SEGURIDAD INFORMATICA

Lic. Walter Liali

TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

TEMARIO

- ✓ Seguridad Física
- ✓ Seguridad Administrativa
- ✓ Amenazas
- ✓ Defensas
- ✓ Administración de la Seguridad

TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

SEGURIDAD INFORMATICA

◇ Es una disciplina que tiene por objeto proteger los recursos informáticos, en especial los datos y los sistemas de información, de todo evento accidental o intencional que pueda afectar los recursos, activos o imagen institucional.

SEGURIDAD INFORMATICA

◇Los mecanismos de seguridad que se implementen:

- No deben inhibir la normal operativa de la empresa.
- Deben guardar relación con el valor del recurso o bien que se protege.

SEGURIDAD INFORMATICA

◇La seguridad no es un conjunto de medidas que se implementan de una vez y para siempre.

Es un proceso continuo donde todos, directivos, usuarios y técnicos, están involucrados permanentemente.

SEGURIDAD INFORMATICA

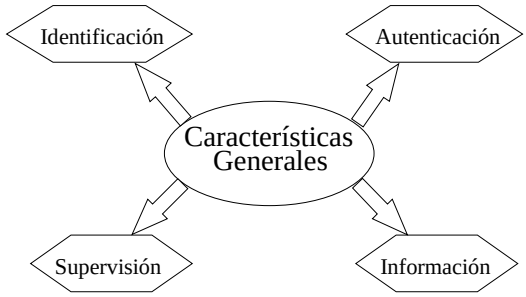
◇ Comprende:

- Seguridad Lógica.
- Seguridad Física.
- Seguridad Administrativa.

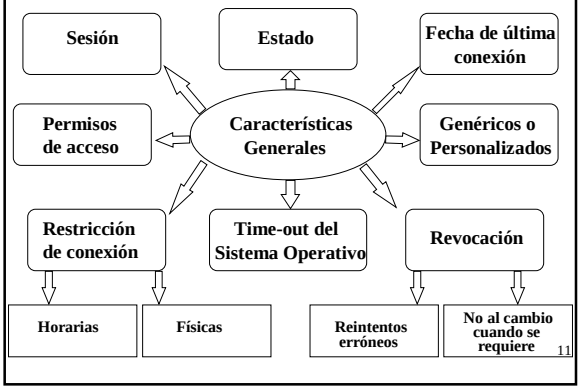
TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

SOFTWARE DE CONTROL DE ACCESO



USUARIOS

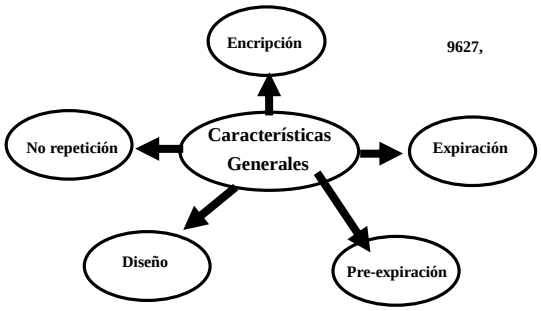


AUTENTICACION

◇ Mecanismo que permite asegurar que el usuario que se identifica ante el sistema es quien dice ser.

- Algo que el usuario sabe.
  Ej: contraseñas
- Algo que el usuario posee.
  Ej: tarjetas magnéticas / inteligentes
- Algo intrínseco del usuario.
  Ej: características biométricas

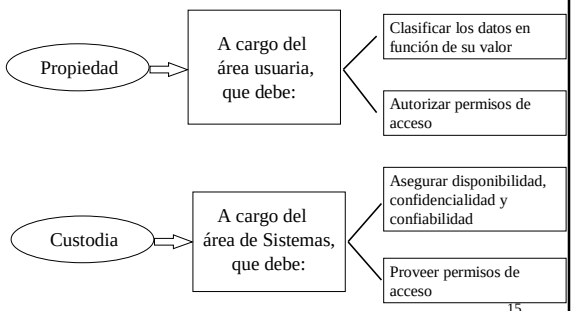
CONTRASEÑAS



TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

SEGURIDAD DE DATOS



TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

CRIPTOGRAFIA

- Es una ciencia que utiliza la Matemática para ocultar el significado de los mensajes.
- Los sistemas criptográficos más usuales se construyen con:
  - Algoritmos
    - Simétricos
    - Asimétricos
  - Funciones de Digesto Seguro (Hash)
- Implementación: software y/o hardware.

