PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

DIRECCIÓN DE INFORMÁTICA

Seguridad Informática en la UC

Jueves 12 de Junio de 2008

Andres Altamirano - aaltamirano@uc.cl

120 años EN EL CORAZÓN DE CHILE

Temas

- Nueva plataforma de seguridad
- Incidentes de seguridad
- Botnets
- Política de uso de recursos
- Política de protección en el acceso a internet

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

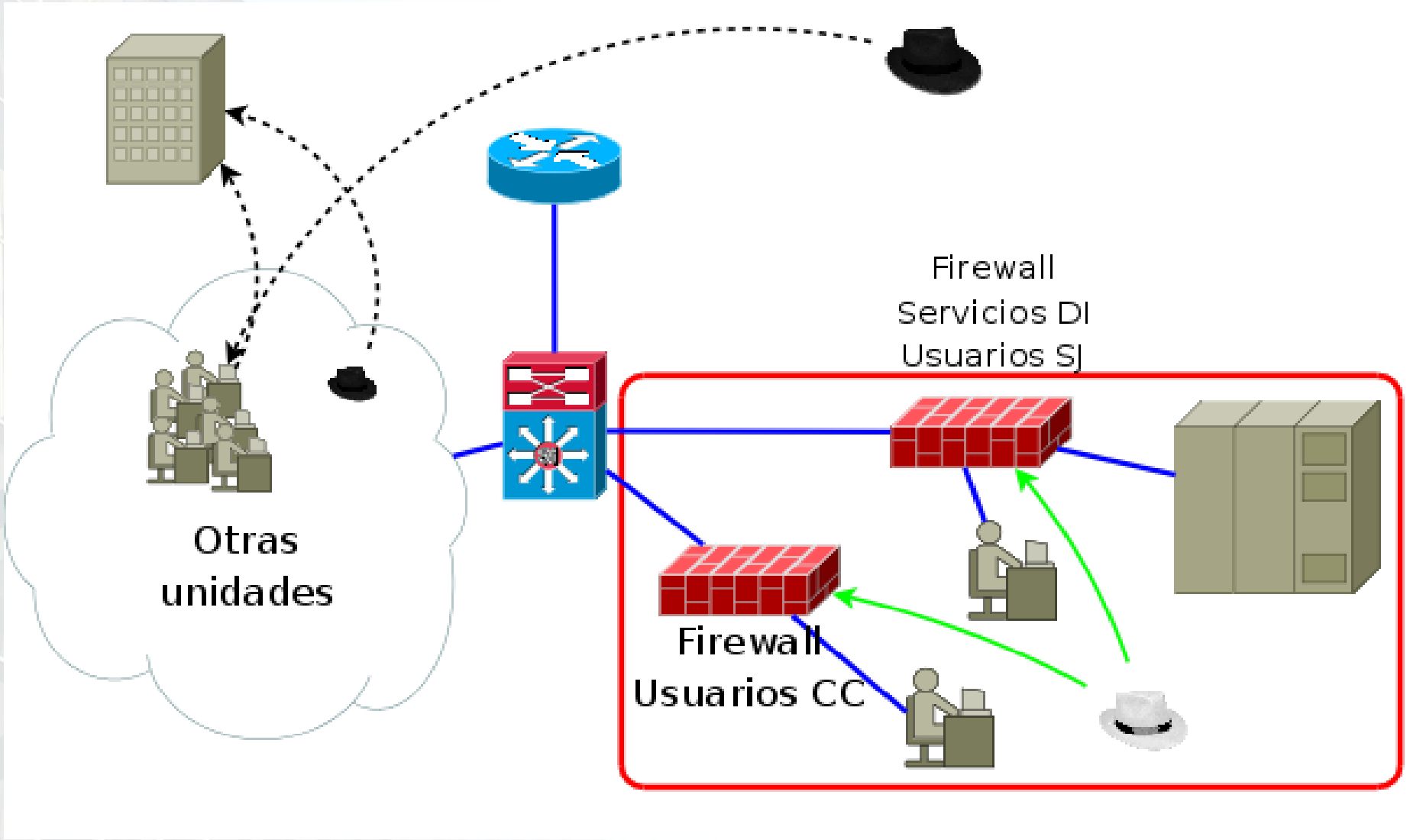
DIRECCIÓN DE INFORMÁTICA

