CIBERTERRORISMO EN LA AVIACIÓN CIVIL

Antecedentes

La proliferación de computadoras conectadas a módems a principios de los 80 aumentó la vulnerabilidad de los sistemas informáticos y permitió el nacimiento de los hackers, individuos capaces de ingresar ilegalmente en las redes e incluso de alterar su contenido.

Antecedentes

Esa vulnerabilidad hizo que los organismos de inteligencia comenzaran a especular con la posibilidad de que grupos terroristas puedan cometer atentados o actos de sabotaje empleando medios telemáticos.

Para designar a esa eventual categoría de actos terroristas, se acuñó el término **CIBERTERRORISMO** (*cyberterrorism*).

Antecedentes

La hipótesis de ataques ciberterroristas se acentuó en los 90 debido a varios factores:

a) El surgimiento de Internet y su masiva penetración en la sociedad.
b) Proliferación de hackers y su capacidad afectar los sistemas informáticos.
c) La sensación de vulnerabilidad por la proximidad del milenio (Falla del Milenio / Y2K)

Definiciones

Terrorismo:

"El empleo o amenaza de violencia, un método de combate o una estrategia para lograr ciertos objetivos, con el propósito de inducir un estado de temor en la víctima que no se ajusta a las normas humanitarias y en cuya estrategia es fundamental la publicidad"

Walter Laqueur

Definiciones

Cibernética:

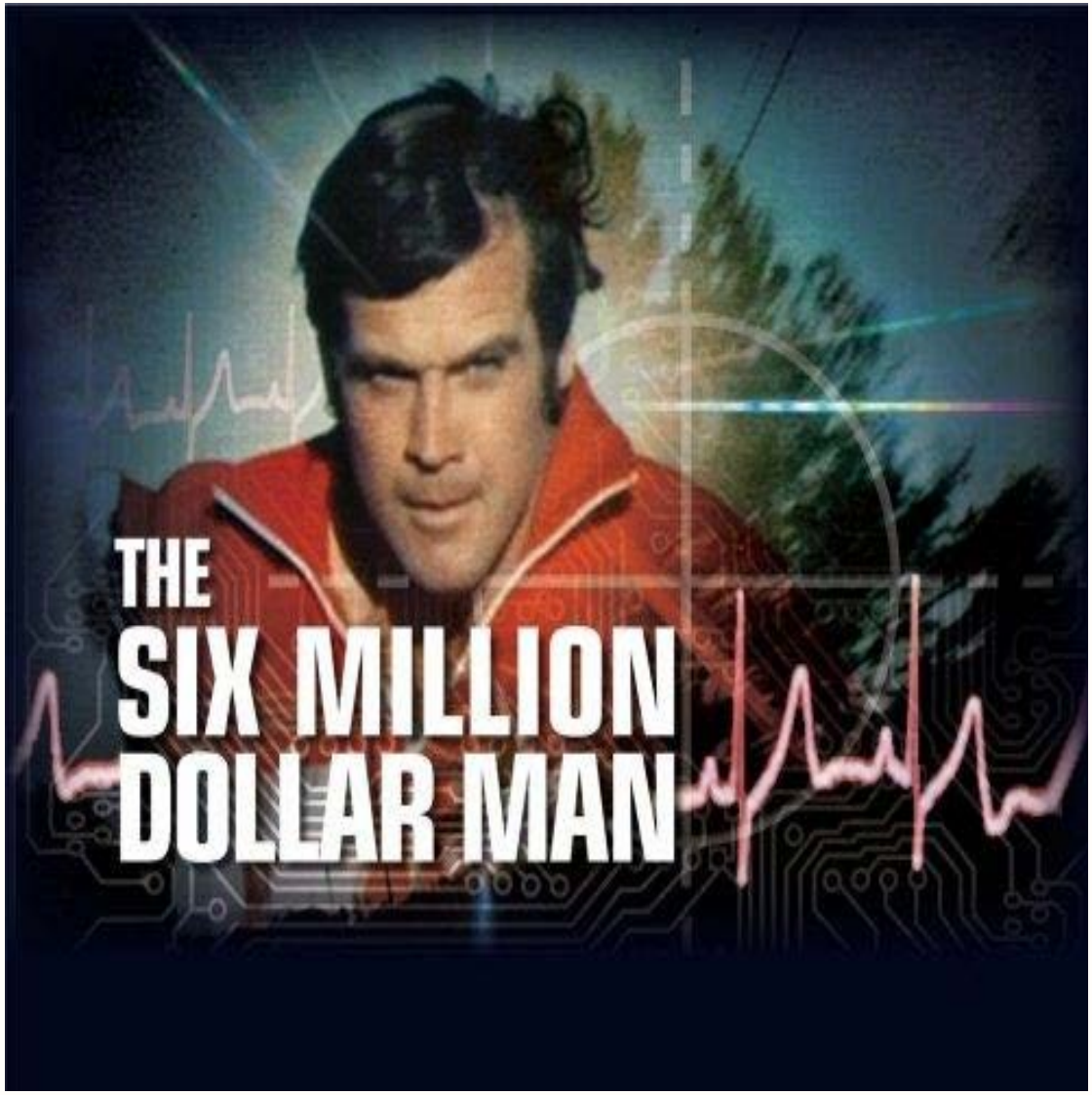
"Ciencia interdisciplinaria que trata de los sistemas de comunicación y control en los organismos vivos, las máquinas y las organizaciones"

