Seguridad y Privacidad en redes

Docentes:

Lic. Paula Venosa

Lic Nicolás Macia

Presentación de la materia

- Objetivos en la carrera
- Contenido
- Cronograma
- Forma de aprobación
- Bibliografía
- Herramientas

Contenidos de la materia

- Conceptos básicos de seguridad y terminología relacionada
- Legislación nacional relacionada.
- Criptografía y sus aplicaciones (Firma digital, PGP, Esteganografía)
- Amenazas: Técnicas de descubrimiento, scanning, sniffing, etc
- Vulnerabilidades de los sistemas – Ataques. Seguridad de aplicaciones WEB
- Mecanismos de protección: Firewalls, IDS y honeypots
- Gestión de seguridad de la información: Serie ISO 27000

Motivación de la materia

- Resulta importante entender la razón por la cual la seguridad es una consideración importante cuando se diseña y se administra redes y cuando se desarrollan sistemas.
- Es necesario:
  - Examinar las amenazas de seguridad existentes en las redes y sistemas.
  - Saber de qué manera incorporar servicios y mecanismos de seguridad frente a las amenazas existentes.

Qué rol juega nuestra materia

- En primer lugar comprender algunos conceptos/terminología básica relacionada con la seguridad. (Amenaza, ataque, vulnerabilidad….).
- Analizar distintas herramientas a fin de comprender: riesgos existentes, cómo descubrir vulnerabilidades y cómo analizar la seguridad de la red y de las aplicaciones.
- Estudiar normas, mecanismos, protocolos y herramientas que pueden ayudar a proteger a la organización, a sus redes y las aplicaciones que en ellas residen .

Clase 1

- Terminología: Información, seguridad, privacidad, confidencialidad,Integridad,Disponibilidad, Autenticidad y No repudio. Amenazas. Incidentes.
- Amenazas:
  - Amenazas sobre las personas
  - Amenazas sobre la información
  - Amenazas sobre el hardware
- Contramedidas:

Concientización en seguridad de la información.

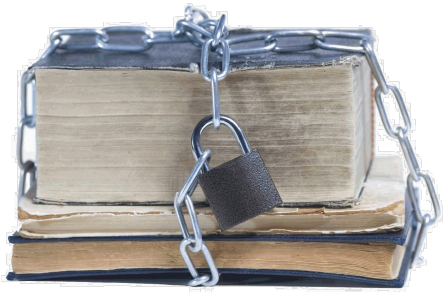
Definiciones

- ¿Qué se debe asegurar?
  - Los activos de una organización

- ¿Cuál es el lugar que ocupa la información?
  - La información constituye un activo muy importante para la organización, ya que tiene un rol fundamental a la hora de cumplir sus objetivos

Debemos proteger la información adecuadamente garantizando su seguridad y privacidad

Seguridad y privacidad de la información



- ¿Qué es seguridad de la información?
  - Significa proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción **no autorizados.**

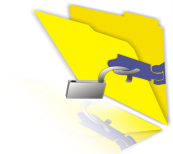
- ¿Qué es la privacidad de la información?
  - Significa **no revelar** la información o revelarla selectivamente de manera de protegerla de cualquier intromisión

Atributos de la información ¿Qué se debe garantizar?

- Confidencialidad: Garantiza que la información sólo sea accesible por las personas autorizadas.

- Integridad: Garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo

- Disponibilidad: Garantiza que los usuarios autorizados tienen acceso a la información y recursos relacionados cuando lo necesiten.



Atributos de la información ¿Qué se debe garantizar?

- Autenticidad: Garantiza que la persona que origina o recibe el mensaje es quien dice ser.

