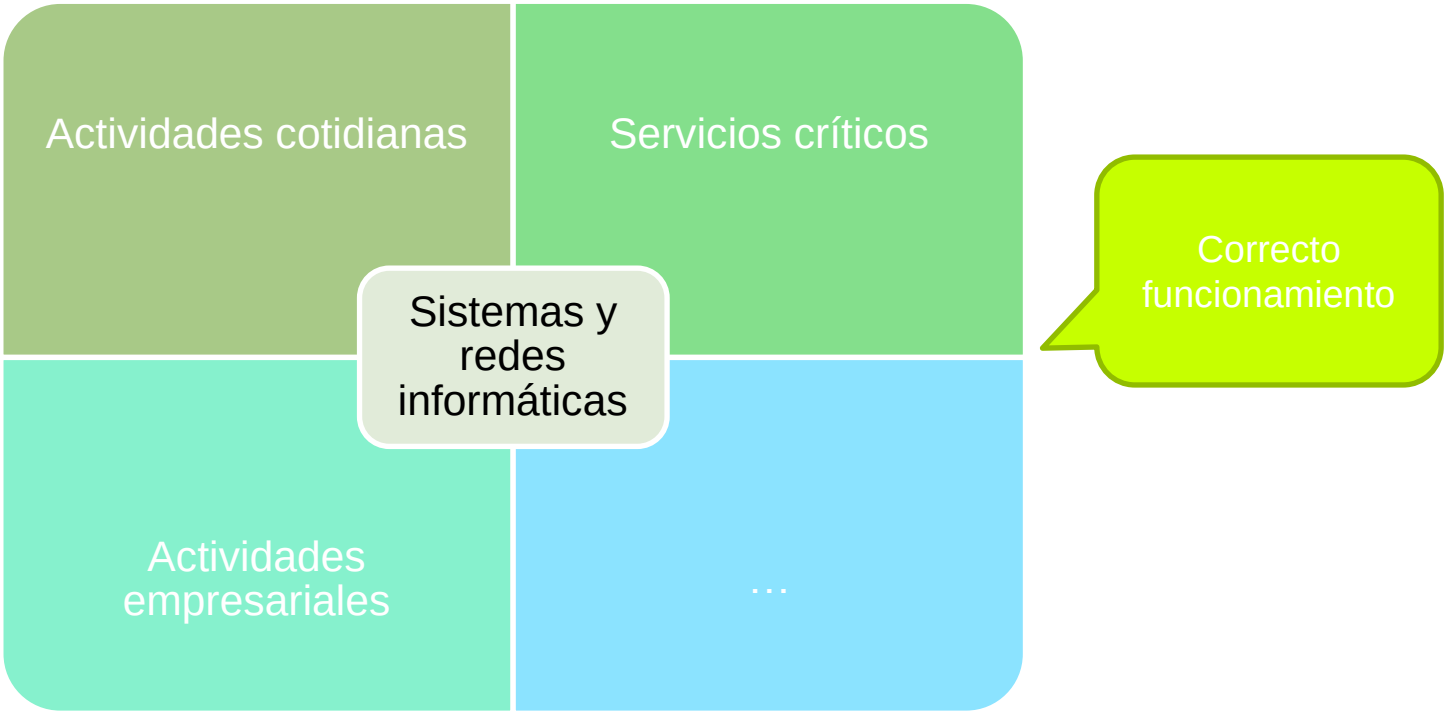
Seguridad

- Rae: “Cualidad de seguro”
- Seguro: adj. “Libre y exento de riesgo”

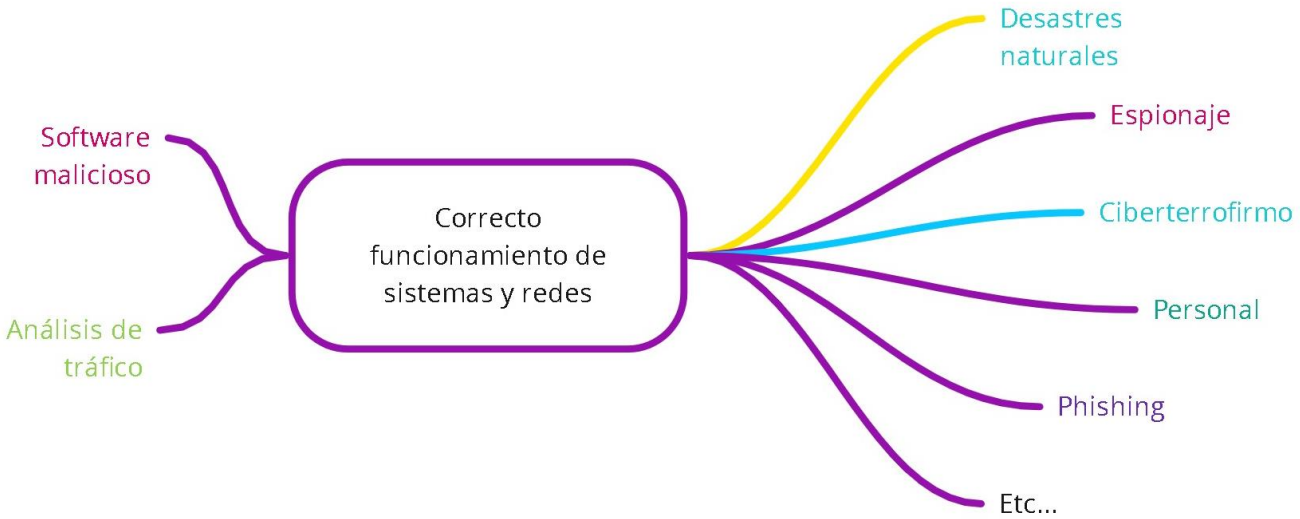
¿De qué hablamos cuando se pide garantizar la seguridad de un sistema informático?

Sistema informático:
- Seguridad Alta
- Seguridad baja
- Seguridad Media…

Seguridad informática



Seguridad informática



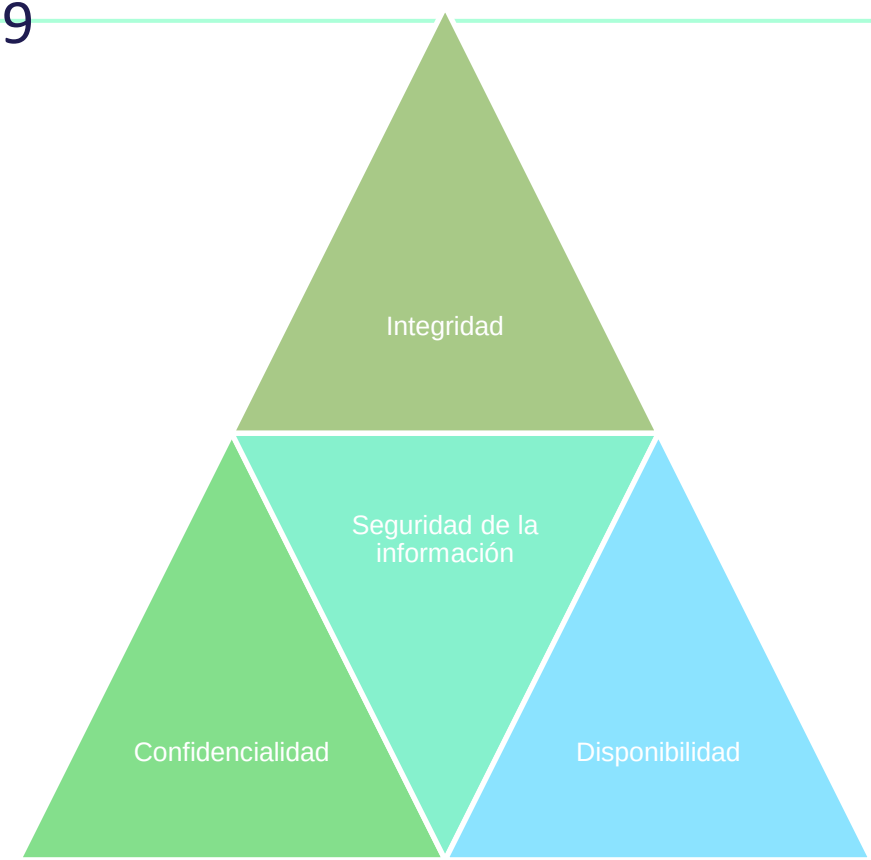
Seguridad informática

- Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso a usuarios autorizados al sistema

- ISO 7498: Serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización.