Nueva plataforma de seguridad

120 años
EN EL CORAZÓN DE CHILE

Nueva plataforma de seguridad

- Año 2006

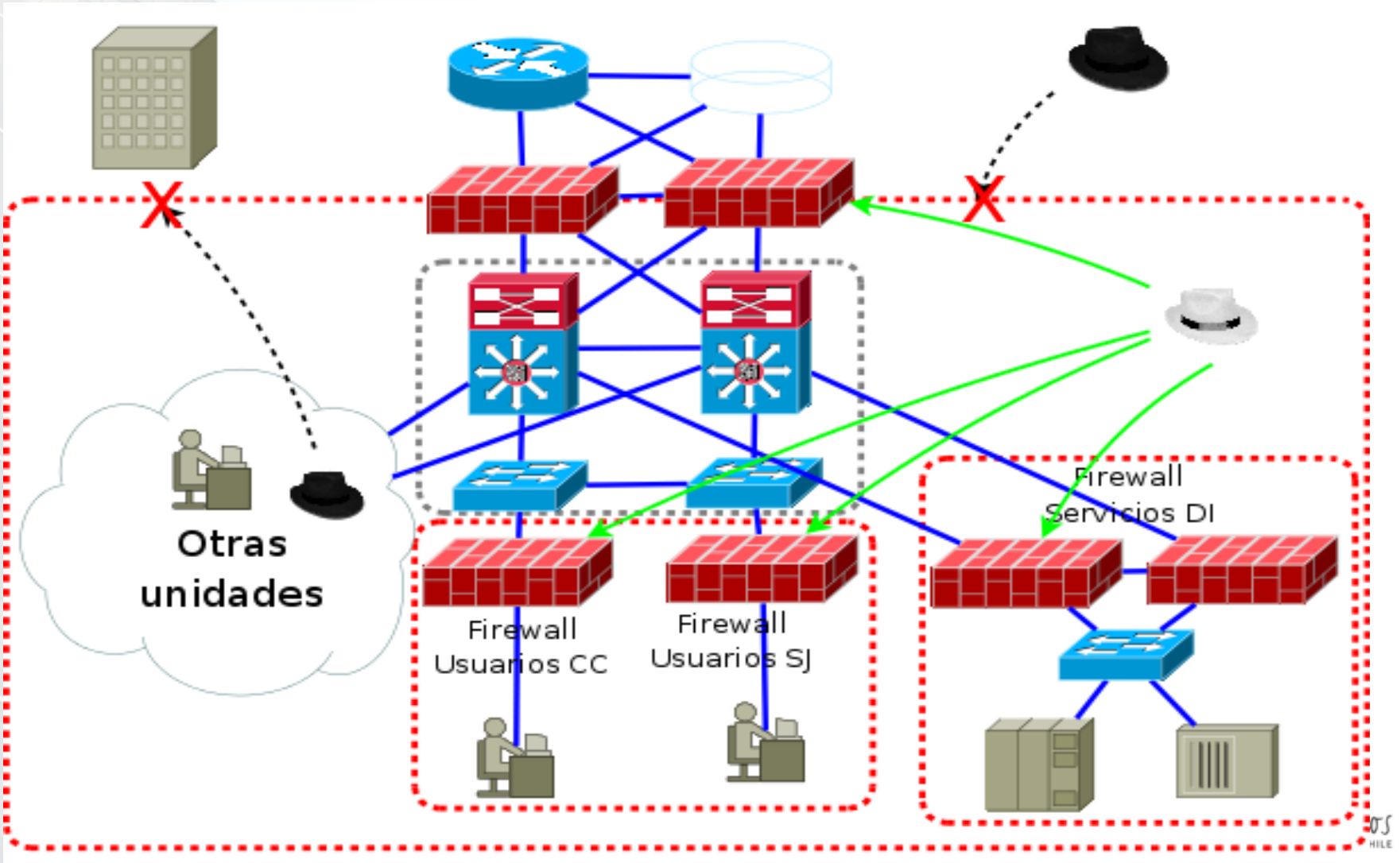


Nueva plataforma de seguridad

Pontificia Universidad Católica de Chile

Dirección de Informática

- Año 2008



Nueva plataforma de seguridad

Pontificia Universidad Católica de Chile

Dirección de Informática

- Posibilidades
  - Protección de la Red UC
  - Detección de comportamientos anómalos.
  - Capacidad de reacción ante ataques detectados
  - Control de acceso