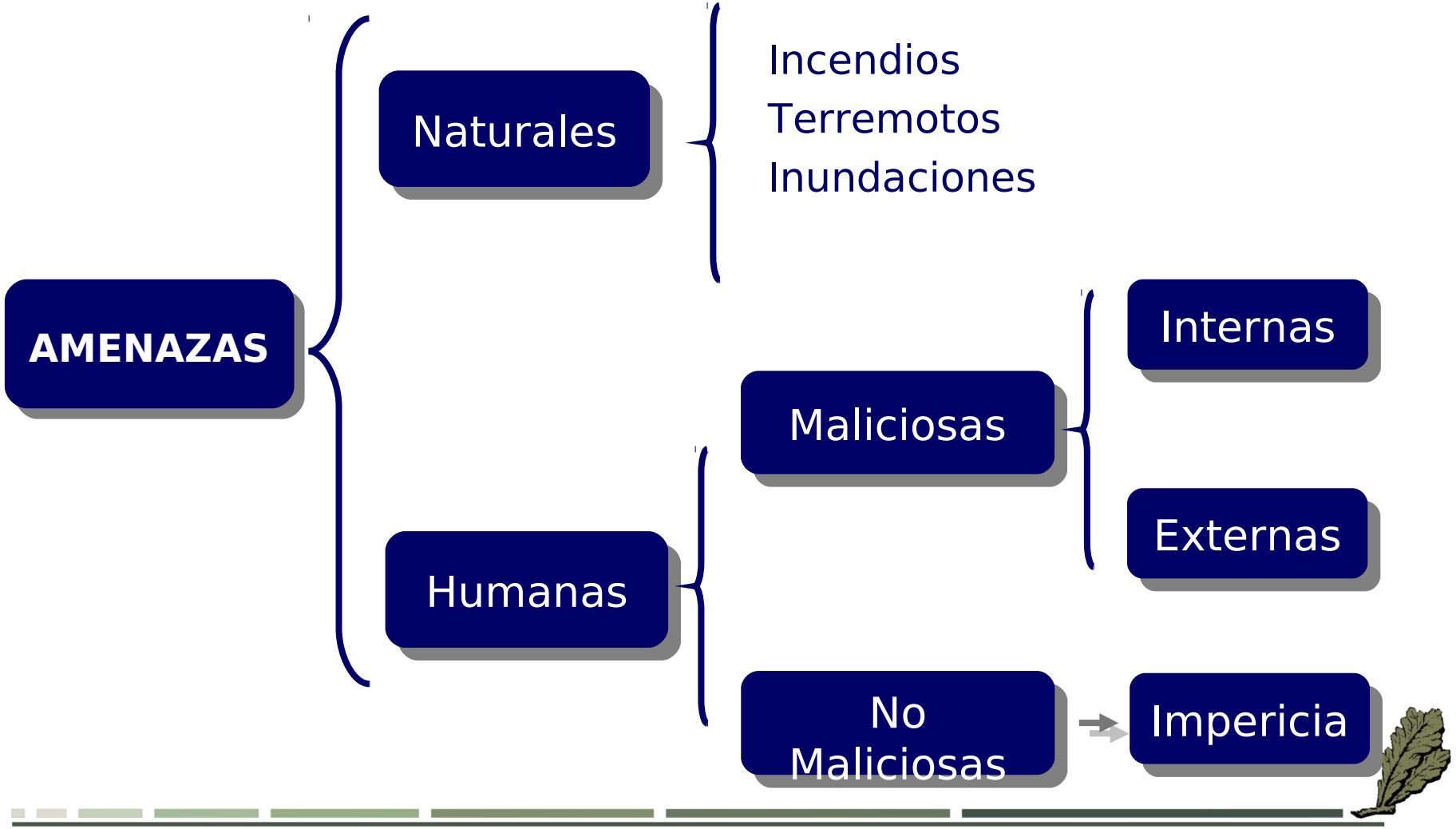
- No repudio: Garantiza que la persona que envió o recibió el mensaje no pueda negar haberlo hecho

Vulnerabilidades y Amenazas

- Una ***vulnerabilidad*** es una debilidad en un activo.
- Una ***amenaza*** es una violación potencial de la seguridad.

Las amenazas sacan ventaja de las vulnerabilidades.

Tipos de amenazas



¿Por qué Aumentan las Amenazas?