- INFOSEC GLOSSARY 2000: medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo software, hardware, firmware y aquella información que procesan, almacenan y comunican.

ISO / IEC 17799



Seguridad informática & Seguridad de la información

- Participación grupal

Objetivos de la seguridad

- Minimizar riesgos, detectar amenazas de seguridad.
- Garantizar el adecuado uso de recursos de los sistemas.
- Limitar pérdidas y conseguir la recuperación del sistema.
- Cumplir con el marco legal y requisitos impuestos por clientes.

Conceptos básicos

- Amenaza
- Ataque
- Vulnerabilidad
- Riesgo
- Impacto

Reflexiones sobre la seguridad

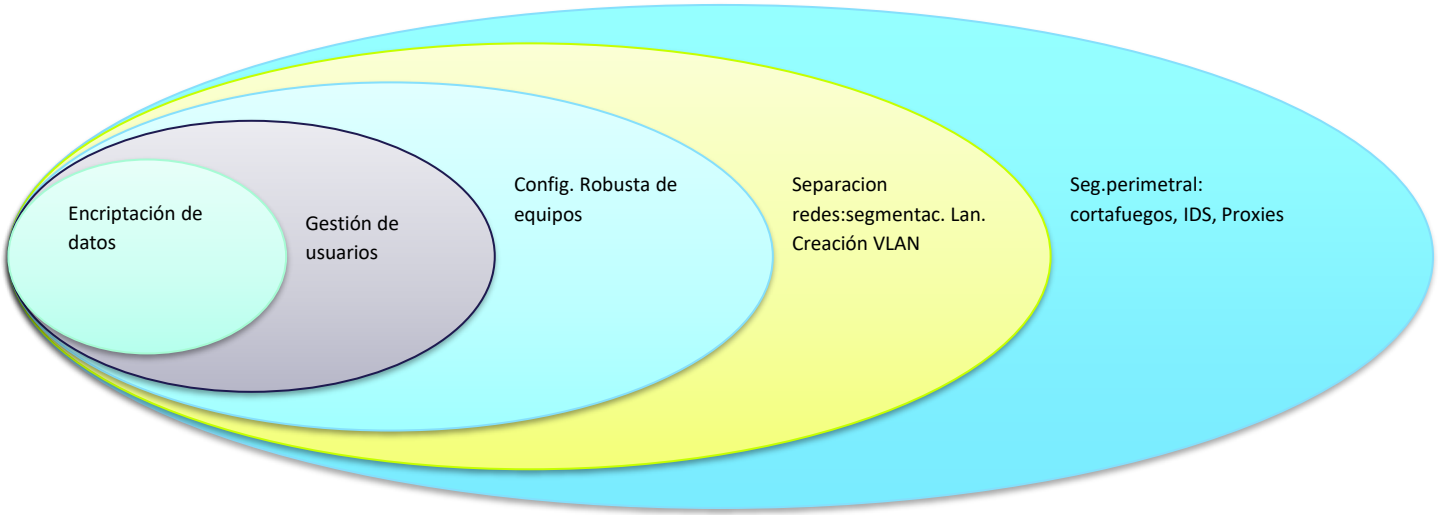
- **¿Dormiríamos hoy en día en nuestra casa con dos ventanas y la puerta del garaje abiertas?**
- **Todo sistema es tan fuerte como su eslabón más débil.**
- **Seguridad total.**

Servicios de la seguridad informática

- Confidencialidad
- Autenticación
- Integridad
- No repudiación
- Disponibilidad
- Autorización
- Auditabilidad
- …

¿Qué técnicas y/o mecanismos se pueden implantar para brindar estos servicios?