Enciclopedia Encarta
Microsoft

Definiciones

Cibernética

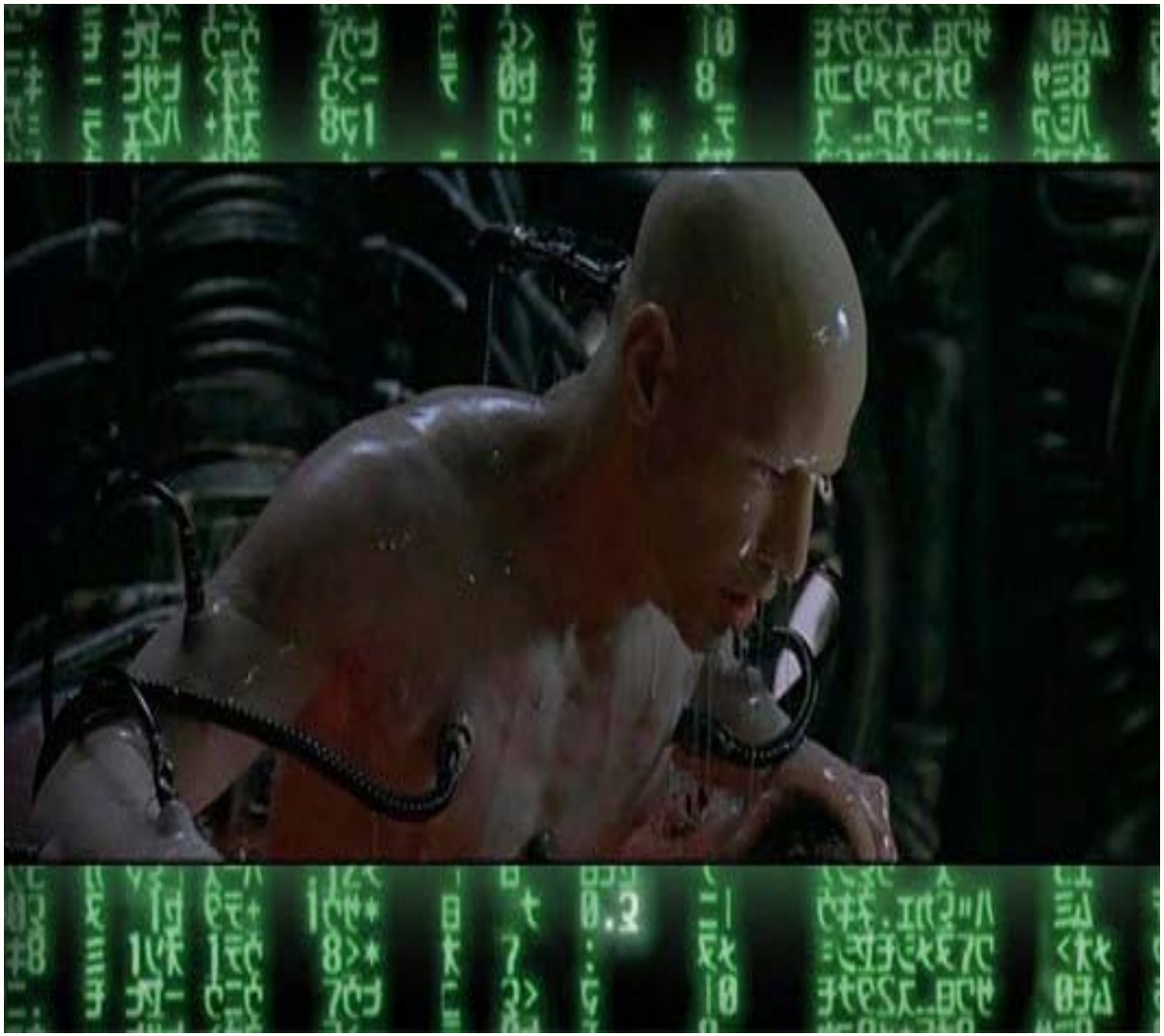
El Hombre Nuclear Años 70



Definiciones

Cibernética

MATRIX
Año 99



Ciberterrorismo:

"El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos o agentes clandestinos”

Mark Pollit
FBI

Que considerar como Ciberterrorismo

Ataques que resulten en violencia contra personas, la propiedad, o causar el daño suficiente para generar miedo.

Ataques que deriven en muertes, personas heridas, explosiones, colisiones de aviones, contaminación de agua o severas pérdidas económicas, serios ataques a la infraestructura crítica de un país, dependiendo de su impacto".

Doroty E. Denning

Universidad de Georgetown

Que considerar como Ciberterrorismo

"Los ataques que interrumpen servicios no esenciales o que son básicamente una molestia costosa **no deberían entran en esta categoría**"

Doroty E. Denning

Universidad de Georgetown

La tecnología y la aeronáutica

El entorno de la aeronáutica civil, es rápidamente cambiante en aspectos tecnológicos y sistemas de comunicación.