120 años en el corazón de Chile

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

DIRECCIÓN DE INFORMÁTICA

Incidentes de seguridad

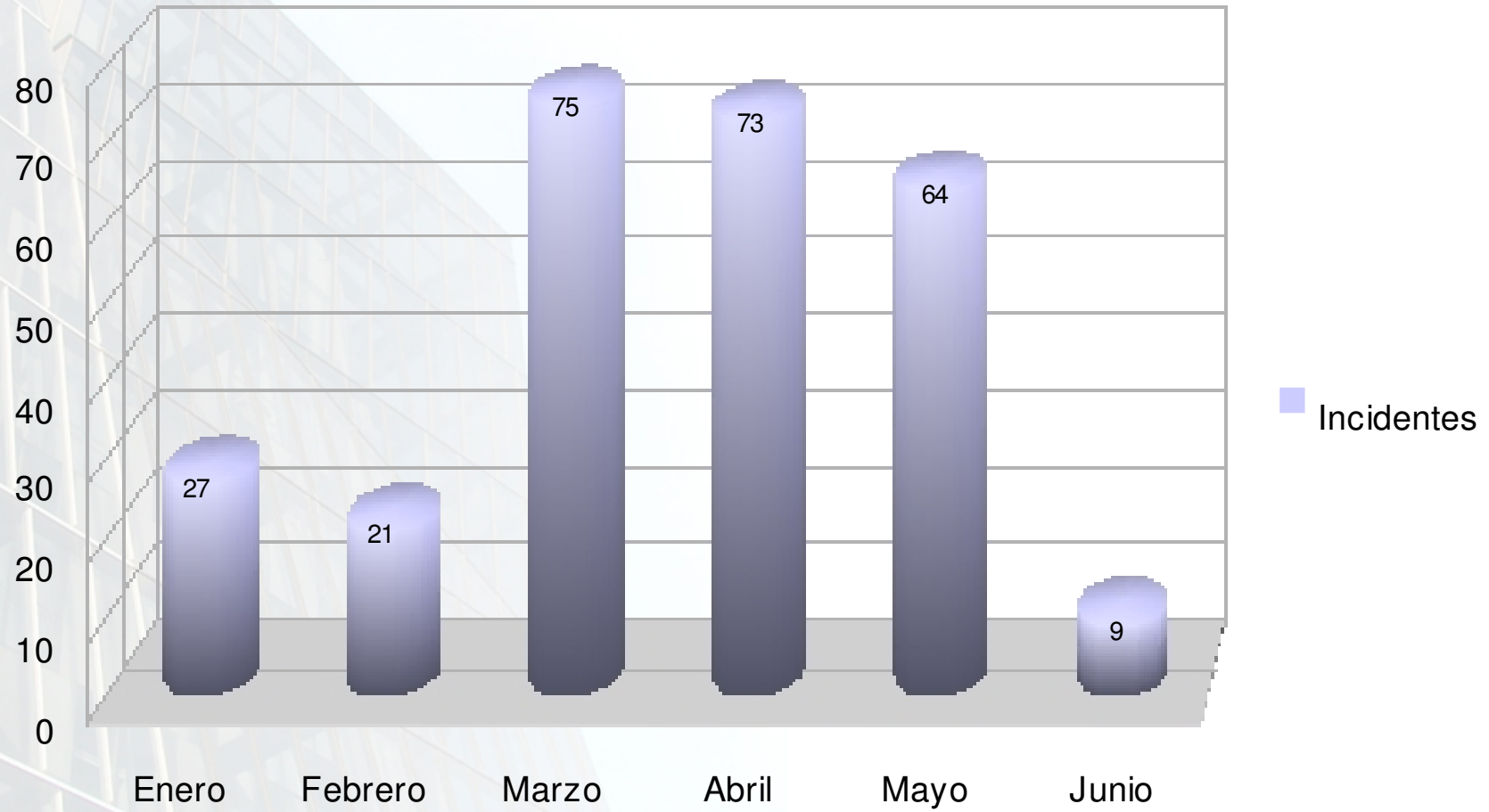
120 años
EN EL CORAZÓN DE CHILE

Incidentes de seguridad

- abuse@uc.cl
- Apoyo en detección de vulnerabilidades
- Investigación de incidentes
- Comunicación de amenzas
- Denuncia a otros SP