Principio de defensa en profundidad

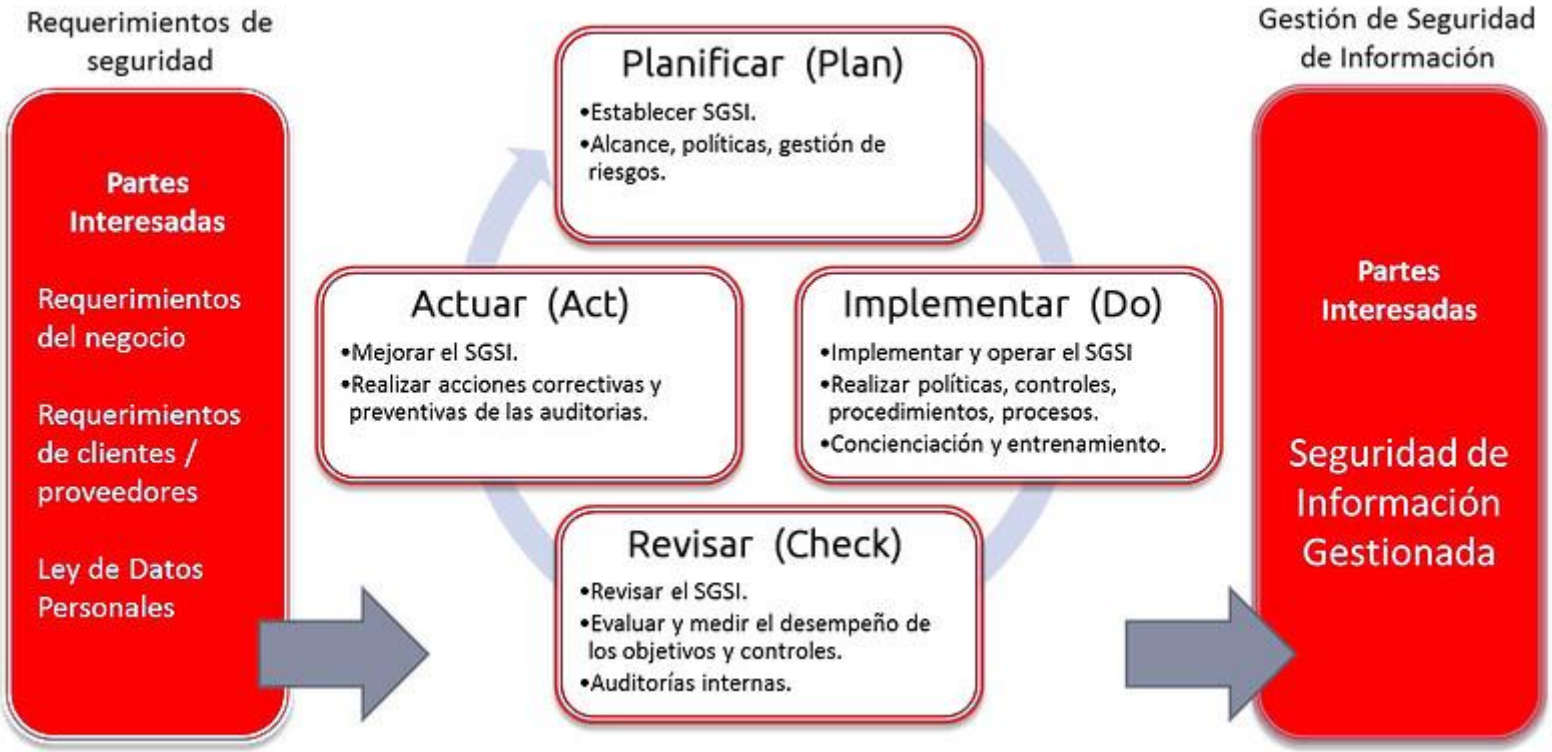


SGSI

- Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

- Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

SGSI



ISO 27001

SGSI - Implantación

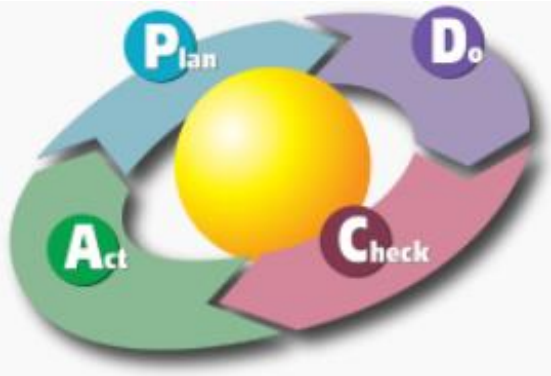
- La implantación de un SGSI es una decisión estratégica que debe involucrar a toda la organización.
- Su implantación depende mucho de la parte gerencial.
- Objetivos de la empresa.
- Alcance: áreas involucradas en el cambio.
- Contar con la ayuda de una empresa especializada para asesoramiento en el proceso, durante un tiempo inicial.

SGSI - Implantación

- El tiempo de implantación depende:
  - Tamaño de la organización
  - Estado inicial de la seguridad de la información.
  - Recursos destinados.
  - Recomendable: 6 meses y un año (para evitar que quede obsoleto).
- “La solución más sencilla de mantener suele ser la más acertada”.
- La empresa debe contar con:
  - Estructura organizativa
  - Recursos necesarios

SGSI – Modelo PDCA

- La implementación generalmente se utiliza el modelo PDCA(**Plan-Do-Check-Act**)



Modelo PDCA

- Plan (planificar): es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- Do (hacer)(ejecución): es una fase que envuelve la implantación y operación de los controles.
- Check (controlar)(seguimiento): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- Act (actuar)(mejora): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

Planificación:

- Estudio de la situación de la organización desde el punto de vista de la seguridad.
- Estimar las medidas que se van a implantar en función de las necesidades detectadas.
- No toda la información de la que se dispone tiene el mismo valor o está sometida a los mismos riesgos.
- Realizar un **análisis** de riesgos que valore los activos de información y vulnerabilidades a las que están expuestas.
- **Gestión** de riesgos para reducirlos en la medida de lo posible.
- Establecer los controles adecuados que permitan minimizar los riesgos.

Ejecución:

- Controles técnicos, como documentación necesaria.
- Requiere de un tiempo para: concientizar y formar para dar a conocer que se está haciendo y por qué, al personal de la empresa.

Seguimiento:

- Evaluar la eficacia y el éxito de los controles implantados.
- Se debe contar con registros e indicadores que provengan de estos controles.

Mejora:

- Se debe llevar a cabo las labores de mantenimiento del sistema.
- Si se ha detectado algún punto débil este es el momento de las mejoras y correcciones.
- Se cuenta con tres tipos de medidas:
    - Medidas correctoras
    - Medidas preventivas
    - Medidas de mejoras.

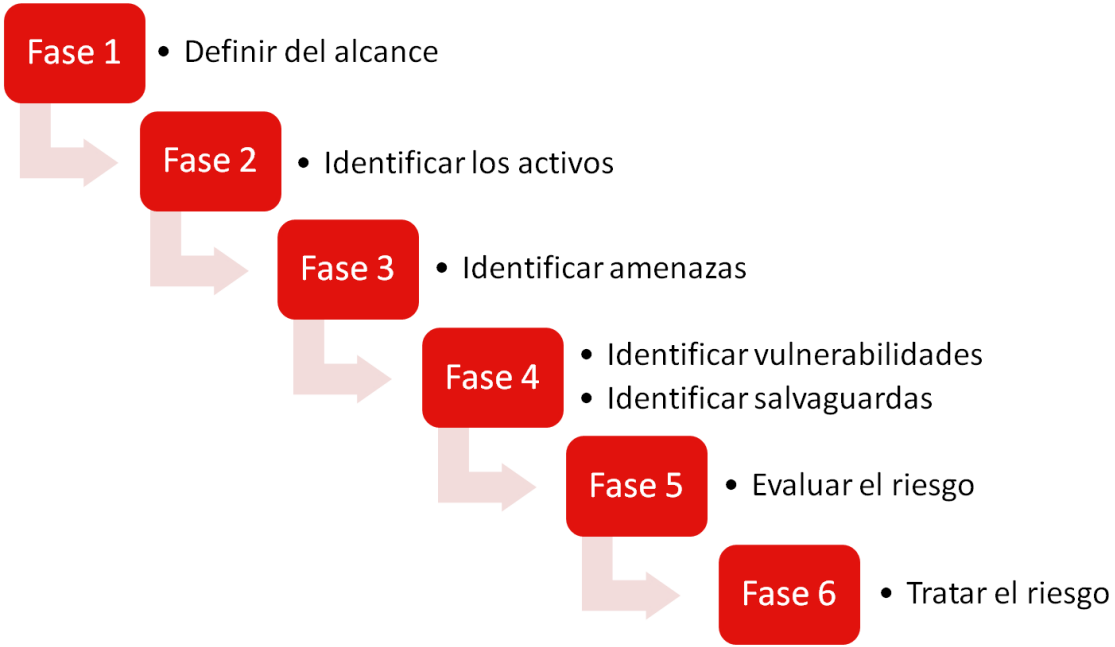
SGSI - Implantación

- Al finalizar las 4 fases se debe tomar los resultados de la última fase y se comienza nuevamente la primera.
- Si el objetivo de la implantación de este sistema era la certificación, el ciclo completo tendrá una duración de un año.
- Se coincidirá con las realizaciones de las auditorías de certificación que se realizan cada año.

SGSI - Implantación

- La implantación de un SGSI debe estar documenta en:
  - Políticas.(Objetivos generales sin entrar en detalles técnicos)
  - Procedimientos.(cómo conseguir los objetivos de las políticas, detalles más técnicos)
  - Instrucciones: comandos técnicos que se deben realizar para la ejecución de procedimientos.
  - Registros: Registros que evidencian la efectiva implantación del sistema y el cumplimiento de los requisitos. Incluyen indicadores, métricas de seguridad que permiten evaluar la consecuencia de los objetivos establecidos.