CRIPTOGRAFIA

- Algoritmos simétricos o de clave secreta
  - Utilizan la misma clave para encriptar y desencriptar.
- Características Generales
  - Longitud de clave: 40 a 168 bits.
  - Ventajas: más rápidos.
  - Desventajas: requieren compartir e intercambiar claves, repudio.
  - K= Inclusión de una clave.

CRIPTOGRAFIA

- Algoritmos asimétricos o de clave pública
  - Utilizan un par de claves relacionadas matemáticamente. Con una de ellas (llamada clave privada) encriptan y con la restante (llamada clave pública) desencriptan.
- Características Generales
  - •Longitud de clave: 512 a 4096 bits.
  - •Ventajas: no requieren compartir claves.
  - •Desventajas: más lentos (100 a 1000 veces).
  - •**Ks**= Inclusión de una clave Privada. **Kp**= Inclusión de una clave Publica.

CRIPTOGRAFIA

- Funciones de Digesto Seguro (Hash)

Transforman un texto en un valor de longitud fija llamado Digesto, tal que es imposible:

- Reconstituir el texto a partir del Digesto.
- Encontrar otro texto diferente que produzca el mismo Digesto.
- Longitud del digesto: 128 a 256 bits según la función utilizada.

CRIPTOGRAFIA

- Los sistemas criptográficos brindan soluciones como:

•*Control de Acceso:* para que solo los usuarios autorizados puedan acceder a los sistemas de información.

•*Confidencialidad:* de la información archivada o transportada en canales de datos, voz o video.

•*Autenticación:* de las partes en comunicación, de modo que cada una tenga certeza de la identidad de la otra.

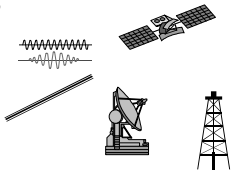
•*Firma Digital:* para la autenticación y el control de integridad de datos transmitidos o almacenados.

TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones ⇐
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

SEGURIDAD DE LAS COMUNICACIONES

- Medios de comunicaciones
  - Por cable
    - Telefónico
    - Par trenzado
    - Coaxil
    - Fibra óptica_
  - Por aire a través de:
    - Rayos láser
    - Rayos infrarrojos
    - Radio de microondas (enlace terrestre, "antena - antena")
    - Radio de microondas (enlace satelital, "antena - satélite - antena")



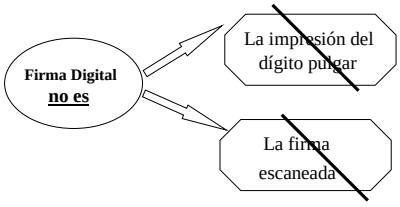
SEGURIDAD DE LAS COMUNICACIONES

- Poseen diferentes niveles de seguridad, pero en general son vulnerables. Es decir la información transmitida puede ser leída y en algunos casos modificada.
- Un medio de comunicación se dice que es seguro o está protegido cuando los datos se transmiten encriptados.

TEMARIO

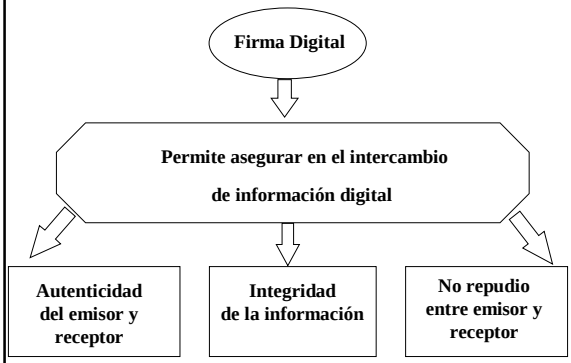
- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

FIRMA DIGITAL



FIRMA DIGITAL

- ◆Es el resultado de un cálculo que se realiza sobre el texto original.
- ◆En el cálculo están involucrados el texto y la clave privada del emisor.
- ◆El resultado se agrega al texto original.