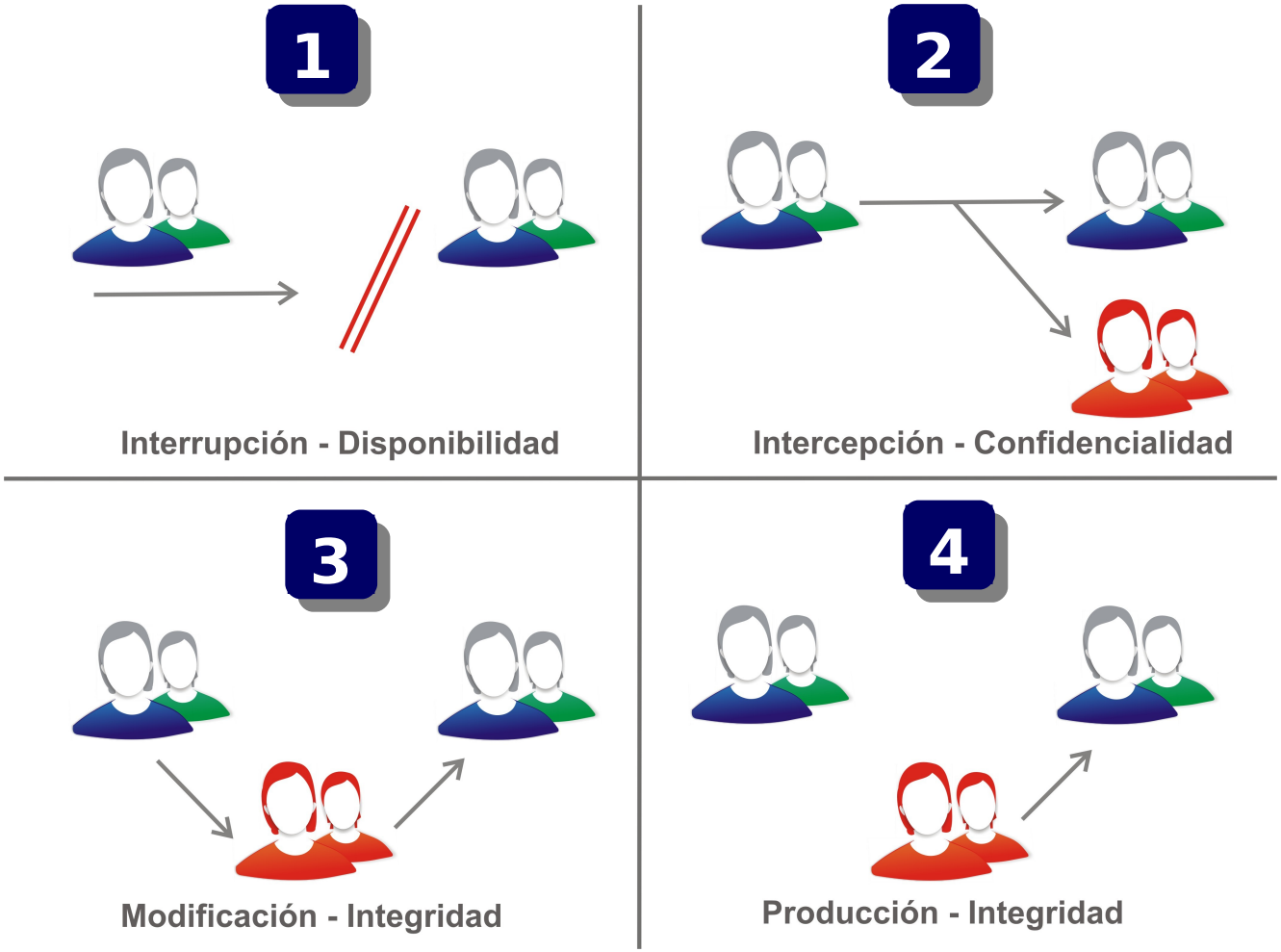
- Mayor dependencia de los Sistemas, Servicios de Información y de tecnologías asociadas.
- Crecimiento exponencial de las Redes y Usuarios Interconectados
- Proliferación de las Bases de Datos en-línea
- Alta disponibilidad de Herramientas Automatizadas para Ataques a la Seguridad
- Nuevas Técnicas de Ataque Distribuido (Ej:DoS)
- Falta o insuficiencia de capacitación
- Rentabilidad de los ataques

Incidente de seguridad

Un incidente de seguridad, es un evento adverso que afecta los activos de la organización

Todo incidente detectado debe ser reportado ante quien corresponda

Algunos Incidentes



Amenazas

- Conceptos generales
- Amenazas sobre las personas
- Amenazas sobre el hardware

Más adelante, retomaremos amenazas:

- Amenazas sobre el software
- Amenazas sobre las redes y los servicios

Amenazas - Conceptos Generales

Las amenazas atentan contra:

- La confidencialidad de la información
- La integridad de la información
- La disponibilidad de la información

Estan son causadas por (de ahí su clasificación mencionada previamente):

- fallas humanas
- ataques malintencionados
- catástrofes naturales

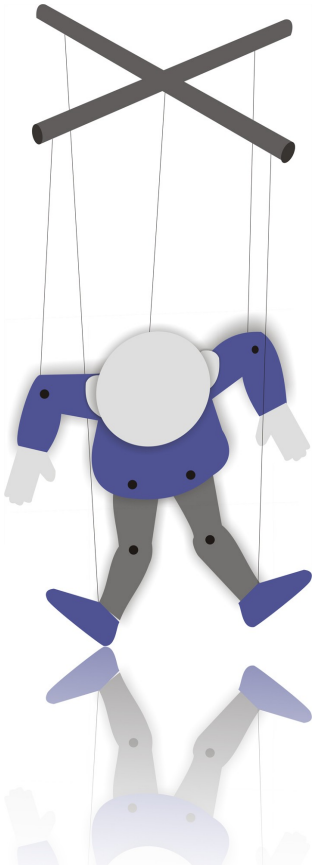
Amenazas - Conceptos Generales

La materialización de una amenaza puede causar:

- el acceso, robo, modificación o eliminación de información no autorizada
- la interrupción de un servicio o el procesamiento de un sistema;
- daños físicos o robo del equipamiento y medios de almacenamiento de información.