Análisis y gestión de riesgos



Análisis y gestión de riesgos

- Fase 1. Definir el alcance
- El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Director de Seguridad. Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad. Por otra parte, también es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas. *Por ejemplo*, **análisis de riesgos sobre los procesos del departamento Administración**, **análisis de riesgos sobre los procesos de producción y gestión de almacén** o **análisis de riesgos sobre los sistemas TIC relacionados con la página web de la empresa**, **el análisis de riesgos es "Los servicios y sistemas del Departamento Informática**, etc.

Análisis y gestión de riesgos

- Fase 2. Identificar los activos
- Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Para mantener un inventario de activos sencillo puede ser suficiente con hacer uso de una hoja de cálculo o tabla, por ejemplo:

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Análisis y gestión de riesgos

- Fase 3. Identificar / seleccionar las amenazas
- Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.
- *Por ejemplo*, si nuestra intención es evaluar el riesgo que corremos frente a la destrucción de nuestro servidor de ficheros, es conveniente, considerar:

    - Las averías del servidor,
    - La posibilidad de daños por agua (rotura de una cañería) o
    - Los daños por fuego

Análisis y gestión de riesgos

- Fase 4. Identificar vulnerabilidades y salvaguardas
- La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. *Por ejemplo,* una posible vulnerabilidad puede ser:
    - Identificar un conjunto de ordenadores o servidores cuyo sistemas antivirus no están actualizados o
    - Una serie de activos para los que no existe soporte ni mantenimiento por parte del fabricante.
- Posteriormente, a la hora de evaluar el riesgo aplicaremos penalizaciones para reflejar las vulnerabilidades identificadas.

Análisis y gestión de riesgos

- Fase 4. Identificar vulnerabilidades y salvaguardas
- Por otra parte, también analizaremos y documentaremos las medidas de seguridad implantadas en nuestra organización. ***Por ejemplo*, es posible que hayamos instalado un sistema SAI (Sistema de Alimentación Ininterrumpida) o un grupo electrógeno para abastecer de electricidad a los equipos del CPD**. **Ambas medidas de seguridad (también conocidas como salvaguardas) contribuyen a reducir el riesgo de las amenazas** relacionadas con el corte de suministro eléctrico.
- Estas consideraciones (vulnerabilidades y salvaguardas) debemos tenerlas en cuenta cuando vayamos a **estimar la probabilidad y el impacto** como veremos en la siguiente fase.

Análisis y gestión de riesgos

- Fase 5. Evaluar el riesgo
- Llegado a este punto disponemos de los siguientes elementos:
  - Inventario de activos.
  - Conjunto de amenazas a las que está expuesta cada activo.
  - Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).
  - Conjunto de medidas de seguridad implantadas
- Con esta información, nos encontramos en condiciones de calcular el riesgo. Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos.

Análisis y gestión de riesgos

- Fase 5. Evaluar el riesgo
- **Tabla para el cálculo de la probabilidad**

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

- **Tabla para el cálculo del impacto**

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Análisis y gestión de riesgos

- Fase 5. Evaluar el riesgo
- **Cálculo del riesgo**
- A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto:

RIESGO = PROBABILIDAD x IMPACTO

- Si por el contrario hemos optado por el análisis cualitativo, haremos uso de una matriz de riesgo como la que se muestra a continuación:

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Análisis y gestión de riesgos

- Cuando vayamos a estimar la probabilidad y el impacto debemos tener en cuenta las vulnerabilidades y salvaguardas existentes.
- *Por ejemplo,* la caída del servidor principal podría tener un impacto alto para el negocio. Sin embargo, si existe una solución de alta disponibilidad (*Ej*. Servidores redundados), podemos considerar que el impacto será medio ya que estas medidas de seguridad harán que los procesos de negocio no se vean gravemente afectados por la caída del servidor.
- Si por el contrario hemos identificado vulnerabilidades asociadas al activo, aplicaremos una penalización a la hora de estimar el impacto. *Por ejemplo*, si los equipos de climatización del CPD no han recibido el mantenimiento recomendado por el fabricante, incrementaremos el impacto de amenazas como “condiciones ambientales inadecuadas” o “malfuncionamiento de los equipos debido a altas temperaturas”.

Análisis y gestión de riesgos

- Fase 6. Tratar el riesgo
- Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. *Por ejemplo,* trataremos aquellos riesgos cuyo valor sea superior a “4” o superior a “Medio” en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

- **Transferir** el riesgo a un tercero. *Por ejemplo*, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
- **Eliminar** el riesgo. *Por ejemplo,* eliminando un proceso o sistema que está sujeto a un riesgo elevado. Por ejemplo podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
- **Asumir** el riesgo, siempre justificadamente. *Por ejemplo,* el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
- **Implantar** medidas para mitigarlo. *Por ejemplo,* contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

Análisis y gestión de riesgos

- Fase 1. Definir el alcance

Políticas, planes y procedimientos de seguridad

Semana 03

Manuel Lagos

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
Real, Pontificia y Nacional
1677

Temario

Conceptos básicos

- **Política de seguridad**
- Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran (RFCs 1244 y 2196)
- **Plan de seguridad**
- Conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.
- **Procedimiento de seguridad**
- Definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Estos permiten aplicar e implantar las políticas de seguridad que han sido aprobadas por la organización.

Jerarquía de conceptos

¿Qué define el qué se debe proteger?
¿Qué define el cómo se debe proteger?

Política y procedimientos de seguridad

Política	Procedimiento	Tareas a realizar
Protección del servidor web de la organización contra accesos no autorizados	Actualización del software del servidor web	- Revisión diaria de los parches publicados por el fabricante. - Seguimiento de las noticias sobre posibles fallos de seguridad.
	Revisión de los registros de actividad en el servidor	- Revisión semanal de los “logs” del servidor para detectar situaciones anómalas. - Configuración de alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataques e intentos de intrusión

Elementos de la política de seguridad

- Alcance
- Declaración
- Responsabilidad
- Sanciones por no cumplimiento
- Excepciones
- Referencias

Implicados en la definición de políticas de seguridad

- Directivos
- Personal del Departamento de Informática y Comunicaciones
- Miembros del Equipo de Respuesta a Incidentes de Seguridad
- Representantes de los usuarios que puedan verse afectados por las medidas adoptadas.
- Consultores externos en seguridad informática

Inventario de los recursos y definición de los servicios ofrecidos

- La implantación de los distintos elementos de las políticas de seguridad requiere de un inventario previo y del mantenimiento de un registro actualizado de los recursos del sistema informático de la organización:
  - Equipamiento Hardware y de comunicaciones
  - Sistemas operativos y aplicaciones informáticas
  - Bases de datos, ficheros y documentación
  - Puntos de acceso a la red y tipos de conexiones utilizadas

Seguridad frente al personal

- Alta de empleados. Referencias, determinación de cláusulas de confidencialidad. Creación de nuevas cuentas de usuario, asignación de permiso. Formación de obligaciones y responsabilidad de la seguridad de datos.
- Baja de empleados.
- Funciones, obligaciones y derechos de los usuarios. Definir con claridad cuáles son los distintos niveles de acceso a los servicios y recursos del sistema informático.
- Formación y sensibilización de los usuarios.

Adquisición de productos

- Evaluación de productos, proveedores, garantías, mantenimientos, asistencia postventa, Instalación y configuración de productos, Formación y soporte a usuarios.
- Guía de compras y evaluación de productos TIC, para garantizar que se satisface las características de seguridad definidas por la organización.