CERTIFICADOS DE CLAVE PUBLICA

- ◇ Documento digital, emitido y firmado digitalmente por una Autoridad Certificante, que asocia una clave pública con su suscriptor. Contiene, como mínimo, los siguientes datos:
  - Nombre del suscriptor.
  - Su clave pública.
  - Período de vigencia.
  - Nombre de la Autoridad Certificante.

LEGISLACION

- **En varios países ya existe legislación que regula el uso de la Firma Digital.**

  Ley modelo de Naciones Unidas, Directivas de la Comisión Europea, Alemania, Francia, Hong Kong, Perú, Estados Unidos de América.

- **En nuestro país, distintas resoluciones de organismos públicos incorporan y autorizan el uso de esta tecnología en el ámbito de la Administración Pública:**
  - Resolución 45/97 de la Secretaría de la Función Pública.
  - Decreto Presidencial 427/98.
  - Actualmente hay distintos proyectos de ley en el Parlamento:
    - . Proyecto Legisladores Del Piero y Molinari Romero.
    - . Proyecto de la Jefatura de Gabinete de Ministros.
    - . CERTISUR S.A:

COMERCIO ELECTRONICO

◇ Se desarrollaron protocolos que utilizan criptografía de clave pública para realizar transacciones electrónicas seguras a través de redes públicas como Internet.

COMERCIO ELECTRONICO

◇ SSL (Secure Sockets Layer)
- Certificados de clave pública.
- Permite la autenticación entre un servidor web y el cliente.
- Establece una conexión segura entre ambos.
- Utilizados por los navegadores de Internet como Navigator y Explorer.

◇ SET (Secure Electronic Transaction)
- Firma Digital.
- Utilizados por Visa y Mastercard para compras con tarjetas de crédito.

◇ SEC (Secure Electronic Commerce)
- Optimización de SET.

COMERCIO ELECTRONICO

◇ Proyección de usuarios y compras con tarjeta de crédito por Internet.

	1997	2000
Usuarios	64 millones	370 millones
Us. T. Crédito	1 %	60 %
Pesos	500 millones	30.000 millones

COMERCIO ELECTRONICO

◇ Bancos en Internet

• Los Bancos brindan servicios a través de Internet entre sus opciones de atención.

• Existen “Bancos Virtuales” que solo operan a través de Internet

Security First Network Bank (SFNB).
- Opera desde Octubre de 1995.
- Realiza Servicios bancarios completos.
- Netscape, SSL y Firma Digital.

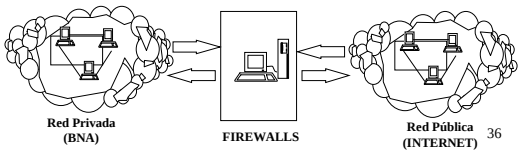
TEMARIO

FIREWALLS

◇ Son sistemas que permiten controlar:

• Que recursos de la red privada pueden ser accedidos desde el mundo exterior.

• Que recursos externos pueden ser accedidos por usuarios internos.



TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos ⇐
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

VIRUS INFORMATICOS

◆ Son pequeños programas que se instalan en la memoria de la computadora, generalmente con el objeto de reproducirse e interferir en el normal funcionamiento del equipo.

Circular 9677

- Clases de virus
  - De booteo: se alojan en el área de arranque de la PC.
  - De archivos ejecutables: se alojan en archivos .EXE, .COM.
  - De macros: se alojan en planillas de cálculo, documentos .

VIRUS INFORMATICOS

- Características principales
  - Subrepticios.
  - Autorreproductores.
  - Dañinos.
- Modo de infección
  - A través de redes o disquetes.
- Formas de ataque
  - Vandalismo indiscriminado.
  - Sabotaje contra una operatoria específica.
  - Sabotaje corporativo.

VIRUS INFORMATICOS

- Síntomas
  - La PC funciona lentamente o deja de funcionar, sin motivos aparentes.
  - Se enciende la luz de la disquetera como si estuviese en funcionamiento.
  - Disminución brusca y no justificada de espacio libre en el disco rígido.
  - Aparición de programas residentes que no fueron instalados por el usuario.
- Consecuencias
  - Leves a muy graves.
- Defensas
  - Políticas y software antivirus.