Los usuarios y su tecnología

Todos los usuarios de la industria están relacionados con la tecnología en menor o mayor grado.

1. Operadores de Aeronaves
2. Operadores de Aeropuertos
3. Servicios de trafico aéreo
4. Autoridad Aeronáutica
5. Prestadores de servicios en aeropuertos

Los usuarios y su tecnología

Aéreas posiblemente vulnerables.

1. Control de acceso,
2. Sistema de alarmas,
3. Sistemas de detección,
4. Sistemas de facturación, control y monitoreo de equipajes.
5. Sistemas de transito aéreo,
6. Comunicaciones,
7. Sistema de reservación de aerolíneas,
8. CCTV,
9. Sistemas de manejo de datos de la Autoridad Competente AVSEC y otros organismos

Objetivo de las medidas

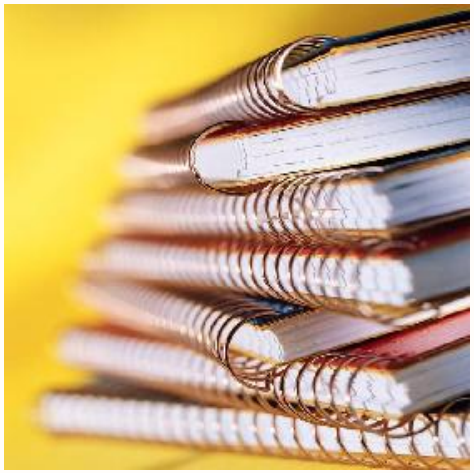
Las medidas de seguridad en los sistemas de Tecnologías de la Información y las Comunicaciones (**TIC**) en la aviación civil, deberían:

1. Proteger los sistemas contra acceso no autorizado,

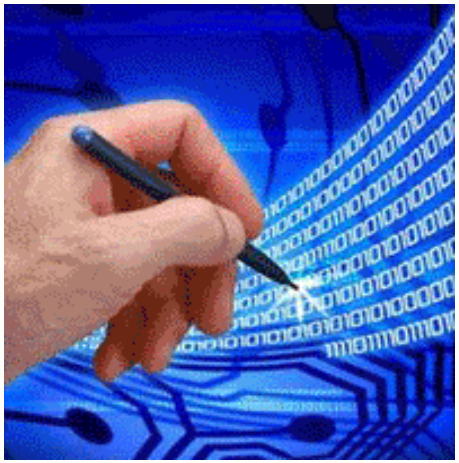
2. Evitar la alteración de los sistemas y su información, y