Amenazas sobre las personas
Ingeniería social

La **ingeniería social** es un conjunto de trucos, engaños o artimañas que permiten confundir a una persona para que entregue información confidencial



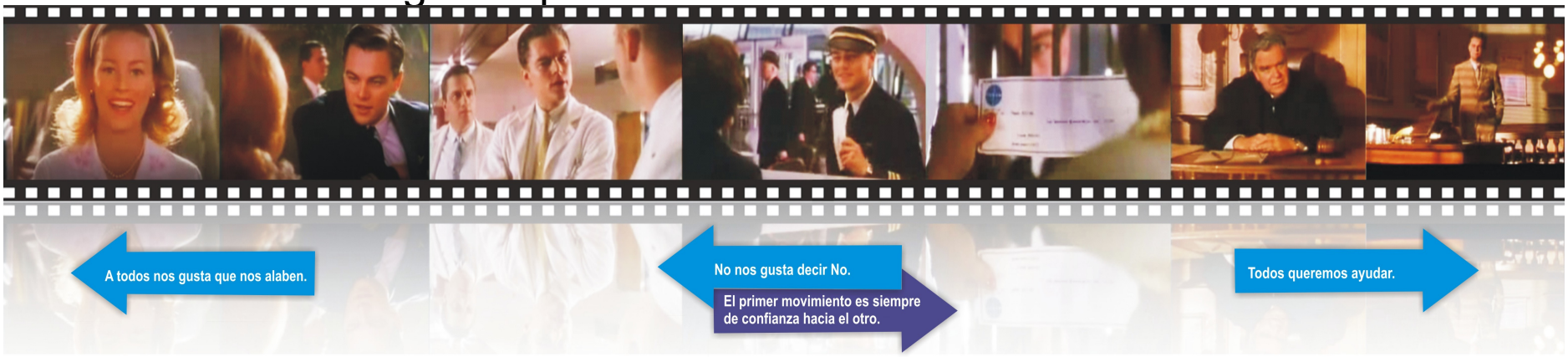
La principal defensa contra la ingeniería social es concientizarnos en el uso de políticas de seguridad

Amenazas sobre las personas
Ingeniería social

¿Por qué funciona?

Según Kevin Mitnick, uno de los ingenieros sociales más famosos de los últimos tiempos, la ingeniería social se basa en estos cuatro principios:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir “No”.
- A todos nos gusta que nos alaben.



Amenazas sobre las personas
Ingeniería social

"La Seguridad muchas veces es una mera Ilusión. Una compañía puede tener la mejor tecnología, firewalls, sistemas de detección de intrusos, dispositivos de autenticación avanzados como tarjetas biométricas, etc y creen que están asegurados 100%. Viven una Ilusión. Sólo se necesita un llamado telefónico y listo. Ya son vulnerables a un ataque. La Seguridad no es un producto, es un Proceso"

Kevin Mitnik

Amenazas sobre las personas
Phishing y pharming

El **Phishing** es una combinación de ingeniería social y elementos técnicos para engañar a un usuario y lograr que éste entregue involuntariamente información confidencial a usuarios malintencionados

La forma más común es mediante el envío de mails falsos, escritos como si hubieran sido enviados por la auténtica organización

