VIII SEMINARIO DE INFORMÁTICA EN LA UC

Seguridad Informática en la Universidad: Riesgos, consecuencias y servicios

Andres Altamirano
aaltamirano@uc.cl

Pontificia Universidad Católica de Chile - Dirección de Informática - Junio 2010

Temas

- ¿Seguridad informática?
- Amenazas
- Consecuencias
- Incidentes
  - Datos
  - Casos
- ¿Cómo protegerse?
- Contraseñas menos expuestas: SSO
- Seguridad perimetral

¿Seguridad informática?

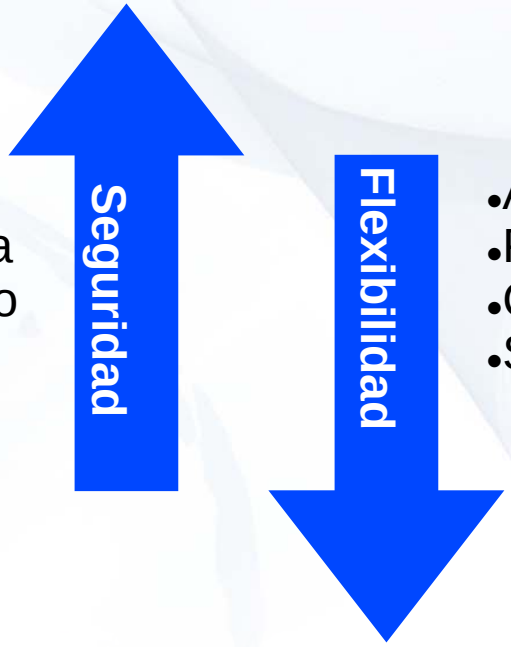
Integridad alteración

Confidencialidad exposición

Disponibilidad destrucción

¿Seguridad informática?

- Control de acceso
- Planificación adecuada
- Verificación del entorno
- Privacidad



- Acceso remoto inmediato
- Producción urgente
- Conectividad “anywhere”
- Servicios gratis

Amenazas

- A los servicios
  - Ataques dirigidos (DoS, enum, exploiting, etc)
  - Eventos imprevistos (fuego, desastres, etc)
  - Exposición de información privada
- A las personas
  - Robo
    - Equipos moviles
    - Gadgets (smartphones, pendrives, iP@ds, etc)
  - Ingeniería social
    - Phishing (email, post-it, llamado telefónico, etc)
    - Gadgets

Consecuencias

- Servicios
  - Interrupciones en la continuidad del negocio.
  - Fuga de información.
  - Pérdida de usuarios/clientes.
  - Prestigio, dinero.
- Personas
  - Recursos tecnológicos degradados.
  - Fraudes.
  - Problemas personales.
  - Exposición

Incidentes 2008-2010

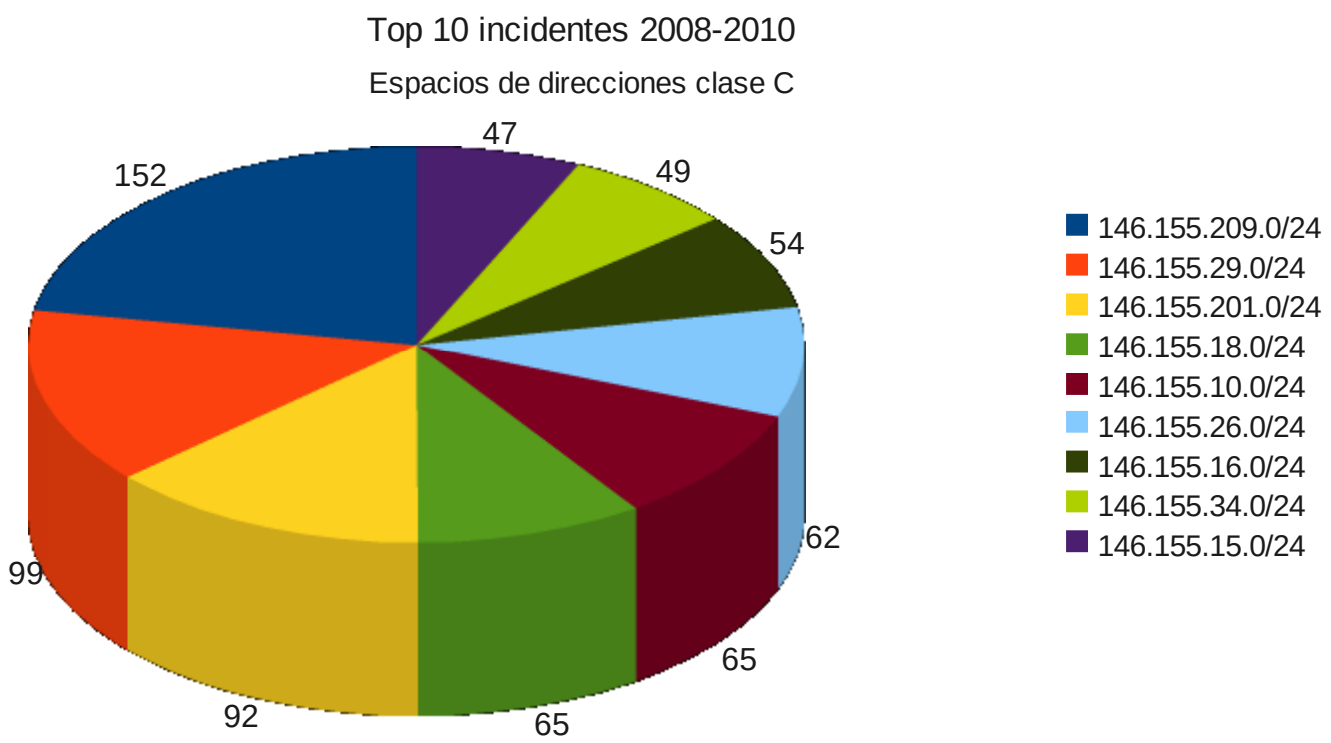
- Registro de incidentes reportados o detectados por al área de seguridad.