VIRUS INFORMATICOS

Pérdidas provocadas por virus
e Intrusos informáticos en EE.UU.
(millones de U$S)

	1995	1996	1er.sem.1999
Intrusión	1.000	5.000	
Virus	1.000	6.000	7.600

TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal ⇐
  - Respaldos de Seguridad
  - Contingencias

SOFTWARE LEGAL

- Ley 11.723 de "Propiedad Intelectual".
- El Decreto 165/94 y la Ley 25036 promulgada en Noviembre '98 incluyen al software dentro del alcance de la Ley 11.723, al considerarlo una obra intelectual.
- La reproducción de software, a través de cualquier medio, que no cuente con la expresa autorización del autor constituye un delito.

TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

RESPALDOS DE SEGURIDAD

Backups

- De equipos

- De archivos

- Acceso restringido
- Disponibilidad
- Apartado del computador
- Identificado

TEMARIO

- ✓ Introducción
- ✓ Seguridad Lógica
  - Software de Control de Acceso
  - Seguridad de Datos
  - Criptografía
  - Seguridad de las Comunicaciones
  - Firma Digital
  - Firewalls
  - Virus Informáticos
  - Software Legal
  - Respaldos de Seguridad
  - Contingencias

CONTINGENCIAS

◊Son interrupciones no planificadas del procesamiento de datos. Si la contingencia involucra al Computador Central y se prolonga en el tiempo es llamada "Desastre".

◊ Afectan la normal operativa del sistema de la empresa.

◊No pueden ser corregidas a través de los procedimientos normales.

◊e deben confeccionar procedimientos alternativos para mantener operativas las funciones vitales de la empresa, llamados "Planes de Contingencia o de Recuperación de Desastre".

TEMARIO

- ✓ Seguridad Física
- ✓ Seguridad Administrativa
- ✓ Amenazas
- ✓ Defensas
- ✓ Administración de la Seguridad

SEGURIDAD FISICA

- Controles de acceso
- Racks
- Depósito de archivos de respaldo
- Archivo de la documentación
- Controles ambientales
- Limpieza




TEMARIO

- ✓ Seguridad Física
- ✓ Seguridad Administrativa
- ✓ Amenazas
- ✓ Defensas
- ✓ Administración de la Seguridad

SEGURIDAD ADMINISTRATIVA

◇ Son procedimientos administrativos que complementan las medidas de seguridad lógica y física:

- Uso del correo electrónico.
- Permiso o nivel de acceso otorgado.
- Diseño y confidencialidad de la contraseña.
- La contraseña y la firma hológrafa.
- Recepción de usuarios.
- Control de usuarios.
- Identificación del personal de mantenimiento técnico.
- Registro de novedades.

TEMARIO

- ✓ Seguridad Física
- ✓ Seguridad Administrativa
- ✓ Amenazas
- ✓ Defensas
- ✓ Administración de la Seguridad

AMENAZAS

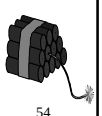
◆ Ocurrencia potencial de incidentes que afectan los recursos, activos o imagen institucional.

◆La Tecnología Informática representa nuevas oportunidades y riesgos. Cada avance tecnológico se convierte inevitablemente en un objetivo para aquellos que buscan aprovecharse de sus debilidades para lograr sus propósitos.

AMENAZAS

❖ Tipos de daños:

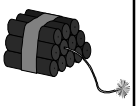
- ◆ Robo, uso indebido o alteración maliciosa de datos sensitivos.
- ◆ Robo, uso no autorizado o destrucción de hardware o software.
- ◆ Utilizar la identidad de usuarios legítimos y ejecutar actividades dañinas bajo nombre supuesto.
- ◆ Denegación o degradación del servicio.
- ◆ Robo de activos.



AMENAZAS

❖ Tipos de ocurrencia:

- ◆ No Intencionales
  - • Errores de las personas por accidente o negligencia.
  - • Mal funcionamiento del hardware o software.
  - • Acontecimientos naturales.
- ◆ Intencionales
  - • Empleados.
  - • Personas externas a la empresa.



VULNERABILIDADES

◆ Debilidades de los sistemas informáticos que hacen posible que las amenazas ocurran.

◆ Las amenazas se minimizan identificando y eliminando las vulnerabilidades.