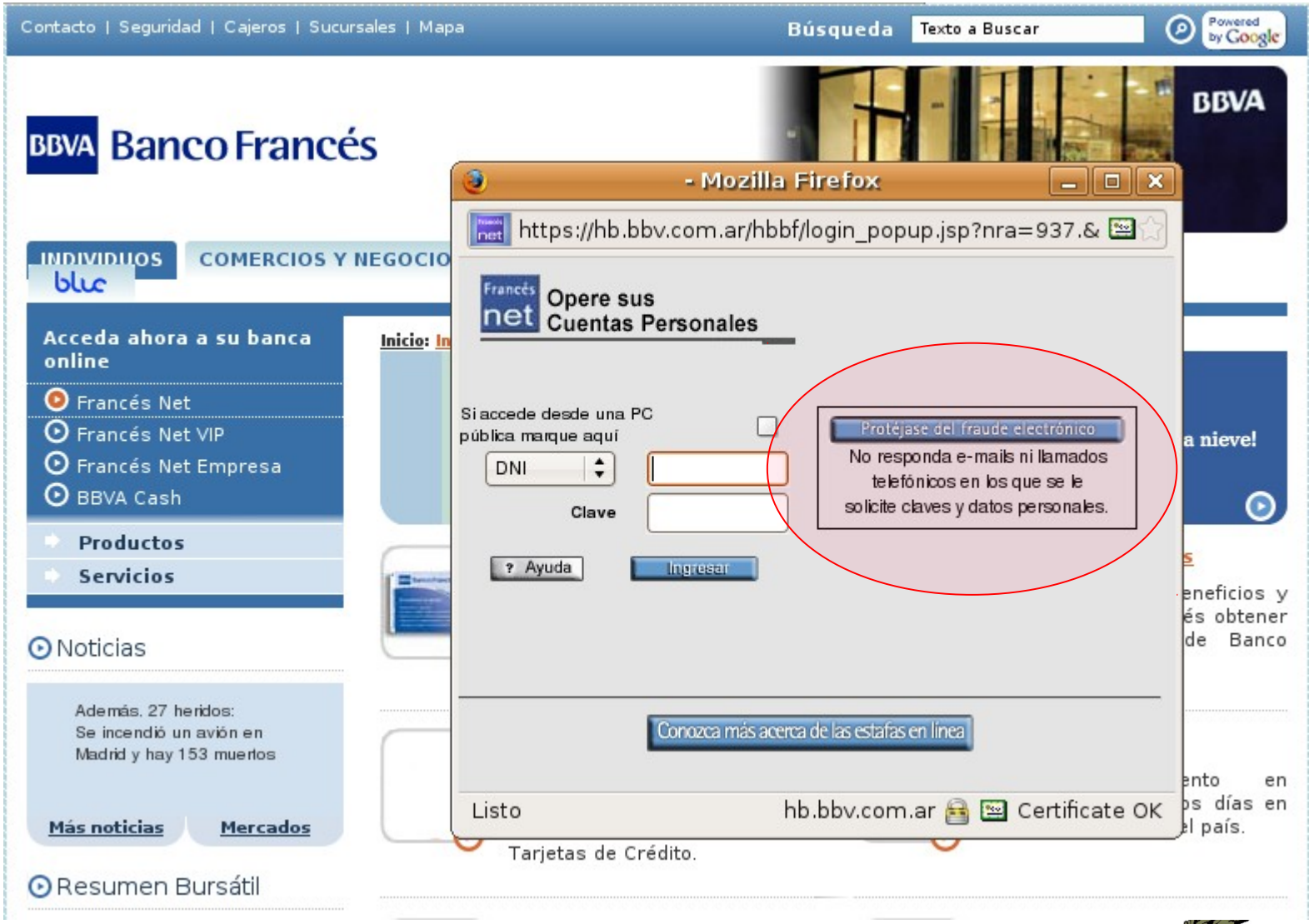
El **Pharming** consiste en alterar la asociación de nombre (www.mibanco.com) a dirección real (IP) para dirigir a un usuario a una dirección que no es la verdadera.
Puede ser desconcertante ya que el usuario escribe por si mismo la dirección de la página web.

Amenazas sobre las personas -Phishing

Phishing
Mail falso

Amenazas sobre las personas -Phishing

Phishing Sitio verdadero



Amenazas sobre las personas -SPAM

También llamado “Correo Basura”. Es uno de los principales medios para hacer llegar todo tipo de problemas a los usuarios del correo electrónico

Utilizado para:

- Publicidad no deseada
- Phishing (se vale de la ingeniería social)
- Transmisión de código malicioso (virus, etc)

Amenazas sobre las personas -SPAM Un ejemplo...

De: Natalia Alonso <ventas385@netservers.com.ar>

Para: ????<????@????.unlp.edu.ar>

Asunto: Si, es imperdible: Todo Sobre VITREAUX

7500 PLANOS Y DISEÑOS LA BIBLIOTECA DE VIVIENDAS POR EXCELENCIA ARCHITECTURAL SOFT® TODO PARA LA CONSTRUCCIÓN DE: CASAS, VIVIENDAS, CABAÑAS, BUNGALOWS, Y MÁS 4 CDs COMPLETOS

CON EL MEJOR SOFTWARE

Y LOS PLANOS MAS COMPLETOS ARCHITECHTURAL SOFT Presentamos a nuestros suscriptores: La biblioteca multimedial de Arquitectura y Viviendas por excelencia. Más de 7.500 planos y diseños expuestos en diagramas, planos, fotos, gráficos.