Incidentes 2008-2010

- Aumento explosivo del SPAM.

Incidentes 2008-2010

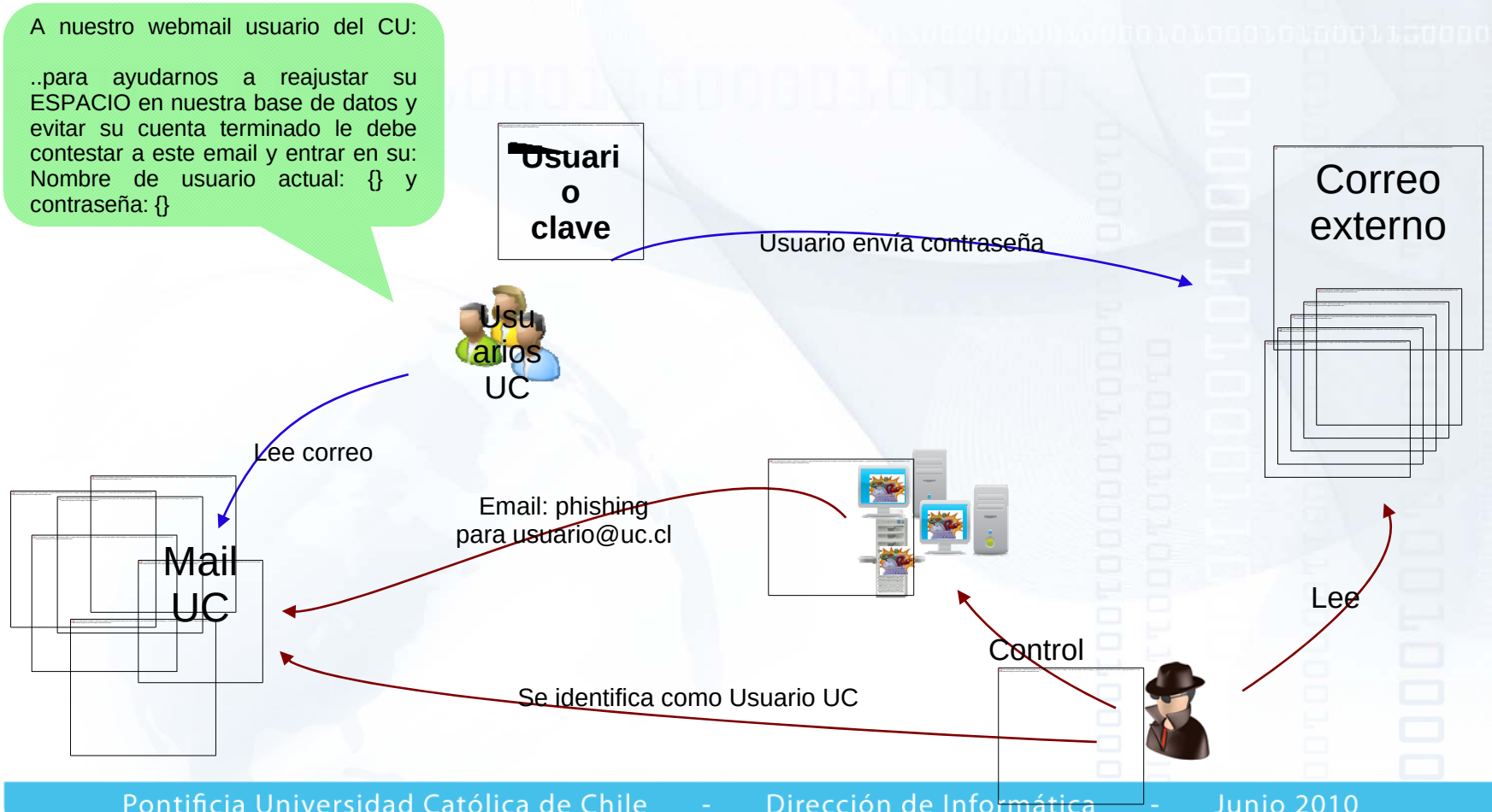
- Subredes con mas incidentes registrados.



