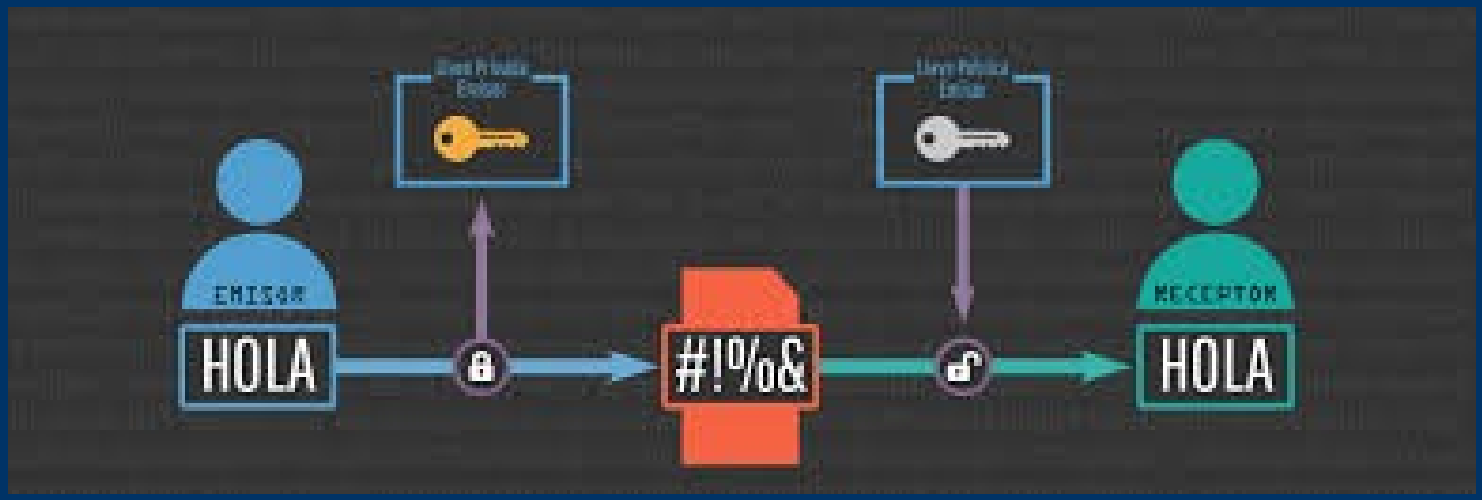
SEGURIDAD INFORMÁTICA
TEMA 1 – INTRO



ÍNDICE

- Primeros ataques
- Conceptos

INTRO

Primeros ataques

En los años 80 y 90 hubo gran aparición de hackers

Eran mentes inquietas buscando conocimiento que atacaron toda clase de sistemas

- Jhon Drape (Capitan Crunch)
- Kevin Poulsen (Dark Dante)
- Robert Morris
- Kevin Mitnick

INTRO

Primeros ataques

- Jhon Drape (Capitán Crunch)

  Con un silbato de una caja de cereales hackeó el sistema telefónico.

  Construyó un aparato que podía hacer llamadas gratuitas.

  Se llamaba blue box y era poco más que un teclado un numérico y alguna tecla más para controlar los tonos importantes para acceder a los servicios telefónicos.

INTRO

Primeros ataques

- Kevin Poulsen (Dark Dante)

  En un concurso de televisión en 1990 se hizo con el control de la centralita telefónica para asegurarse que la llamada 102 fuera suya y así ganar un porsche 944.

  Fue arrestado en 1995 acusado de siete delitos cibernéticos.

  Después trabajó para varias empresas tecnológicas para utilizar su conocimiento al servicio del bien.

INTRO

Primeros ataques

- Robert Morris

  Creó un virus que infecto a 6000 ordenadores en 1988

  El programa utilizó una vulnerabilidad en UNIX que hacía que se transmitiese a gran velocidad a otros ordenadores.