Relación con proveedores

- Contemplar aspectos como la negociación de los niveles mínimos del servicio y calidad.
- Cumplimiento de normativas nacionales e internacionales. SGSI

Seguridad física de las instalaciones

- ¿Locales críticos?
- Sistema de control de acceso físico
- Protección frente a daños por fuego, inundación, explosiones, accesos no autorizados.
- Elementos de construcción adecuados: puertas, paredes, suelos, falsos techos, canalizaciones.
- Áreas públicas, internas, acceso restringido.
- Implantación de sistemas de vigilancia.
- Control de condiciones ambientales en las instalaciones

Vigilancia de la red y de los elementos de conectividad

- Proteger dispositivos de red.

Otros aspectos a considerar

- Seguridad en los dispositivos de almacenamiento
- Protección en el acceso y configuración de los servidores
- Protección de los equipos y estaciones de trabajo
- Control de los equipos que pueden salir de la organización
- Copias de seguridad
- Control de seguridad de impresoras y otros dispositivos periféricos
- Gestión de soportes informáticos
- Gestión de cuentas de usuarios
- Identificación y autenticación de usuarios
- Autorización y control de acceso lógico.
- Monitorización de servidores y dispositivos de la red.
- Protección de datos y documentos sensibles
- Seguridad de conexiones remotas

Trabajo grupal

Amenazas a la seguridad informática

Semana 06

Manuel Lagos

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
Real, Pontificia y Nacional
1677

Temario

Clasificación de los intrusos en las redes

- Hackers. Intrusos que se dedican a tareas de asalto a los sistemas informáticos como pasatiempo y como retos técnicos. Término anglosajón: Hack (golpear con un hacha)
- Crackers (“blackhats”): Individuos que buscan obtener beneficios de sus ataques. Tienen intereses económicos, políticos, religiosos entre otros. Delitos informáticos.
- Sniffers. Rastrean y tratan de recomponer y descifrar la información que circulan por las redes de ordenadores.
- Pheakers. Sabotean las redes telefónicas.
- Spammers. Responsables de los envíos masivos de miles de mensajes de correos electrónicos no solicitados, a través de internet. ¿Qué provocan?

Clasificación de los intrusos en las redes

- Piratas informáticos
- Creadores programas dañinos y virus
- Lammers. Personas sin conocimientos con herramientas para realizar ataques informáticos. ¿Qué atacan?
- Personal interno. “insiders”.
- Ex empleados. Uso de cuentas activas, bombas lógicas.
- Intrusos remunerados.

Famosos

- Jhon Draper “Capitán Crunch”
- Vladimir Levin
- Kevin Poulson
- Kevin Mitnick

Motivaciones de los atacantes

- FBI:
  - Consideraciones económicas
  - Diversión
  - Ideología
  - Autorrealización
  - Búsqueda de reconocimiento social y estatus en la comunidad

Fases de un ataque informático

- Descubrimiento y exploración del sistema informático.
- Búsqueda de vulnerabilidades en el sistema
- Explotación de vulnerabilidades detectadas (exploits)
- Corrupción o compromiso del sistema.
- Eliminación de las pruebas

Triángulo de la intrusión

Triángulo de la intrusión

- Escáneres de puertos
- Sniffers
- Exploits
- Backdoors kits
- Rootkits
- Auto-rooters
- Password crackers
- Generadores de virus
- Herramientas que facilitan la ocultación y suplantación de IP’s (técnicas de spoofing)
- Herramientas de cifrado y protocolos criptográficos(PGP, SSH, SSL o IPSec)

Tipos de ataques

- Ataques activos
- Ataques pasivos (**participación grupal**)

Virus informáticos y otros códigos dañinos

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
Real, Pontificia y Nacional
1677

Programas Maliciosos

- The terminology in this area presents problems because of a lack(carencia) of universal agreement on all of the terms and because some of the categories overlap.

Stallings- Cryptography And Network Security 4Th Ed

Frases

- "Jo, le voy a meter un virus a mi enamorada para espiarle lo que hace por Internet“
- “Si!, Yo necesito un virus para que el día de la publicación de notas estalle el servidor central de la Universidad“
- “Programemos un virus tan potente como el Melissa o el ILoveYou...i need money!!"

Frases

- Primer Caso.
- Segundo Caso.
- Tercer Caso.
- Muchas veces virus, troyanos, bombas lógicas y gusanos utilizan técnicas de unos y otros entremezcladas, por lo que es difícil establecer fronteras fijas.

Terminología

- Malicious software: is software that is intentionally included or inserted in a system for a harmful(perjudicial) purpose.
- Código malicioso(malware): cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algun sistema informatico.
- No debe ser confundido con software legítimo que contiene errores (*bugs).*

Malware - Consecuencias

- Causar interrupción de los sistemas
- Causar daño a los sistemas
- Romper restricciones de los sistemas
- Controlar funciones existentes en los sistemas.

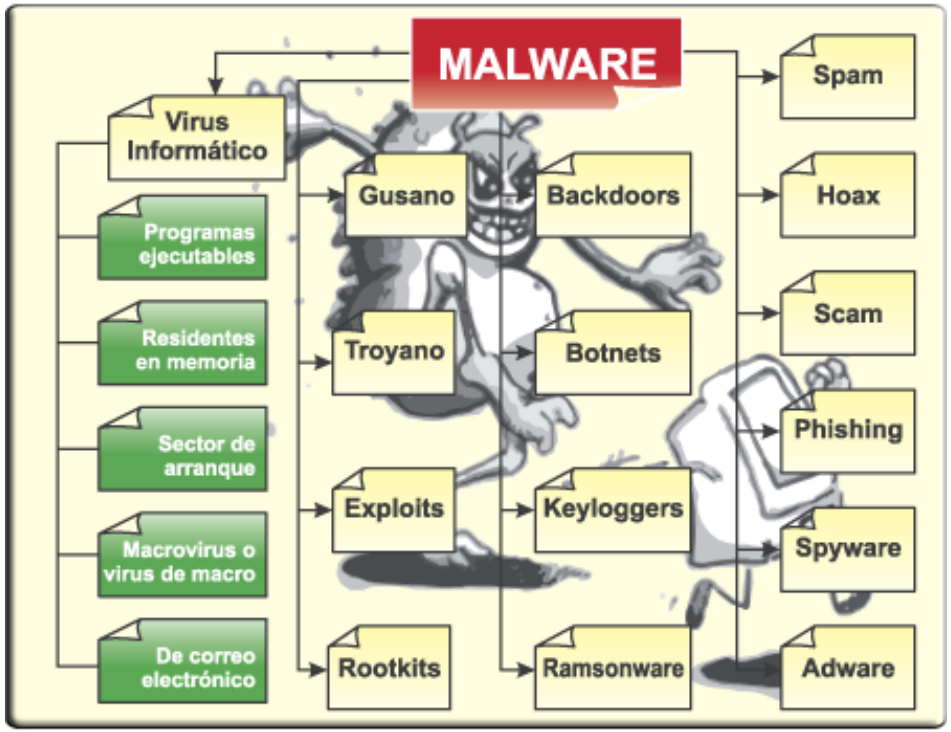
Código Malicioso

- **¿Siempre un código malicioso tiene éxito?**

Clasificación

- Malicious software can be divided into two categories: those that need a host program, and those that are independent.
- Principal clasificación:
  - Virus
  - Gusanos
  - Troyanos
  - Bombas lógicas