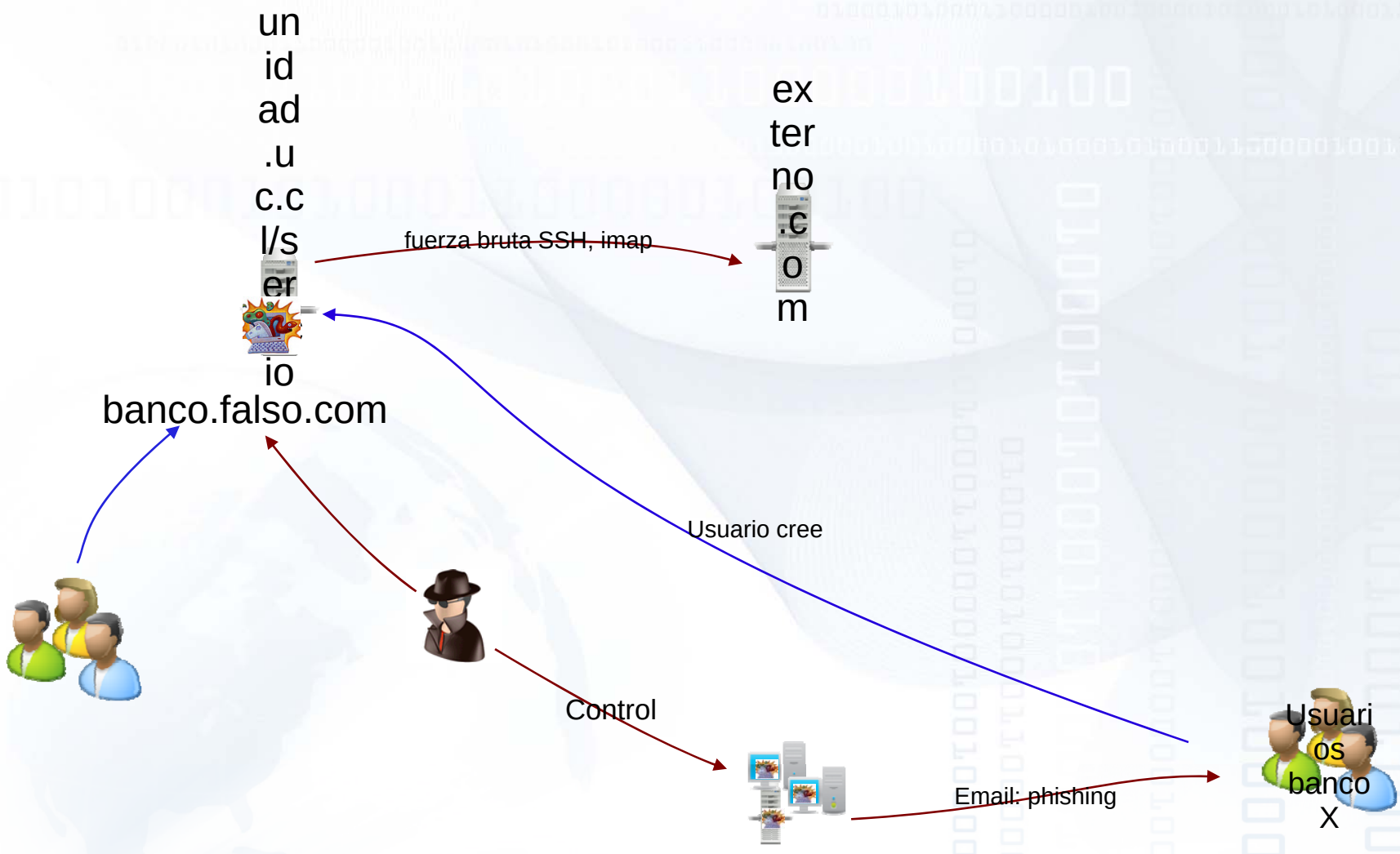
Incidentes 2010

- Objetivo nuevo: Cuentas de usuario UC.
- Mas de 100 casos durante el año 2010 de cuentas de usuario UC comprometidas.