SI NO DESEA RECIBIR MAS INFORMACIÓN ESCRIBIR UN MAIL INDICANDO "FUERA DATOS"

Amenazas sobre las personas

Hoax (Engaño, burla)

Son mensajes de correo electrónico engañosos que se distribuyen en cadena. Algunos tienen textos alarmantes sobre catástrofes (virus informáticos, perder el trabajo o incluso la muerte) que puede suceder si no se reenvía el mensaje o se hace lo que el mismo indica.

La motivación de un hoax es recolectar direcciones de correo y otros datos confidenciales

Amenazas sobre las personas - Hoax
Un ejemplo

Subject: ALERTA VIRUS!!!!!!! Por favor SEGUIR EL PROCEDIMIENTO

Yo lo tenia y lo borre

OJO ES EN SERIO,

CASI TODAS LAS COMPUS LO TIENEN,

Queridos Amigos:

El motivo de este e-mail es advertir a todos los usuarios de hotmail sobre un nuevo virus que circula por medio del MSN Messenger.

El virus se llama jdbgmgr.exe y se transmite automáticamente por medio del Messenger y tambien por la libreta de direcciones.

El virus no es detectado por McAfee o Norton y permanence en letargo durante 14 días antes de dañar el sistema entero. Puede ser borrado antes de que elimine los archivos de tu computadora Para eliminarlo, solo hay que hacer los pasos siguientes:

1. Ir a Inicio, pulsar "buscar"

2.- En búsqueda "archivos o carpetas" escribir el nombre jdbgmgr.exe

3.- Asegurarse de que este buscando en disco "C"

4- Pulsar en "buscar ahora"

5.- Si aparece el virus (el icono es un osito que tendrá el nombre de jdbgmgr.exe NO ABRIR POR NINGUN MOTIVO

6.- Pulsar en el botón derecho del ratón y eliminarlo (ira a la papelera de reciclaje).

7.- Ir a la papelera de reciclaje y borrarlo definitivamente o bien vaciar la papelera entera.

SI ENCUENTRAN EN VIRUS EN SUS EQUIPOS MANDAR ESTE MENSAJE A LAS PERSONAS QUE TENGAN EN SU LIBRETA DE DIRECCIONES ANTES DE QUE CAUSE ALGUN DAÑO GRACIAS

Amenazas sobre las personas - Hoax Otro ejemplo..

Hoax "Nokia - Ericsson"

"Nuestro mayor competidor, Nokia, esta regalando telefonos a traves de internet.

Aqui en Ericcson queremos mejorar la oferta, asi que estamos regalando nuestros nuevos telefonos WAP tambien!.

Estos modelos WAP estan especialmente diseñados para nuestros felices clientes de internet quienes apreciaran la nueva tecnología. Regalando telefonos nosotros obtenemos clientes agradecidos y un enorme efecto "boca a boca".

Todo lo que hay que hacer para recibir un WAP es enviar este mail a 8 personas, a las dos semanas , el WAP estara llegando a su casa (Ericsson T18). Si en lugar de enviar este mail a 8 personas, se envia a 20 personas, el regalo sera el mas nuevo de nuestros modelos , un Ericsson R320 WAP!

Importante: Cada vez que envies uno de estos mails, envia una copia a Anna.Swelund@ericsson.com (respetar mayusculas), es la unica forma de que sepamos que estas mandando el mail.

Mucha suerte!

Anna Swelund - Gerente Ejecutiva de Promocion para el sector Marketing de Ericsson".

Amenazas en controles de acceso

Elementos del control de acceso

- **Identificación:** es una secuencia de caracteres que identifica unívocamente al usuario: nombre de usuario.
- **Autenticación:** es la verificación que realiza el sistema sobre la identificación. Se puede realizar a través de:
  - Algo que se conoce: clave de acceso
  - Algo que se posee: tokens / tarjeta
  - Algo que se es: huella digital, iris, retina, voz
- **Autorización:** son los permisos asociados al usuario autenticado.

Amenazas en controles de acceso

Ataques de contraseñas:

Consiste en la prueba metódica de contraseñas para lograr el acceso a un sistema, siempre y cuando la cuenta no presente control de intentos fallidos de logueo. Este tipo de ataque puede ser realizado:

- Por diccionario: existiendo un diccionario de palabras, una herramienta intentará acceder al sistema probando una a una las palabras incluidas en el mismo.
- Por fuerza bruta: una herramienta generará combinaciones de letras, números y símbolos formando posibles contraseñas y probando una a una en el login del sistema.