Clasificación



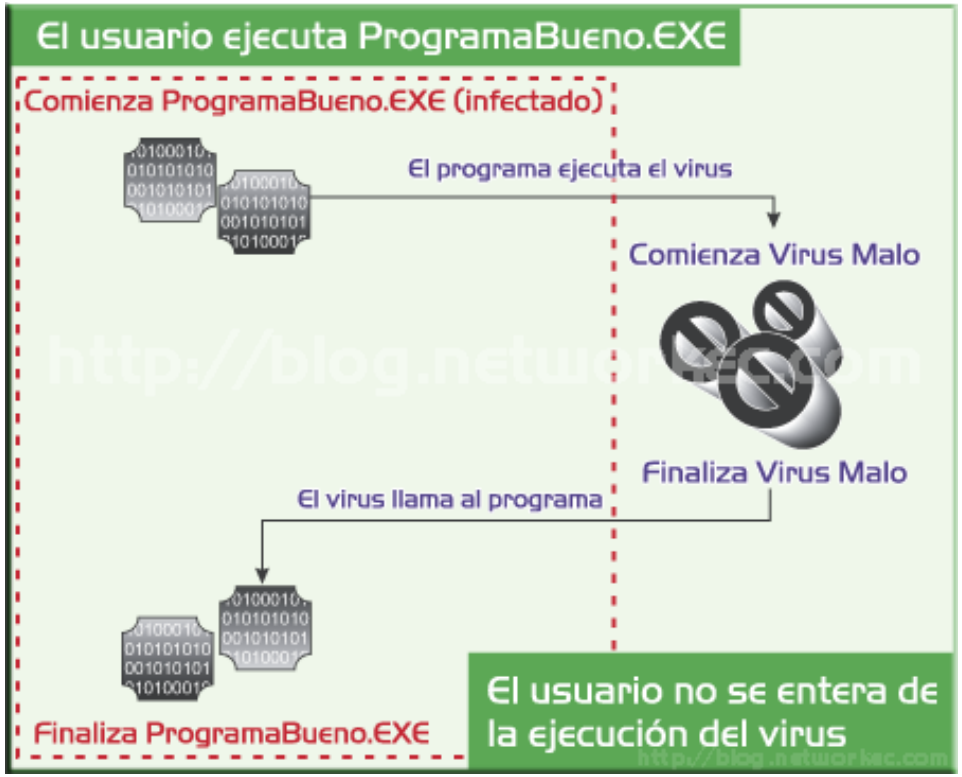
VIRUS

- Un virus biológico destruye las células por las que pasa, monopolizando todo su trabajo vital para su provecho, hasta que termina por matar al organismo.
- Un virus de computadora puede "convivir" durante años con un sistema de producción, y los buenos virus hacen todo lo posible para no interrumpir la funcionalidad de sus programas "huéspedes".

VIRUS

- Origen Latín: refiere a una sustancia capaz de causar una infección mortal.
- Los virus informáticos utilizan los recursos de la PC, se cargan y ejecutan sin permiso del usuario, se propagan y replican con ayuda de archivos infectados, en los cuales se alojan.
- Fred Cohen inventor del término virus informático define un virus como un programa que es capaz de infectar otros programas modificándolos para que incluyan una copia, quizá evolucionada, de él mismo". Es decir, un virus lo que hace es tratar de añadir una copia de su propio código en otros programas.

Ejemplo de ejecución de un virus



Virus – Terminologia

- Payload
- Marca de infección
- Cavity(4kb)

Virus - Tipos

- Polimórficos
- De sector de arranque
- De Macro
- De correo electrónico*

Virus Polimórficos

- Aquellos que mutan con cada infección, haciendo imposible su detección en función de su resumen hash.
- Durante su replicación crean copias que son funcionalmente equivalentes pero con diferentes patrones de bits.

Virus de Sector de arranque(BSI)

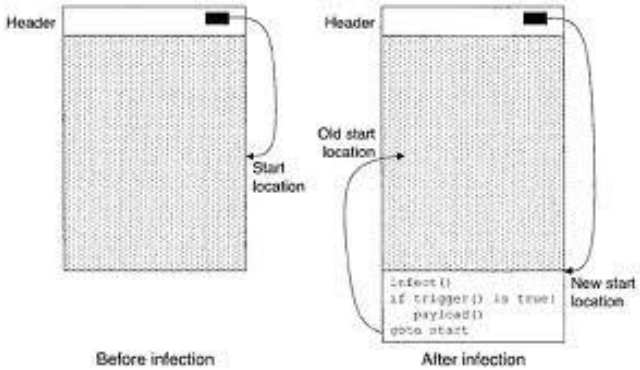
- Infecta el master boot record (MBR) o boot record de un disquete o disco duro y se dispersa cuando un sistema arranca desde el disco que contiene el virus.
- A partir de la infeccion, el virus se ejecuta antes del Sistema Operativo, quedando residente en la memoria del equipo
- Ejm: Polyboot

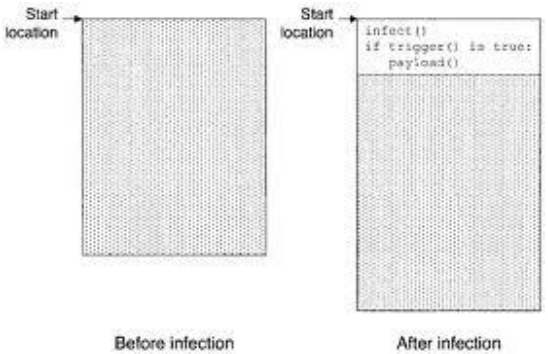
Virus de Macro

- Estos virus son peligrosos por las siguientes razones:
  - Todo sistema operativo que soporta Word puede ser infectado.
  - Infectan documentos, no porciones ejecutables de código.
  - Se dispersan fácilmente. El método más común es vía correo electrónico.
- Una macro es un programa ejecutable embebido en un documento .