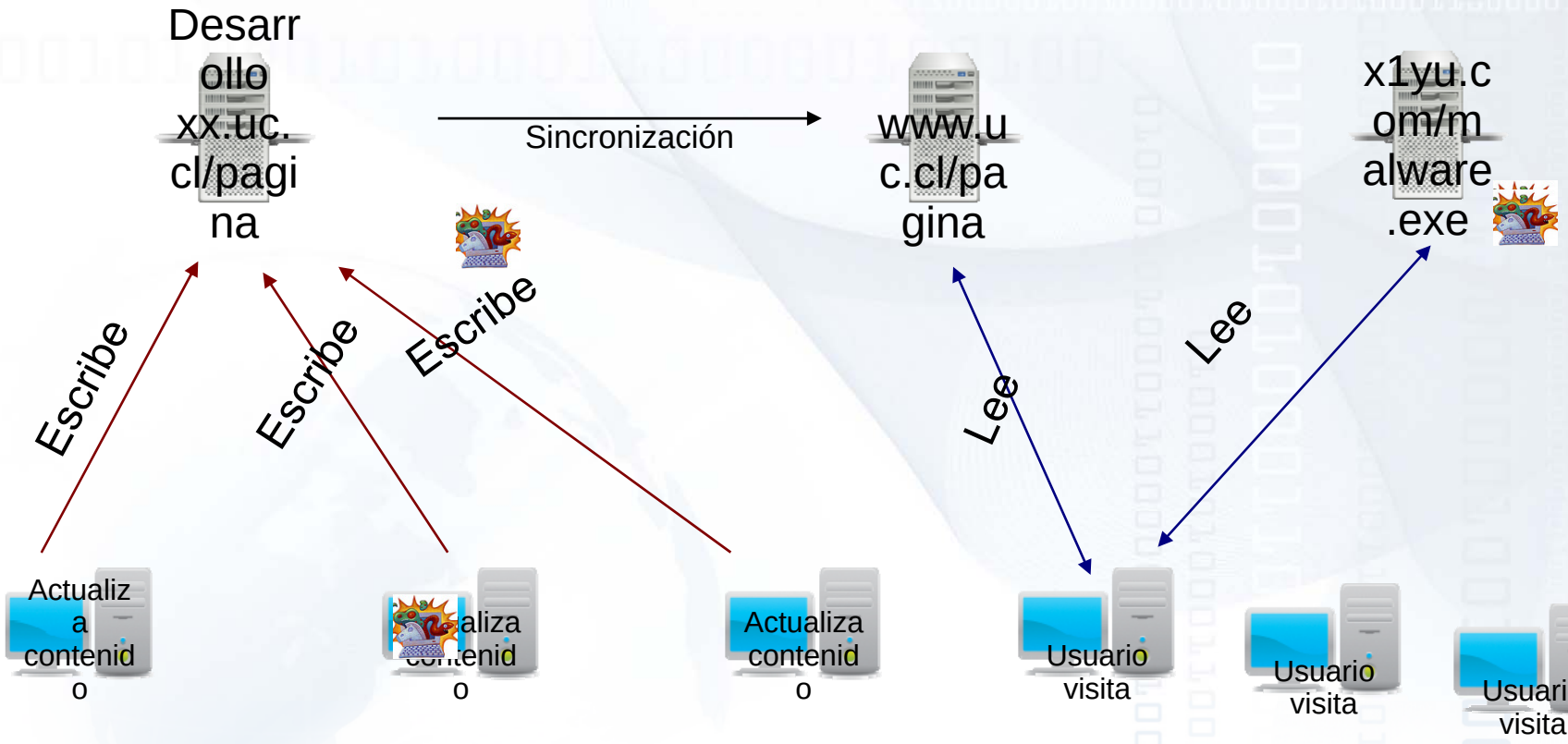
Caso I:Usuarios UC comprometidos



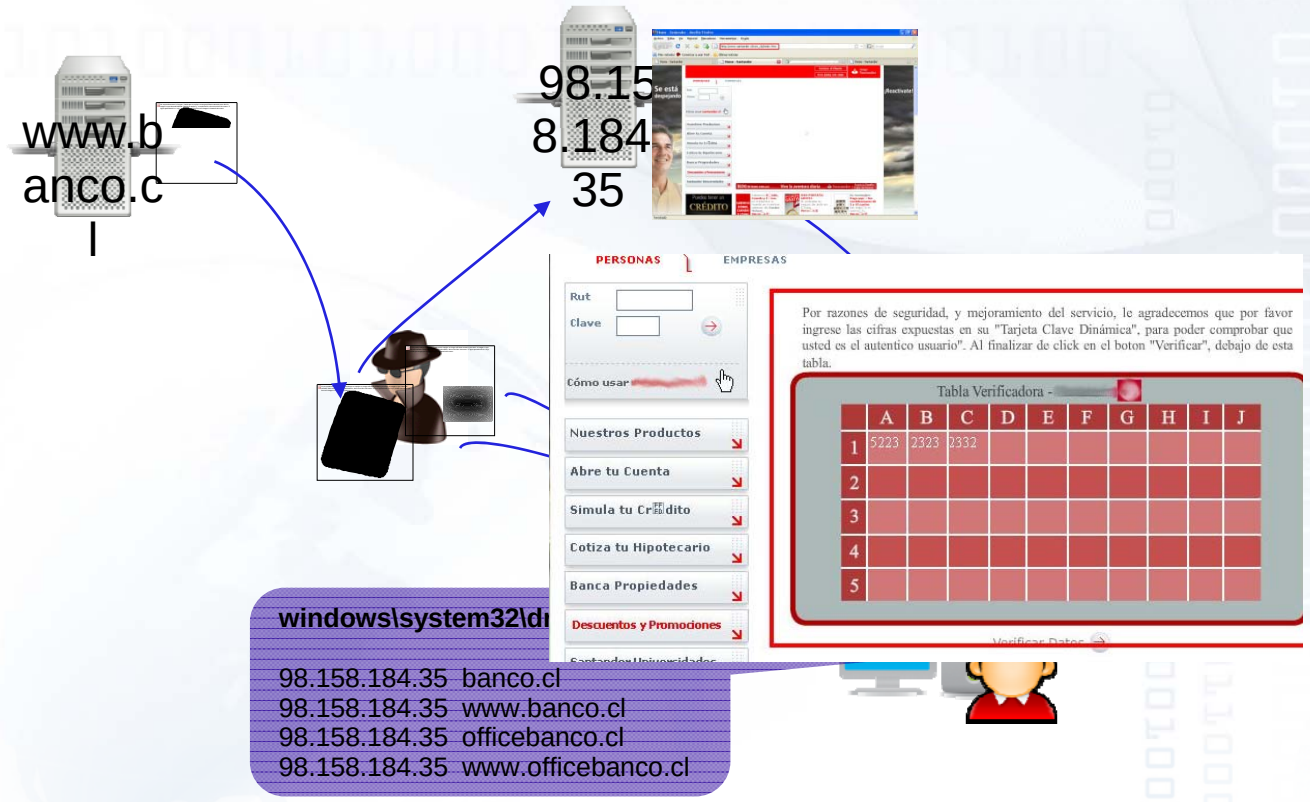
Caso II: Servidor comprometido en phishing y ataques de fuerza bruta



Caso III: Sitios web contaminados



Caso IV: Robo de credenciales bancarias



¿Cómo protegerse?

- Software y antivirus actualizado.
- Tomarse el tiempo para leer los cuadros de diálogo
- Verificar con la fuente ante dudas.