3. Detectar ataques a los sistemas

Medidas de seguridad



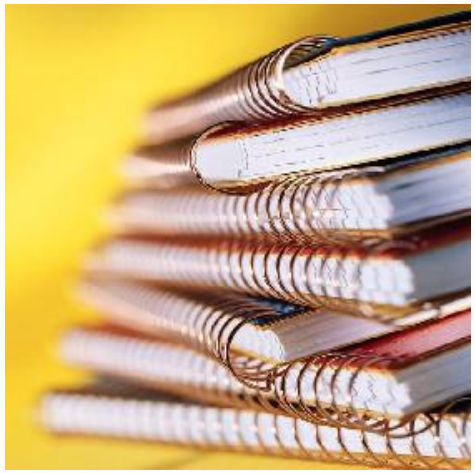
Políticas y Procedimientos



Controles virtuales

Controles físicos

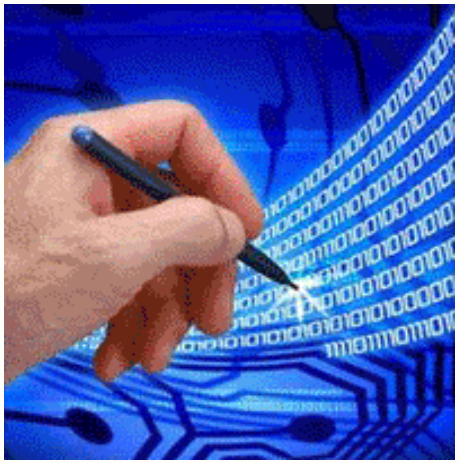
Medidas de seguridad



Políticas y Procedimientos:

1. Normas, Procedimientos, políticas.
2. Designación de responsables en la operación y supervisión TIC.
3. Evaluación de las amenazas
4. Procesos de control de la calidad.
5. Selección del Hardware.

Medidas de seguridad



Controles virtuales:

1. Sistemas de seguridad Software.
2. Cifrado de datos.
3. Sistema detección intrusos en la red.
4. Sistemas antivirus.
5. Actualización periódica.

Medidas de seguridad

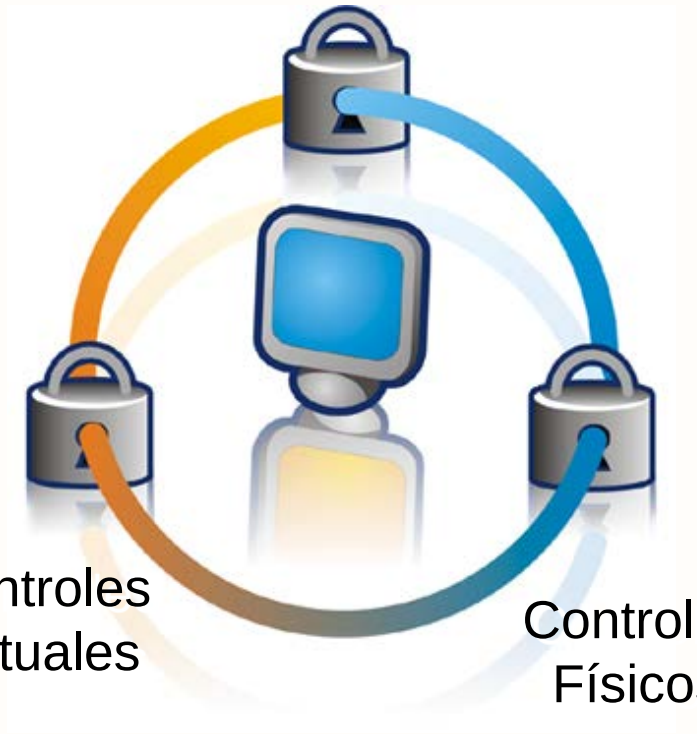
Controles físicos:

1. Zonas de acceso controlado.
2. Autentificación de acceso a los TIC.
3. Control de operarios.
4. Redundancia en las aprobaciones.
5. Copias de seguridad de los datos.
6. Utilización de redes seguras.
7. Pruebas de seguridad.