Técnicas de Escritura

- Overwrite
- Prepending
- Postpending
- **Companion***





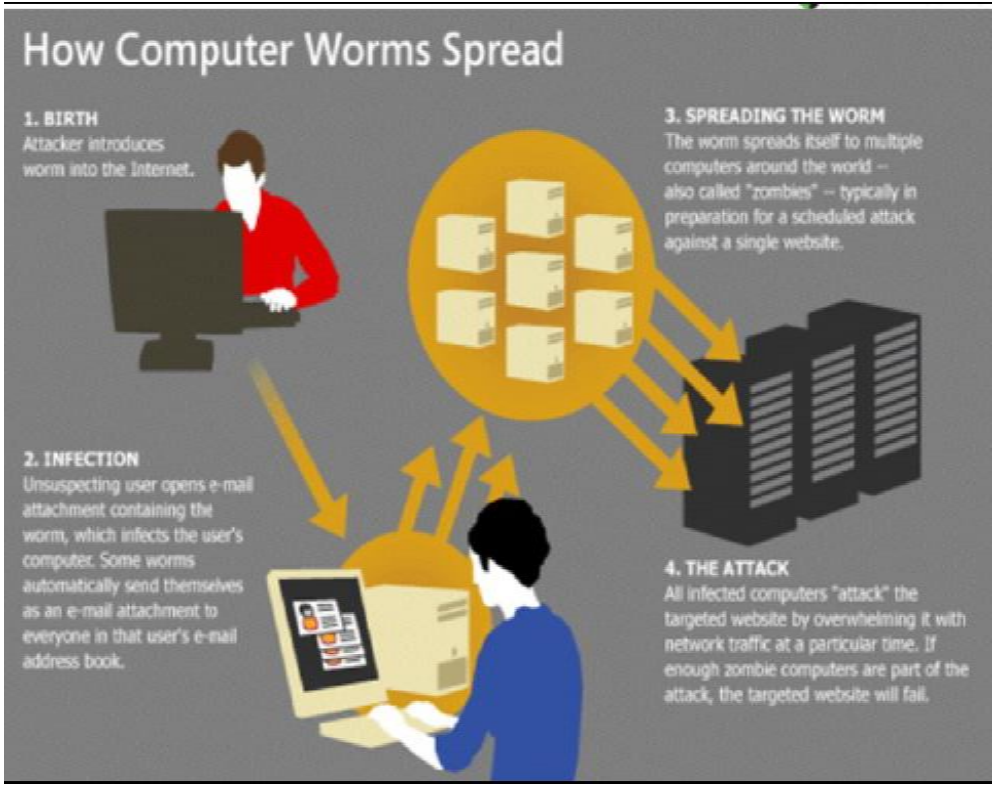
Gusanos

- Programas capaces, al igual que los virus, de reproducirse e insertarse en otros programas o archivos, con la **diferencia** de que no necesitan la ayuda de otro programa para propagarse.
- Originalmente diseñado por dos ingenieros de Xerox para búsqueda en red de procesadores disponibles y asignación de tareas a los mismos.
- Desde 1988, gracias al gusano Morris, existen leyes severas que sancionan la implementación en Internet de gusanos.

Gusanos

- Programas que se replican a sí mismos y se dispersan a través de una red.
- Para propagarse hacen uso de servicios de red existentes en el sistema, como por ejemplo email, telnet, web, ftp.
- Una de sus **características distintivas** es que no modifican otros programas.

Propagación de gusanos



Propagación de gusanos

- **Nacimiento.** El atacante introduce el gusano en Internet.
- **Infección.** El usuario abre el archivo adjunto de un email, lo cual infecta la computadora. Muchos gusanos automáticamente se envían en un email a todos los contactos de la libreta de direcciones del usuario.
- **Dispersión del gusano.** El gusano se dispersa a múltiples computadoras alrededor del mundo – llamadas “zombies” –típicamente preparándose para un ataque programado a un sitio web específico.
- **Ataque.** Todas las computadoras infectadas atacan el sitio web objetivo al recargarlo de tráfico al mismo tiempo. Si hay suficientes “zombies”, el objetivo caerá.

Contramedidas

- Antivirus
  La solución ideal a la amenaza de virus es la prevención: No permitir que ningún virus ingrese al sistema. Esto es imposible, sin embargo se puede tomar ciertas medidas.
  - **Detección**. Una vez que ocurrió la infección, determinarla y ubicar el virus.
  - **Identificación**. Identificar el virus que ha afectado al sistema.
  - **Eliminación**. Remover todo rastro del virus en el programa infectado y regresarlo a su estado original. Remover el virus de los sistemas para que no se propague.

Medidas de seguridad internas

- Pese a la seguridad aparente que puedan brindar medidas de protección tales como los firewalls y antivirus, el aumento de *malware ocasiona cada vez mayor daño a organizaciones y* usuarios.
- Está demostrado que **la mayor parte de los ataques por *malware* provienen desde los equipos de los mismos usuarios de la organización** que, consciente o inconscientemente, permiten la propagación de éstos gracias a permisos excesivos concedidos en el equipo/sistema.

Medidas de seguridad internas - Recomendaciones

- Mantener los **sistemas operativos y aplicaciones actualizados**, en especial los antivirus, pues muchos de ellos ayudan a prevenir ataques de gusanos.
- Trabajar como **usuario sin privilegios, sólo utilizar el** administrador en caso de necesidad.
- Comprender y colaborar con las políticas de seguridad de red existentes.
- Siendo administrador, **no aceptar la instalación de aplicaciones desde un navegador** a menos que se tenga suficiente conocimiento de las mismas.

SPIWARE

- Software que se **instala con el consentimiento, voluntario o involuntario, del administrador** de un equipo de computación. A través de la red, frecuentemente utilizando un socket oculto al comando netstat, **transmite información** del equipo infectado a los creadores del *spyware.*

Sw Anti-spyware -medidas de seguridad internas

- Software diseñado para detectar y eliminar algunos tipos de malware.
- Se debe tener cuidado, pues muchos de ellos instalan su propio spyware.
- Se pueden configurar en diferentes niveles de advertencia y actuación.
- No son 100% confiables.

Bombas lógicas

- Programas diseñados para ejecutarse a partir de cierto evento. Por ejemplo: una fecha y hora específica, o el resultado de cierto cálculo matemático.

Bombas lógicas

- En junio de 2002, un empleado de la empresa de armamentos bélica General Dynamics, Michael Lauffenburger, fue arrestado por insertar una bomba lógica que borraría datos vitales del proyecto de un cohete. Él alegó que su plan era regresar a la compañía como un consultor altamente pagado para arreglar el problema una vez que la bomba lógica entrara en operación. Sin embargo, fue descubierto por un colega y tuvo que ir a cárcel y pagar una multa.

Troyanos

- Aparentemente inofensivos con una funcion especifica, pero…
- Tienden a tener las capacidades de una puerta trasera (backdoor), un programa que se ejecuta silenciosamente permitiendo al atacante ingresar a la computadora.

Troyanos

- Troyanos destructivos
- Troyanos de envió de datos(Badtrans.B,spyware).
- Troyanos de denegación de servicios(WinTrinoo, Amazon, CNN, Yahoo, eBay).
- Troyanos de acceso remoto(BackOrifice, Netbus, Bugbear)

Backdoors

- Un backdoor es un programa que permite al atacante accesar a un sistema, pasando por controles de seguridad

Back Orifice

- ¿Que puede hacer un Back Orifice?
  - **Permite control remoto de máquinas Windows en la red**
    - **Si logro instalarlo, soy dueño de tu máquina**
    - **Atacante controla pantalla y teclado**
- “En una LAN o a través de Internet, BO da a su usuario más control de las máquinas remotas que a la persona en frente del teclado de la máquina remota.”

Contramedidas – Back Orifice

- Eliminarlo manualmente.
- Programas especificos.
- Antivirus
- No aceptar cotroles ActiveX sin autentificar.

Windows

¿Deben instalarse controles ActiveX?

Esta información corresponde a Windows Internet Explorer 7 y Windows Internet Explorer 8.

Depende. Debe actuar con precaución a la hora de instalar controles ActiveX (también denominados complementos) en el equipo, aunque tengan una firma digital válida. Aunque los controles ActiveX pueden mejorar la exploración web, también pueden constituir un riesgo para la seguridad y es mejor evitarlos si la página web funciona bien sin ellos. Pero es posible que algunos sitios web o tareas los necesiten y, si el contenido o las tareas son importantes para usted, tendrá que decidir si instalar el control ActiveX.

Antes de instalar un control ActiveX, tenga en cuenta lo siguiente:

Mostrar todo

- ¿Estaba esperando recibir el control?
- ¿Confía en el sitio web que ofrece el control?
- ¿Sabe para qué sirve el control y lo que hará en el equipo?