- Contraseña fuerte y cambio frecuente.
- Medios portables, evitar utilización crítica.
- No entregar contraseñas u otra información a terceros.
- No ejecutar archivos que no han sido solicitados.
- Resguardos al navegar (HTTPS, cache, claves).

Contraseñas fuertes o cambios frecuentes.

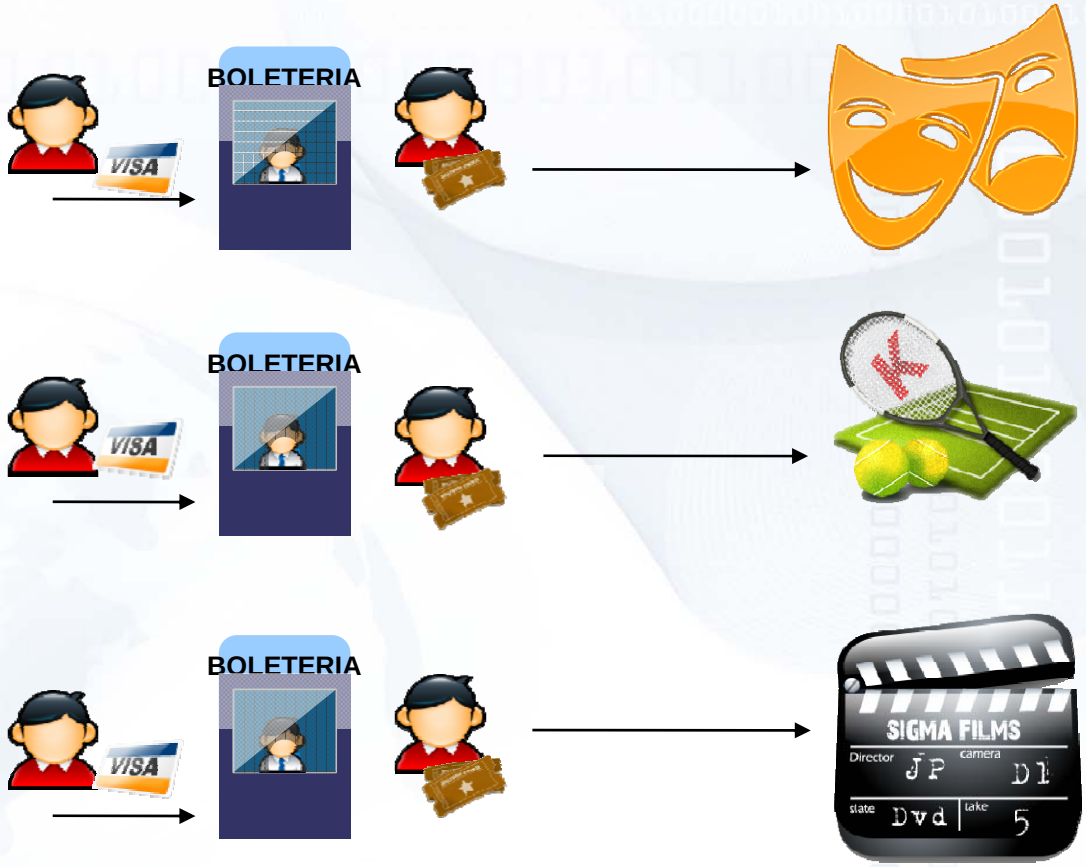
- Análisis de seguridad realizado en abril de 2010: Contraseñas mas usadas.