  El resultado de la infección es que la CPU se ponía al 100%

INTRO

Primeros ataques

- Kevin Mitnick (El Cóndor)

  Disfrazado de electricista entraron en las oficinas de una empresa telefónica y robaron manuales e información de seguridad.

  Tras varios delitos su abogado convenció al juez de que sufría adicción a las computadoras

INTRO

Hackers en la actualidad

- La red se ha llenado de timos y estafas

  phising, cartas nigerianas, ofertas de trabajo falsas
- La red se ha llenado de malware, hay 70 nuevas amenazas por minuto
- El malware es principalmente robo de información, botnets,

INTRO

Hackers en los gobiernos

- Los gobiernos han creado sus propios equipos de hackers y especialistas en ciberseguridad
- En china se llama el APT1
- Corea del Norte Lázarus
- Los rusos Sandworm y Turla

INTRO

Que se entiende por seguridad

- Seguridad física – no dejar pasar personas no autorizadas
- Seguridad del personal – acceso a individuos autorizados a realizar las tareas.
- Seguridad en las operaciones – organizar las tareas y como hacerlas.
- Seguridad en las comunicaciones – proteger la información transmitida
- Seguridad en las redes – protege las redes para que funcionen sin cortes
- Seguridad en la información - la confidencialidad, integridad y disponibilidad de la información.

INTRO

Objetivos de la seguridad

- Detectar, minimizar y gestionar los riesgos y amenazas
- Garantizar una utilización adecuada y autorizada

  Ejemplo: Los programas no pueden permitir una combinación de botones que hagan cosas raras.
- Limitar la extensión, alcance y posibles pérdidas en caso de un incidente de seguridad, y planificar una recuperación del sistema lo más rápida y eficiente posible.

  Ejemplo: se pierden los trabajos en el ordenador de clase y no los tenías guardados.
- Cumplir con la normativa legal vigente.

INTRO

Planos de actuación para cumplir los objetivos

- Técnico – nivel lógico y físico.

  Ejemplo: tener bien configurados los antivirus o evitar haya una intrusión física.
- Legal – leyes para tratar los datos y LOPD.
- Humano – formación y sensibilización de los empleados

  por ejemplo: alerta con email que no son de la compañia
- Organizativo – definir una forma de trabajar y buenas prácticas.

  Ejemplo: no instalar programas para uso personal en el ordenador del trabajo.

INTRO

Objetivos de la seguridad de la información

- Confidencialidad – el dato solo puede ser leído por su dueño
- Integridad - indica que un mensaje no ha sido modificado
- Disponibilidad (DDOS, Ransomware, recuperación en caso de accidente, equipos antiguos.)

¿de qué sirve una información perfectamente protegida si no puedo acceder a ella ?

INTRO

Otros conceptos

- Activo - es un recurso de la organización que debe ser protegido. Una web, documento, persona, USB….
- Ataque - acto intencionado de una persona contra un sistema de información con el fin de robar información, destruirla o ganar el control del mismo
- Amenaza – cualquier cosa que suponga un peligro
- Vulnerabilidad - debilidad o falla en un sistema o mecanismo de protección que facilita que se lleve a cabo un ataque
- Riesgo = amenaza * vulnerabilidad

INTRO

Tipos de amenazas

Ataques a la propiedad intelectual	Copia ilegal (no respetar el copyright)
Ataques vía software	Virus, ddos
Ataques a la calidad de servicio	Cortes de electricidad, ataques al ISP
Espionaje o intrusión	Acceso no autorizado
Catástrofes naturales	Fuego, terremostos...
Error humano	Fallos de los empleados
Extorsión y secuestro de la información	Publicar la información robada
Pérdidad de información	Plan de backup inadecuado
Controles inadecuados	Cortafuegos mal config.
Sabotaje	Destrucción o robo físico
Fallos hardware	Fallos en el disco duro
Fallos de software	bugs
Obsolescencia tecn.	Equipos anticuados

INTRO

Vídeo

Historia secreta de los Hackers

- https://www.youtube.com/watch?v=PqMci8R0wsw