– Existen vulnerabilidades a nivel de:
- • Hardware
- • Software
- • Datos
- • Personas

FRAUDE INFORMÁTICO

◆ Abarca una amplia gama de delitos en los que el perpetrador se aprovecha intencionalmente de las vulnerabilidades de los sistemas informáticos.

◆ Los ataques, cuando son exitosos, hacen que las amenazas preexistentes ocurran. Estos son motivados por interés:
- • Comercial
- • Financiero
- • De hacer daño
- • De entretenimiento

LEGISLACION

◆ Varios países ya han modificado su legislación incorporando las diversas modalidades delictivas que plantean las nuevas tecnologías.

◆ En Argentina existen varios proyectos de reforma del Código Penal en materia de delitos informáticos, ninguno ha recibido tratamiento legislativo.

TEMARIO

- ✓ Seguridad Física
- ✓ Seguridad Administrativa
- ✓ Amenazas
- ✓ Defensas ⇦
- ✓ Administración de la Seguridad

DEFENSAS

◇ Conjunto de técnicas utilizadas para proteger a los sistemas informáticos. Se valen de:

- ◆ Análisis de Riesgos
- ◆ Políticas de Seguridad
- ◆ Normas y Procedimientos
- ◆ Capacitación y Entrenamiento
- ◆ Controles

ANALISIS DE RIESGOS

◇ La empresa debe evaluar, en forma permanente, los expuestos de seguridad.

- ◆ Identificando y evaluando riesgos
- ◆ Promoviendo acciones de seguridad:
  - Lógica
  - Física
  - Administrativa
  - Operativa

61

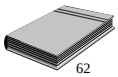
POLITICAS DE SEGURIDAD

➔Directivas generales de cumplimiento obligatorio.

➔ Independientes de las plataformas.

➔ Generalmente están vigentes por varios años.

Actualmente en implementación.



62

NORMAS Y PROCEDIMIENTOS

➔ Directivas específicas de cumplimiento obligatorio.

➔ Dependientes de cada plataforma.

➔ Necesitan ser modificadas más frecuentemente.

63

CAPACITACION Y ENTRENAMIENTO

📖 En el uso de sistemas informáticos, en especial en temas de seguridad.

64

CONTROLES

◆ Es el medio más importante para reducir el impacto de las amenazas sobre los recursos, activos y prestigio del Banco.

◆ Estos son implementados en puntos donde el riesgo es más alto, para disminuir la probabilidad de que ese riesgo se convierta en pérdida.

65

CONTROLES

Tipos

◇ Control Preventivo

Ejemplo: Control de acceso, políticas, capacitación.

◇ Control de Detección

Ejemplo: Logs de auditoria, listado de usuarios.

◇ Control de Corrección

Ejemplo: Eliminación de virus

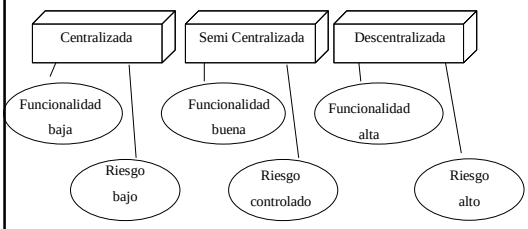
66

TEMARIO

- ✓ Seguridad Física
- ✓ Seguridad Administrativa
- ✓ Amenazas
- ✓ Defensas
- ✓ Administración de la Seguridad

ADMINISTRACION DE LA SEGURIDAD

La administración y control de los recursos relacionados con la seguridad de los sistemas de informáticos puede ser:



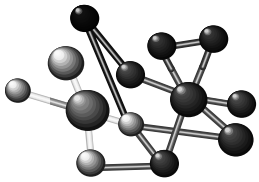
ADMINISTRACION DE LA SEGURIDAD

- **Plataforma de Host (plataforma cerrada):** Con administración de seguridad centralizada.
- **Plataforma de Redes (plataforma abierta):** Según el tamaño de la red se planificara la administración.

ADMINISTRACION DE LA SEGURIDAD

Debemos tomar CONCIENCIA que:

La seguridad en una Organización se logra con la participación activa de todos y cada uno de los usuarios de los sistemas informáticos.



Gracias por su atención.