Contraseña
1234
123456
12345678
12345
catalina
carolina
password
sebastian
alejandro
alejandra

Single Sign On

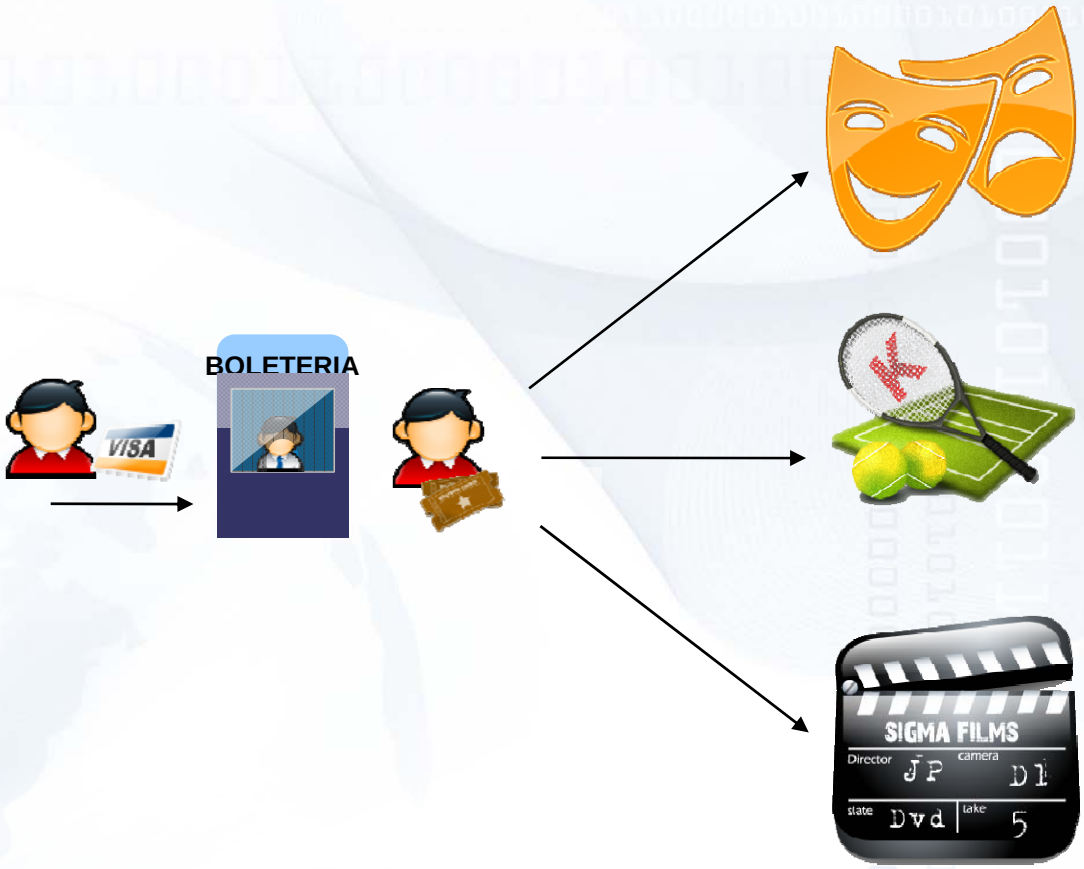
Contraseñas menos expuestas

- Analogía de la autentificación común.

