UNIVO
UNIVERSIDAD DE ORIENTE
EL SALVADOR, C.A.

Seguridad Física y Lógica en los Centros de Cómputo

AUDITORIA DE SISTEMAS COMPUTARIZADOS

Lic. Francisco D. Lovos Turcios
Contador Público – Inscripción No. 5147

UNIVO
UNIVERSIDAD DE ORIENTE
EL SALVADOR, C.A.

Contenido

Seguridad Física y Lógica en un Data Center

Existe un viejo dicho en la seguridad informática que dicta:

"Todo lo que no está permitido debe estar prohibido"

UNIVO
UNIVERSIDAD DE ORIENTE
EL SALVADOR, C.A.

Seguridad En Los Centros De Procesos De Datos

Un fallo en la seguridad de un Centro de Procesamiento de datos (CPD) podría detener las operaciones de la organización, afectando a la imagen de la empresa y del diseñador del CPD

para garantizar que los proceso y el sistema funcione y que la información está protegida se suelen agrupar en cuatro áreas

- Seguridad física
- Seguridad Lógica
- Seguridad en la red
- Control de accesos adecuados tanto físicos como los denominados lógicos.

Seguridad Física

- la Seguridad Física consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*".
- En un Data center: Se refiere a los controles y mecanismos de seguridad dentro y alrededor, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Riesgos en un Data Center

- **Las Personas:** Cuando se menciona la seguridad del centro de datos, lo más probable es que en primer lugar pensemos en sabotaje, espionaje o robo de datos. Si bien la necesidad de protección contra intrusos y el daño intencional que estos podrían causar son obvios, los peligros derivados de la actividad del personal que trabaja en el centro de datos representan un riesgo cotidiano más importante en la mayoría de Data center.

¿Quién eres y porque estas aquí?

Si bien las nuevas tecnologías de seguridad pueden parecer exóticas e inescrutables. Lectores de huellas digitales y de mano, tarjetas inteligentes, geometría facial. El objetivo de seguridad subyacente, que no cambió desde que las personas comenzaron a tener cosas para proteger, nos resulta sencillo y familiar: recibir una respuesta confiable ante la pregunta

Criterios de Acceso

- ¿Qué personas pueden acceder a qué áreas?

- Identidad personal.

- Motivo para estar allí.

- Necesidad de conocimiento.

- Importancia de la ubicación a la hora de garantizar la seguridad del centro de datos.

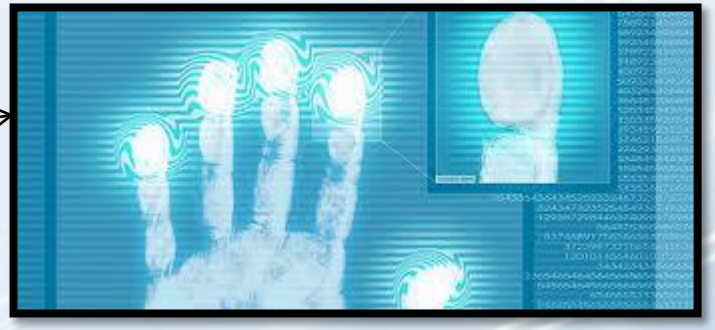
Es importantísima. Hay que pensar en la seguridad desde el punto de vista de fenómenos naturales y también seguridad propiamente dicha a nivel de atentados externos.

UNIVO
UNIVERSIDAD DE ORIENTE
EL SALVADOR, C.A.

Mecanismos de seguridad básicos en un centro de datos.

Sistemas con los que cuenta un data center:

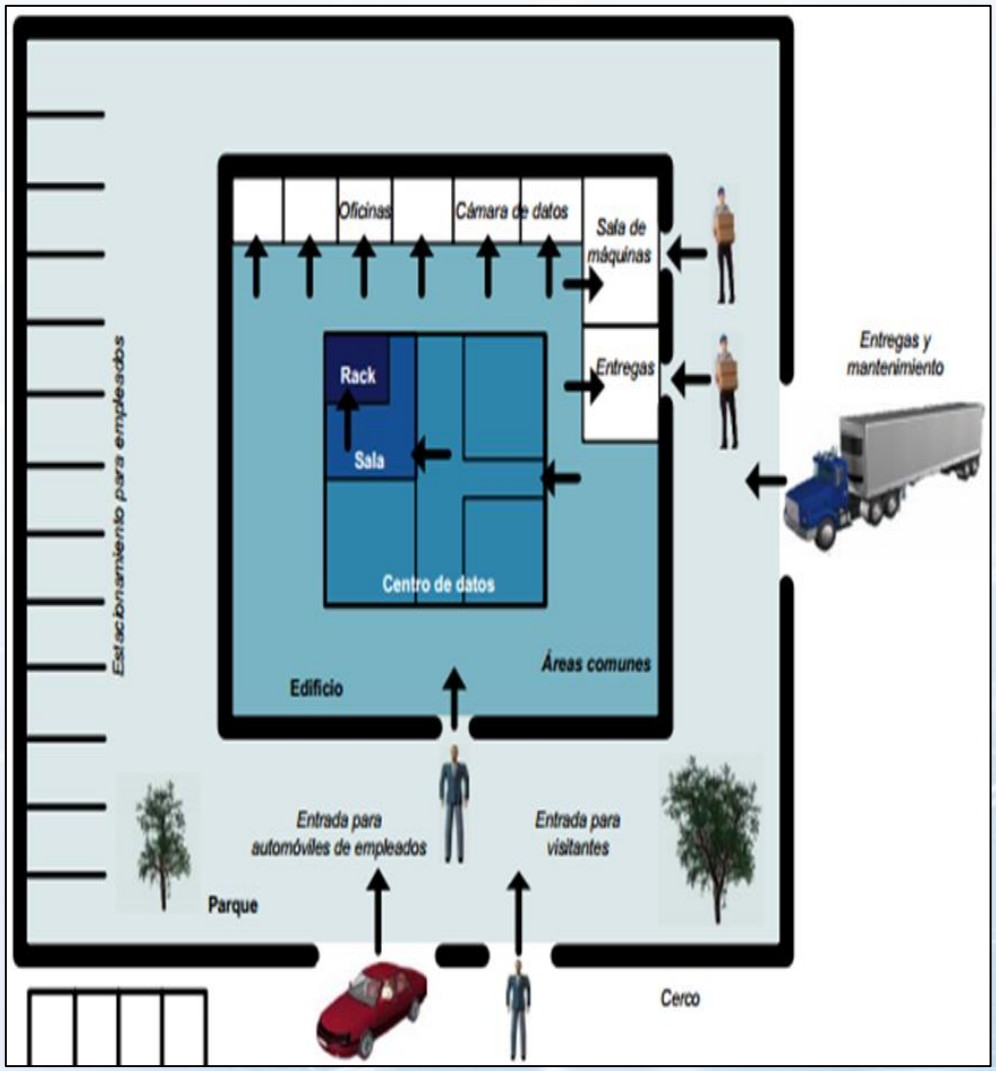
Sistema Biométrico.



Cámaras

UNIVO
UNIVERSIDAD DE ORIENTE
EL SALVADOR, C.A.

Mecanismos de seguridad básicos en un centro de datos.



Sistemas de Detección de Incendios.
Se utilizan analizadores precoces de partículas de humo, que actúan cuando comienza un posible cortocircuito y avisan al operador a través de la central de incendios del BMS.
Aparte, se colocan sistemas de extinción.

UNIVO
UNIVERSIDAD DE ORIENTE
EL SALVADOR, C.A.

Medidas que hay que tener en cuenta en caso de incendios.

- Es necesario contar con un sistema precoz de detección de humo.

- Las puertas de acceso hacia el centro de datos deben tener una resistencia al fuego RF-120 .

- Todos los componentes del interior del data center deben ser ignífugos, desde el piso falso hasta los conductores que alimentan eléctricamente los racks o los UPS.

- ¿Utilizar gases extintores o agua nebulizada?.

Medidas de seguridad en caso de inundaciones

Todo se centra en sensores que buscan identificar agua bajo el piso técnico del dataCenter.

Combinación de métodos para aumentar el grado de confiabilidad

En un esquema de seguridad típico se emplean métodos que ofrecen grados crecientes de confiabilidad, con costos también crecientes, a medida que se avanza desde las áreas de más fácil acceso ,hacia las más remotas en la estructura de seguridad.

Administración de los Sistemas de Seguridad

Proporcionan:

A

Información remota.

B

Control de dispositivos.

C

Emisión de alarmas.

¿Por qué es tan complicado?

No se cuenta con tecnología para determinar con absoluta certeza la identidad de una persona de manera rápida, sencilla y económica.

Los dispositivos de control de acceso

OFRECEN DIVERSOS GRADOS DE RENDIMIENTO COMO:

- Capacidad de reprogramación
- Resistencia a la falsificación
- Fácil interacción con las lectoras de tarjetas
- Conveniencia
- Volumen de datos que incluye
- Costo de tarjetas y lectoras

Sistemas más habituales en Control de Accesos

RFID

Lector de Proximidad

Lector Magnético

Lector Biométrico

Tabla comparativa de sistemas biométricos:

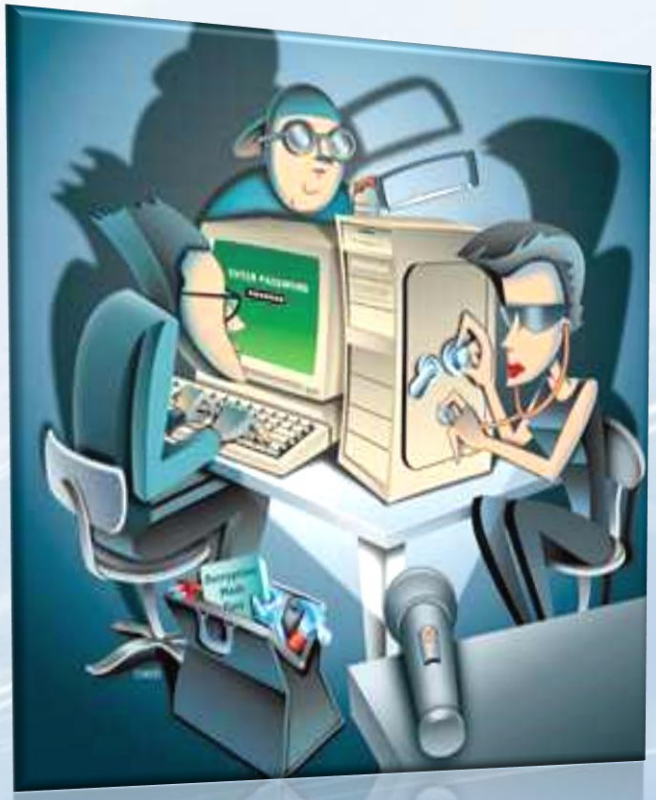
	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Geometría de la mano	Escritura y firma	Voz	Cara
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