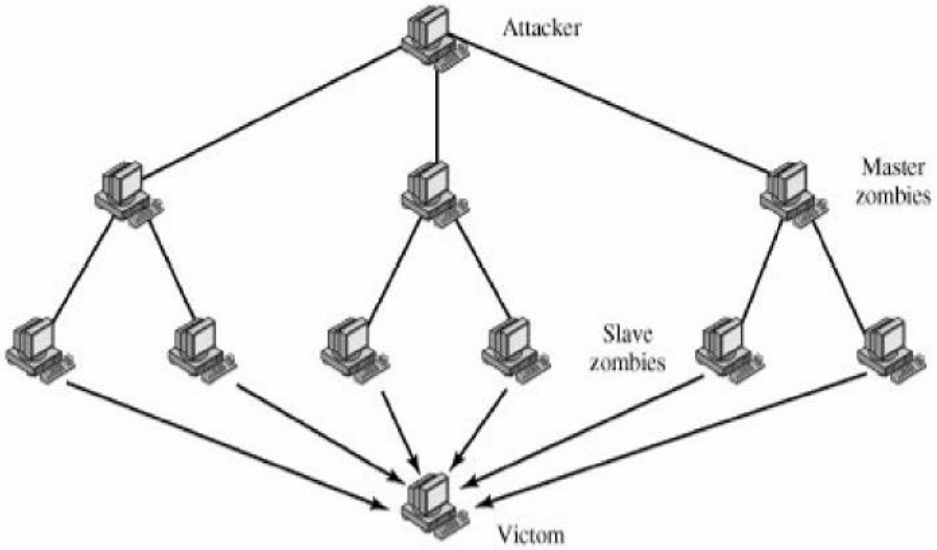
Nota

Es posible que no pueda instalar controles ActiveX si el administrador del sistema deshabilita la opción de instalarlos o si usa una cuenta de usuario estándar.

Denial Of Service - Smurf

- Ataques dirigidos con broadcast, uno de los mas comunes es llamado “smurf attacks”. Una versión mas sofisticada es PapaSmurf.
- Smurf envía llamadas de ICMP (como “ping”) haciendo un broadcast de todas las direcciones de la red. El perpetrador envía grandes cantidades de tráfico ICMP (ping) a la dirección de broadcast, todos ellos teniendo la dirección de origen cambiada (spoofing) a la dirección de la víctima.
- La máquina atacada recibe una gran cantidad de llamadas consumiendo la mayor parte de su ancho de banda.

Denial Of Service - Smurf



Defensas Smurf

- Filtrar mensajes de ICMP (en particular, responses) en el gateway: Firewall o router
- Esta “solución” puede dañar la habilidad de monitorear su red. Entonces sólo permita ICMP de host confiables
- No permita que sus routers o firewalls respondan a llamadas de broadcast
    - En Cisco IOS, “no ip directed-broadcast” por cada interface.

L0phtCrack 4

- ¿Cómo un hacker obtiene el archivo de password?
  - L0phtCrack por si mismo puede robar el archivo de passwords
  - La nueva y mejor característica de 2.5: Integración GUI-basada en sniffer
- Nuevas características
  - Integración con Sniffer
  - Mejora la velocidad (450 %)
  - Rompe todos los passwords alfanumericos en 24 horas con 450 MHz Pentium II

Password Cracking - Defensa

- **Use passwords complicados**
  - **Políticas**
  - **Herramientas para reforzar - construídas en el SO o de terceras compañías**
- **Utilizar otras formas de autentificación**
  - **Autentificación Token-based* (one-time passwords)**
  - **Autentificación Crypto-based**
  - **Infraestructura de llaves públicas.**

Hijacking

- **Herramientas que permiten al atacante:**
  - **Robar, compartir, terminar, monitorear, o registrar cualquier sesión que esté en proceso.**
- **Permite al atacante moverse a través de la red con facilidad**
- **Robar sesiones a través de la red**
- **Robar sesiones de la máquina que las está originando**
- **Transpasar todas las formas fuertes de autentificación y Redes Privadas Virtuales**

Herramientas para Apoderarse de una Sesión

- **Hunt**
  - **Nueva, muy bien diseñada**
  - **Automáticamente detecta conexiones**
  - **Permite la inserción de comandos...**
  - **O simplemente apoderarse de la sesión**
- **Juggernaut**
  - **Permite monitoreo de conexiones, inserción de comandos sencillos o apoderarse de la sesión**
  - **Menos estable al Hunt**

Herramientas para Apoderarse de una Sesión

- **TTYWatcher**
  - **Muchas características más avanzadas (registrar, robar, observar, etc.)**
  - **Corre en la máquina atacada**
  - **Interface amigable**
- **IPWatcher**
  - **Software comercial**
  - **Los crackers la piratean**
  - **Buena interface gráfica**

Defensa - Hijacking

- **Para defenderse contra ataques dirigidos a la red, se usan sesiones encriptadas y autentificación fuerte**
- **Si la máquina que manda la información es comprometida, lo anterior no sirve de mucho. ¡La información es robada al salir!**
- **Defensa:**
  - **Ser muy cuidadoso con las conexiones externas a su red**
  - **Ser aún más cuidadoso con las sesiones de administración de sus dispositivos de red**
    - **Firewalls!!! No hacer telnet al firewall**
    - **No hacer telnet al CA**
  - **Utilizar autentificación fuerte y encripción de datos para este tipo de administración**
    - **Secure Shell (ssh) o Virtual Private Network**

Daños ocasionados

6.1 CIH (1998)

- Daño estimado: 20 a 80 millones de dólares, sin contar las pérdidas producidas por la

6.2 Blaster (2003)

- Daño Estimado: 2 a 10 billones de dólares, aproximadamente cientos de miles de

6.3 Melissa (1999)

- Daño Estimado: 300 a 600 millones de dólares

6.4 Sobig.F (2003)

- Daño Estimado: De 5 a 10 billones de dólares y más c

6.5 ILOVEYOU (2000)

- Daño Estimado: 10 a 15 billones de dólares

6.6 Bagle (2004)

- Daño Estimado: 10 millones de dólares aunque continua

6.7 Code Red (2001)

- Daño Estimado: 2.6 billones de dólares

6.8 MyDoom (2004)

- Daño Estimado: Disminuyó el rendimiento de interr un 50%.
- Localización: En pocas horas del 26 de Enero de 200 transmitido vía mail enviando un supuesto mensa carpetas compartidas de usuarios de la red Kazaa.
- Curiosidades: MyDoom estaba programado para de 2004.

6.10 Sasser (2004)

- Daño Estimado: 10 millones de dólares
- Localización: 30 de Abril de 2004 fue su fecha de lanzamiento y fue suficient destructivo como para colgar algunas comunicaciones satélites de agencias francesa También consiguió cancelar vuelos de numerosas compañías aéreas.
- Curiosidades: Sasser no era transmitido vía mail y no requería usuarios para pro Cada vez que el gusano encontraba sistemas Windows 2000 y Windows Xp no actua éste era replicado. Los sistemas infectados experimentaban una gran inestabilidad.

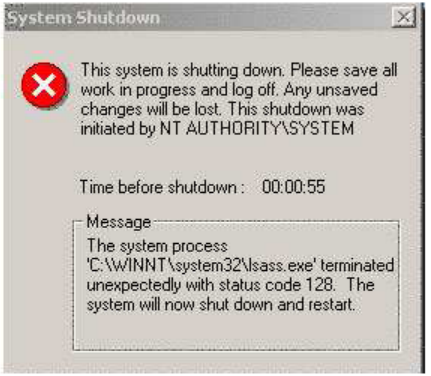


Figura 3. Virus Sasser

Recomendaciones

- "salud" informática

Encargos

- Bajar y probar herramientas de clase.