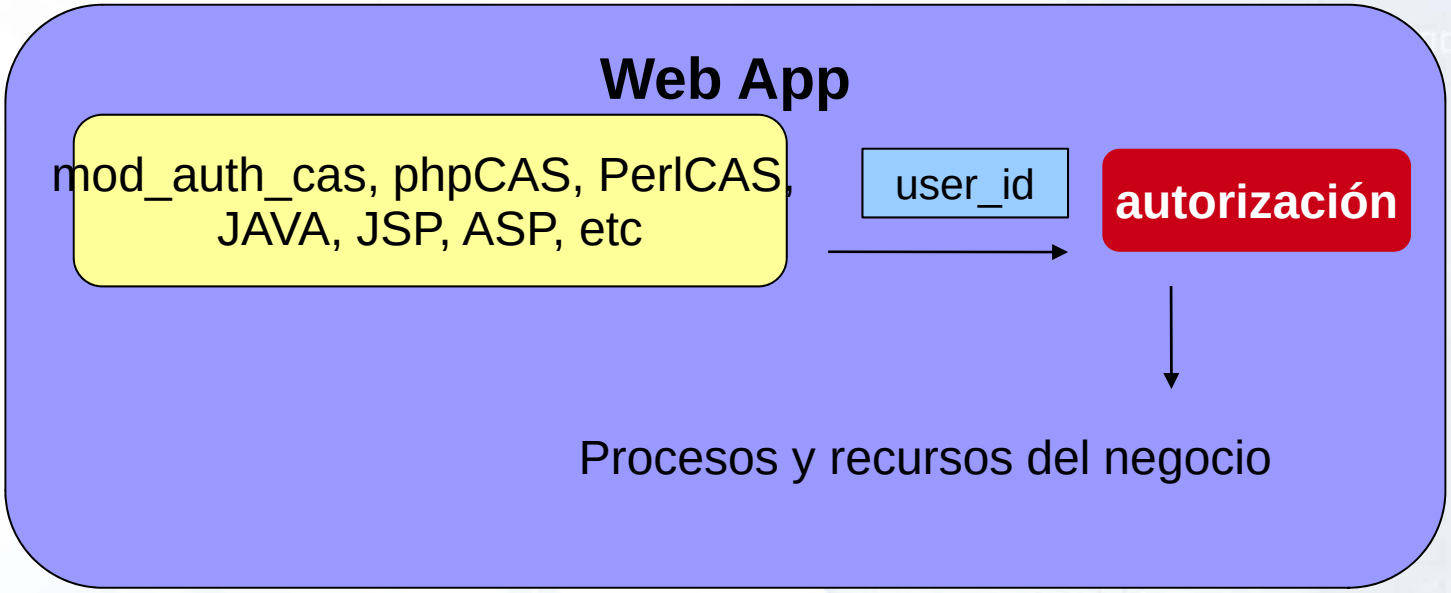


Contraseñas menos expuestas: SSO.