¿QUÉ ES LA SEGURIDAD LÓGICA?

Seguridad Lógica.

Es la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

LA SEGURIDAD LÓGICA COMPLEMENTA Y SE CONTRAPONE A LA SEGURIDAD FÍSICA.



Seguridad Lógica.

La seguridad lógica involucra todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas.

Objetivos de la Seguridad Lógica

1. Restringir el acceso a los programas y archivos

2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

4. Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.

Características de la seguridad de la información.

Seguridad Lógica

Aspectos a recalcar en la seguridad lógica

La importancia de la información para la organización

La necesidad de la seguridad

La importancia de definir los activos sensibles y críticos a Proteger.

Las responsabilidades

De que se encarga la seguridad Lógica:

Controles de acceso para salvaguardar la integridad de la información almacenada.

Identificar individualmente a cada usuario y sus actividades en el sistema.

Controlar y salvaguardar la información generada.

Causantes de violaciones al acceso Lógico

Piratas informáticos (Hackers)

Personal tiempo parcial/temporal

Competencia

Ex-empleados

ASPECTOS A EVALUAR RESPECTO A LAS CONTRASEÑAS PUEDEN SER:

- ✓ Quien asigna la contraseña: Inicial y sucesivas.
- ✓ Vigencia, incluso puede haberlas de un solo uso o dependientes de una función tiempo.
- ✓ Numero de intentos que permiten al usuario
- ✓ Protección o cambios de la contraseña inícialesque llegan a los sistemas

Siempre se ha dicho que la contraseña ha de ser difícilmente imaginable por ajenos y fácilmente recordables por el propio usuario, y este último aspecto se pone en peligro cuando un mismo usuario ha de identificarse ante distinto sistemas, para lo que puede asignar una misma contraseña, lo que supone una vulnerabilidad si la protección es desigual.

La seguridad lógica tiene dos dimensiones que son:

- ✓ **La autenticación o acreditación de usuarios.**

- ✓ **El secreto de archivos y transmisiones.**

a) **Penetración externa**

Se verifican los sistemas de forma que estén protegidos frente a ataques desde fuera de la organización.

b) **Penetración interna**

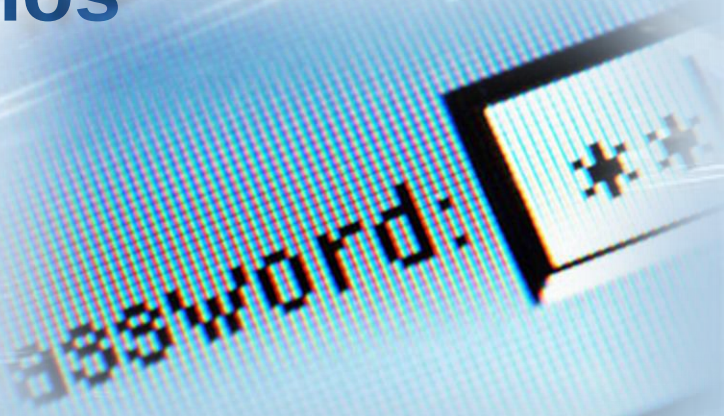
Consiste en el mismo estudio de la penetración externa, pero haciendo la suposición que el ataque procederá desde el interior de la empresa, es decir, por usuarios del sistema.

Algunas áreas de estudio que pueden formar parte de la seguridad lógica:

- ✓ *Virus*
- ✓ *Hackers*
- ✓ *Sistemas Operativos Inestables*
- ✓ *Copias de Seguridad*
- ✓ *Programas mal diseñados*.

Estandares de Seguridad

- ✓ Identificacion y Autentificacion
- ✓ Roles
- ✓ Transacciones
- ✓ Limitaciones a los servicios
- ✓ Modalidad de Acceso
- ✓ Ubicacion y Horario



RECOMENDACIONES

- Utilización de un sistema operativo relativamente seguro (NT, 2000, UNIX, Linux, etc.)
- Elección de buenos passwords (es el principal).
- Activado del protector de pantalla con password cuando el equipo queda desatendido y hacer logoff antes de retirarse del mismo.
- Utilización de un buen firewall.

“LA SEGURIDAD NO ES UN PRODUCTO, ES UN PROCESO CONSTANTE”