Medidas de seguridad

Plan de Continuidad del Negocio

Políticas y procedimientos



Controles Virtuales

Controles Físicos

Sistema de Gestión de la Seguridad de la Información (SGSI)

ISO / 27001:2005

(Organización Internacional de Estandarización)

Requisitos para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales de la organización

Es utilizado para la certificación

ISO / 27001:2005 Elementos Claves

Política del SGSI

Definir la política del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología para su aplicación a través de objetivos y tratamiento del riesgo

ISO / 27001:2005 Elementos Claves

Planear (Establecer el SGSI)

Establecer política, procesos y procedimientos relevantes para manejar el riesgo y la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

ISO / 27001:2005 Elementos Claves

Hacer (Implementar y operar el SGSI)

Implementar y operar la política, controles, procesos y procedimientos SGSI.

ISO / 27001:2005 Elementos Claves

Chequear (Monitorear y revisar el SGSI)

Evaluar y medir el desempeño del proceso en comparación con la política, objetivos y experiencias practicas SGSI y reportar los resultados a la gerencia para su revisión.

ISO / 27001:2005 Elementos Claves

Actuar (Mantener y mejorar el SGSI)

Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna al SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI .


Planear
Hacer
Chequear
Actuar
SGSI

Principios de seguridad en sistemas y redes de información

1. Toma de Conciencia
2. Responsabilidades
3. Respuesta
4. Evaluación del Riesgo
5. Diseño e implementación de la seguridad
6. Gestión de la Seguridad
7. Reevaluación

Conciencia

Los participantes deben estar concientes de la necesidad de los sistemas de seguridad de la información y redes y de que pueden ellos hacer para incrementar la seguridad

Responsabilidad

Todos los participantes son responsables de la seguridad de los sistemas y redes de información

Respuesta

Los participante deben actuar de manera oportuna y cooperativa para prevenir, detectar y responder a los incidentes de seguridad

Evaluación del Riesgo

Los participantes deben conducir evaluaciones del riesgo

Diseño e implementación de Seguridad

Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información y las redes

Gestión de la Seguridad

Los participante deben adoptar un enfoque amplio para la gestión de la seguridad

Reevaluación

Los participantes deben revisar y deben re-evaluar la seguridad de los sistemas de información y redes, y hacer modificaciones apropiadas a las políticas, prácticas mediciones y procedimientos de seguridad

Código para la practica de la gestión de la seguridad de la información

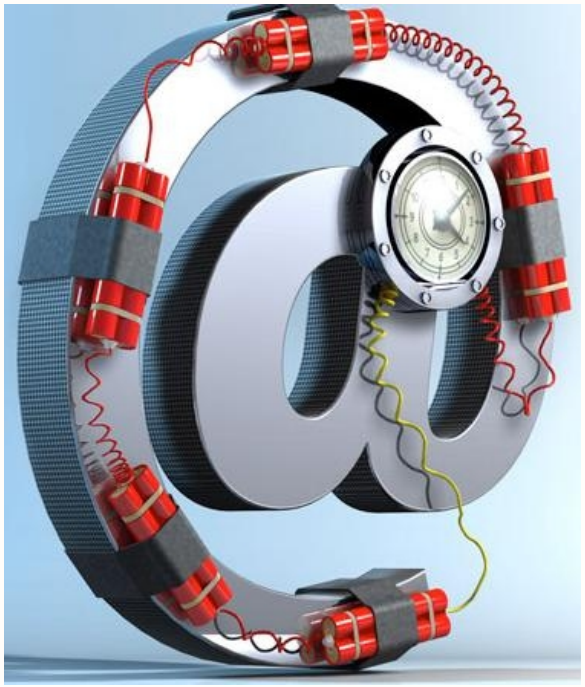
ISO/IEC 27002 (Antes 17799)

Organización Internacional de Estandarización
Comisión Electrónica Internacional

Recomendaciones para buenas prácticas. Establece los lineamientos y principios para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización

ISO/IEC 27002

1. Evaluación y tratamiento del riesgo.
2. Políticas de seguridad.
3. Organización de la seguridad.
4. Gestión de activos.
5. Seguridad de recursos humanos.
6. Seguridad física y ambiental.
7. Gestión de las comunicaciones y Operaciones.
8. Control de Acceso.
9. Adquisición, desarrollo, mantenimiento de los sistemas.
10. Gestión incidentes.
11. Gestión continuidad del negocio.



"No hay dudas, La única pregunta es cuándo. Pero un Pearl Harbor electrónico ocurrirá"

Paul A. Strassmann
Departamento de Defensa
EEUU

GRACIAS POR SU ATENCIÓN…

INAC

INSTITUTO NACIONAL DE AERONÁUTICA CIVIL

VENEZUELA