Más amenazas sobre las personas

- Robo de identidad: Ocurre cuando alguien obtiene y utiliza, mediante medios informáticos, información personal ajena (nombre, número de tarjeta de crédito, información bancaria, número de afiliado a un sistema de salud, etc.) sin su autorización, con el propósito de realizar actividades fraudulentas.
- Fraude informático: Se trata del perjuicio económico efectuado a una persona mediante la utilización de un sistema informático, ya sea, modificando datos, introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee la seguridad del sistema.

Amenazas sobre la información

Acceso no autorizado a información sensible, como puede ser:

- Información confidencial impresa.
- Información confidencial guardada en medios de almacenamiento removibles (CDs, DVDs, pendrives).
- Información confidencial guardada en notebooks.

Amenazas sobre la información

- Trashing: Consiste en la búsqueda de información dentro de la basura. Esto puede representar una importante amenaza para aquellos usuarios que no destruyen información crítica o confidencial al descartarla.
- Pérdida de copias de resguardo: provocadas por daños físicos a causa de desastres naturales, por obsolescencia de los medios físicos que contienen la información, etc.

Amenazas sobre el hardware

- Daños físicos al equipamiento
- Robo de equipos o componentes

Obviamente también afectan a la información que en ellos residía

Cómo enfrentamos las amenazas

- Hay mucho por hacer en este sentido, dentro de un marco de gestión de la seguridad, para establecer controles preventivos y correctivos.
- Una de las tareas más importantes es la capacitación, y dentro de ella podemos distinguir:
  - Concientización de los usuarios/personal de la organización.
  - Especialización del personal que tiene a cargo la seguridad de la Información

Concientización

- Un programa de concientización de Seguridad resulta fundamental para fortalecer los eslabones más débiles de la cadena de seguridad, las personas por:
  - Desconocimiento de las amenazas.
  - Desconocimiento de las medidas de seguridad
  - Desconocimiento de los roles y responsabilidades de cada persona, con respecto a la seguridad
- Este programa debe estar dirigido a todo el personal que trabaje con información de la organización.

Concientización

- El programa de concientización debe incluir:
  - Acciones de impacto, como ser:
    - Sesiones de concientización para los directivos
    - Sesiones de concientización para personal de TI
    - Sesiones de concientización para usuarios finales
  - Acciones de seguimiento, como ser:
    - Eventos de seguridad
    - Boletines internos
    - Posters
    - Tips en el sitio web, etc

Concientización

- El programa de concientización debe ser realizado a medida, teniendo en cuenta perfil de la empresa, tareas que se realizan y rasgos del personal.
- Las actividades/ejemplos deben relacionarse con las actividades diarias del personal

Concientización- Algunos tips

- Lograr que los usuarios entiendan:
  - Qué deben proteger?
  - Contra qué?
  - Cómo? (Buenas prácticas)
- Como ejemplo, veamos algunos temas a incluir y la forma de hacerlo:
  - Amenazas en controles de acceso
  - Acceso no autorizado a la información

Concientización - ejemplos
Amenazas en controles de acceso

Clave: Conjunto de caracteres asociados a nuestro identificador, que nos permite realizar la autenticación.

Características deseables:

- Debe ser personal y secreta
- No se debe prestar
- Puede ser cambiada sólo por el usuario al que pertenece
- Debe ser difícil de descubrir
- Debe renovarse periódicamente

Concientización - ejemplos
Amenazas en controles de acceso

Riesgos Inherentes a la Clave:

- Pérdida u olvido de la misma.
- Sustracción por parte de un tercero.
- No renovación periódica de la clave.
- Descuidos en su operación.

Concientización - ejemplos
Amenazas en controles de acceso

Aplicaciones que evalúan la fortaleza de las claves

Pruebe su Contraseña		Requerimientos Minimos
Clave:		• Mínimo 8 caracteres de largo • Contener 3/4 de los siguientes puntos: - Letras mayúsculas - Letras minúsculas - Números - Símbolos
Ocultar:	1	
Puntuación:	0%	
Complejidad:	Muy Corta	

Adiciones	Tipo	Puntaje	Conteo	Bonus
Numero de Caracteres	Flat	+(n*4)	0	0
Letras mayúsculas	Cond/Incr	+((len-n)*2)	0	0
Letras minúsculas	Cond/Incr	+((len-n)*2)	0	0
Números	Cond	+(n*4)	0	0
Símbolos	Flat	+(n*6)	0	0
Números o Símbolos Centrales	Flat	+(n*2)	0	0
Requerimientos	Flat	+(n*2)	0	0
Deducciones				
Solo Letras	Flat	-n	0	0
Solo Números	Flat	-n	0	0
Caracteres Repetidos (Case Insensitive)	Incr	-(n(n-1))	0	0
Letras Mayúsculas Consecutivas	Flat	-(n*2)	0	0
Letras Minúsculas Consecutivas	Flat	-(n*2)	0	0
Números Consecutivos	Flat	-(n*2)	0	0
Letras Secuenciales (3+)	Flat	-(n*3)	0	0
Números Secuenciales (3+)	Flat	-(n*3)	0	0