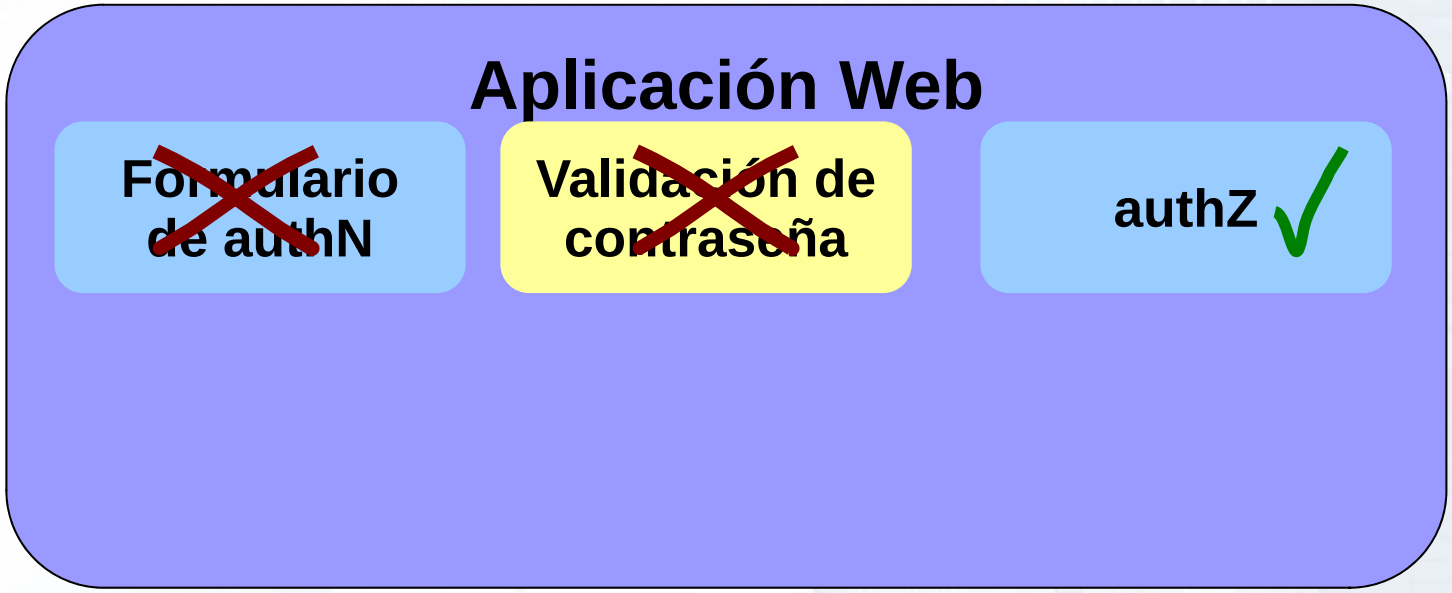
- Autentificación con Single Sign On



Separacion funcional



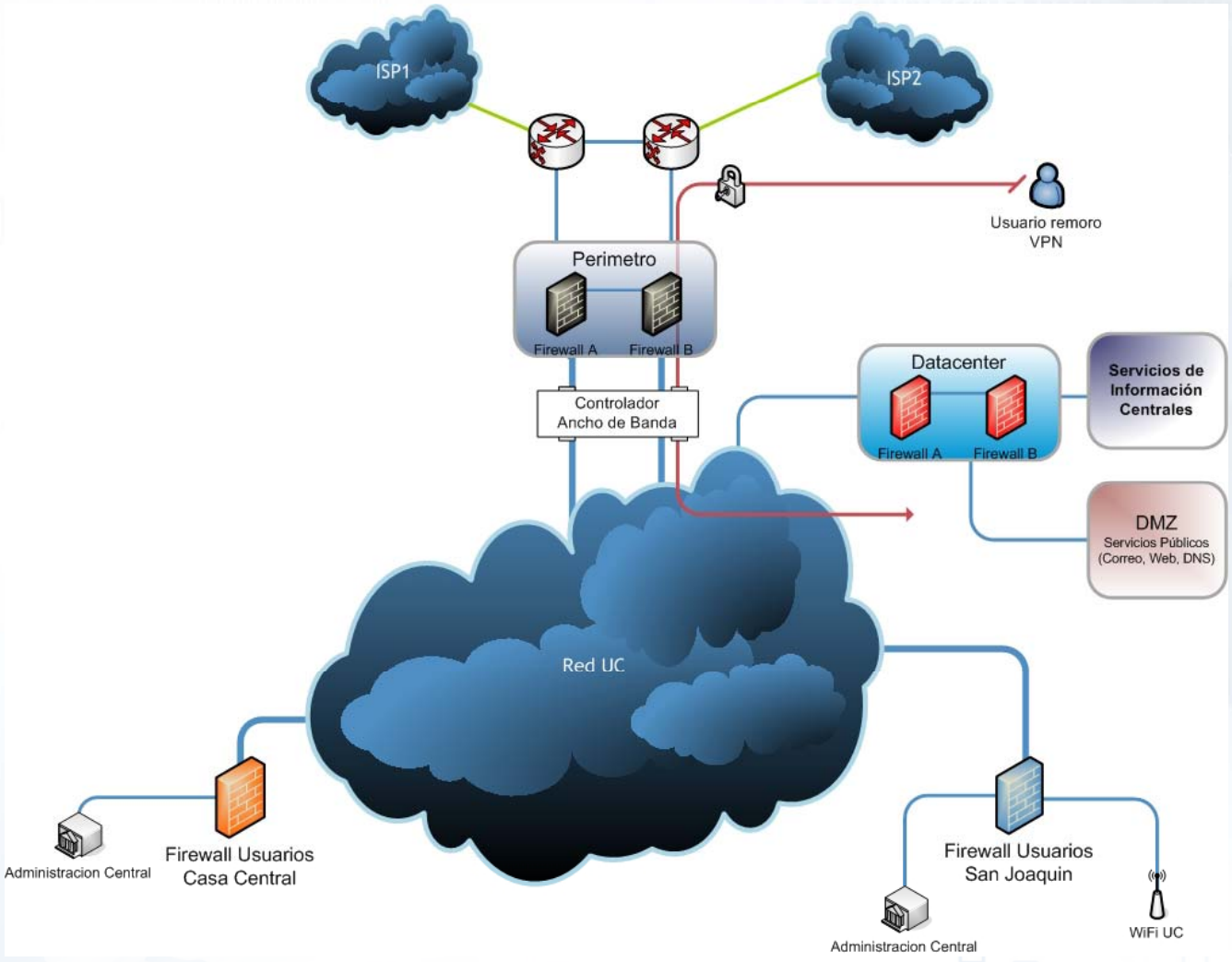
Resultado


Aplicación Web
Formulario de authN
Validación de contraseña
authZ

Seguridad perimetral

- Plataforma
- Normativa: estado de avance
- VPN

Plataforma de seguridad



Normativa de seguridad perimetral

- Estado de avance: 52% del espacio de direcciones en uso.
- Accesos VPN para unidades protegidas.
- Redefinición de la necesidad de los accesos remotos: escritorio remoto.
- Mala práctica: carpetas compartidas.

Servicio VPN

- Permite acceder desde e exterior a recursos internos utilizando un canal cifrado.
- Disponible para las unidades adscritas a la política de seguridad perimetral.
- Disminuye los riesgos de exponer servicios al exterior.
- No evita problemas derivados de descuidos.

Contacto

- Incidentes: abuse@uc.cl o 5555@uc.cl

EOF