Leyenda

Excepcional: Supera los requisitos. Se suman puntos extras.
Suficiente: Cumple los requisitos mínimos. Se adicionan puntos extras.
Advertencia: Advertencia sobre la utilización de malas prácticas. Se reduce la puntuación general.
Insuficiente: No cumple los requisitos mínimos. Se reduce la puntuación general.

Concientización - ejemplos
Amenazas en controles de acceso

Cuidados en el uso de las claves

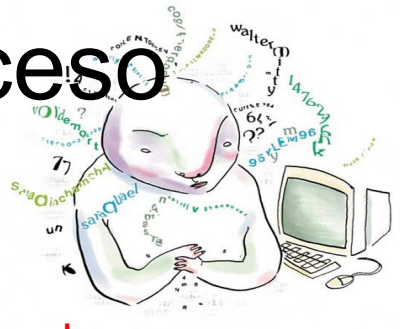
- Cuidar que no te vean cuando tipea su clave. No observar a otros mientras ingresan su clave.
- No pedir la clave de otro ni compartir su clave.
- No escribir la clave en papelitos ni en archivos no protegidos. Si por algún motivo se debe que escribir la clave, no dejarla al alcance de terceros.
- No habilitar la opción de “recordar claves” en los programas.
- No envíar la clave por correo electrónico o mensajería instantánea. Tampoco la mencionarla en una conversación.

Concientización - ejemplos Amenazas en controles de acceso

Normas para construir una clave de acceso

- No utilizar palabras comunes ni nombres de fácil deducción.
- No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, etc.)
- No utilizar terminología técnica conocida.
- Elegir una contraseña que combine caracteres alfabéticos (mayúsculas y minúsculas), números y caracteres especiales.
- Utilizar una longitud mínima de 8 caracteres.
- Utilizar contraseñas distintas para máquinas diferentes y/o sistemas diferentes. Puede usarse una contraseña base y ciertas variaciones lógicas para distintos sistemas.

Concientización - ejemplos Amenazas en controles de acceso



Elección de una clave de acceso – Ejemplo

1-Pensar en una oración que puedas recordar. Por ejemplo: “no lo soñeeeeiiieeeieeiee, se enderezo y brindó a tu suerte”

2-Tomá la primera letra de cada palabra: ”nlsseybats”

3-Incorporar alguna mayúscula, en alguna palabra que pueda ser significativa, por ejemplo BRINDO: ”nlsseyBats”.

4-Agregar números o reemplazá alguna letra por número, los reemplazos mas comunes son: A → 4 ; E → 3 ; o → 0 ; s → 5 ;

=> “nl553yBat5”

5- Usar algún caracter especial, por ejemplo: i → ! ; a → @ ; x → %

=> ”nl553yB@t5”

Concientización - ejemplos
Acceso no autorizado a la información

Política de pantallas y escritorios limpios

Es de vital importancia tomar todas las acciones necesarias para que la información sensible no llegue a manos de quienes no están autorizados.

Generalmente a las oficinas ingresan personas externas a la misma (proveedores, consultores,clientes, personal de otra oficina/sector de la organización, personal de limpieza).

Para proteger la información es deseable mantener los escritorios limpios y organizados evitando dejar información “a la vista”

Concientización - ejemplos
Acceso no autorizado a la información

Política de pantallas y escritorios limpios

Elementos que debemos proteger manteniendolos fuera del alcance de terceros yen lugares no visibles:

- Documentación impresa: datos confidenciales de empleados y/ó terceros, resultados de auditorías, contratos, números de cuenta, entre otros.
- Medios de almacenamiento externo como pendrives, CD's ó DVD's.
- Notebooks
- Bolsos, portafolios

Concientización - ejemplos
Acceso no autorizado a la información

Cada día cuando se retira de su oficina:

- Apague su terminal, o si debe dejarla encendida para que otro la utilice, salga de su sesión.

Cada vez que abandone su puesto de trabajo, aunque sólo sea temporalmente:

- No deje desatendida su terminal.
- Bloquee su terminal con las facilidades que provee su sistema operativo o con un protector de pantalla que requiera volver a ingresar su clave para desbloquearla.