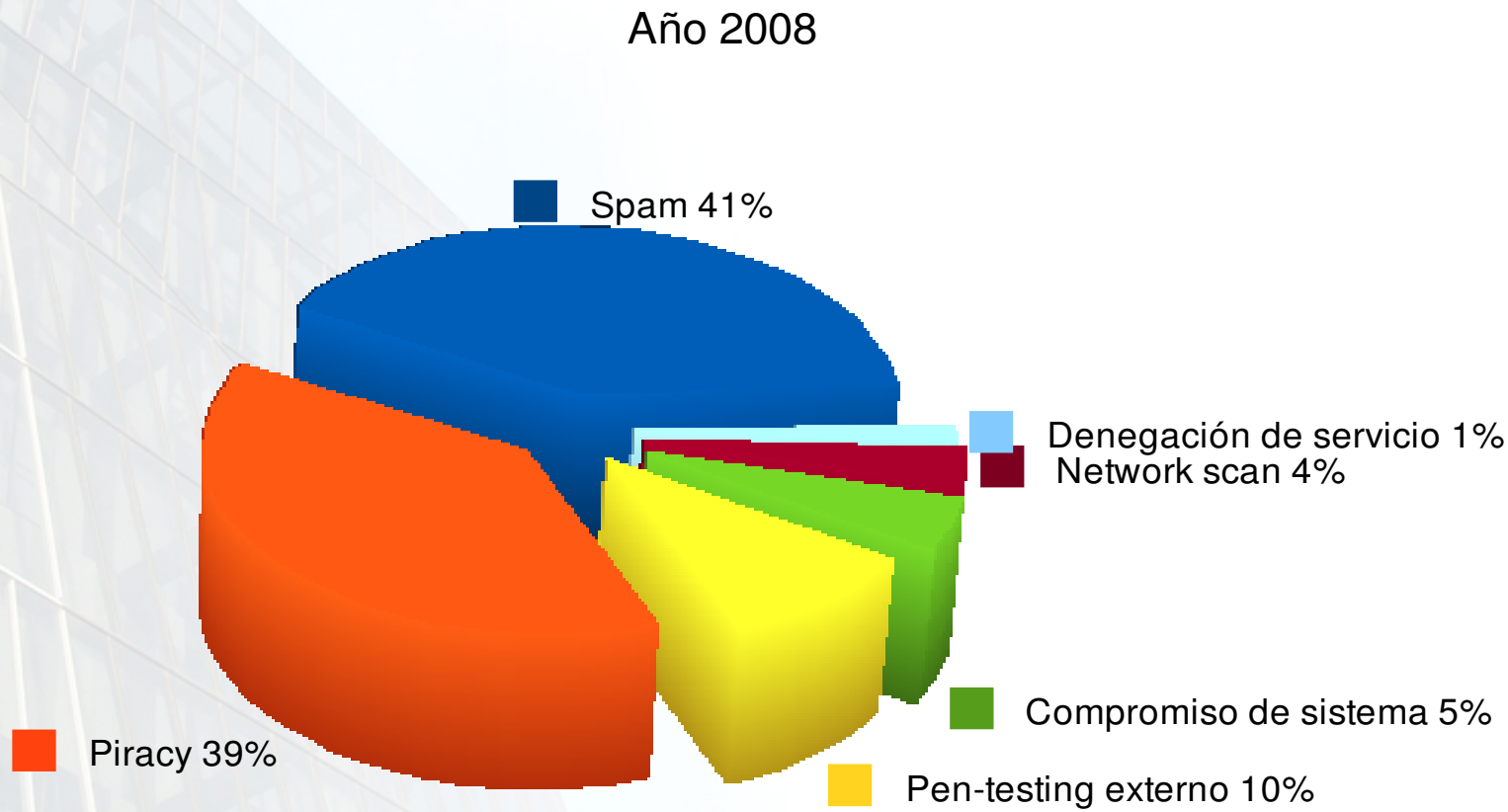
Incidentes de seguridad

- Registro de incidentes año 2008



Incidentes de seguridad

- Tipos de incidentes



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

DIRECCIÓN DE INFORMÁTICA

Botnets

120 años
EN EL CORAZÓN DE CHILE

Botnets

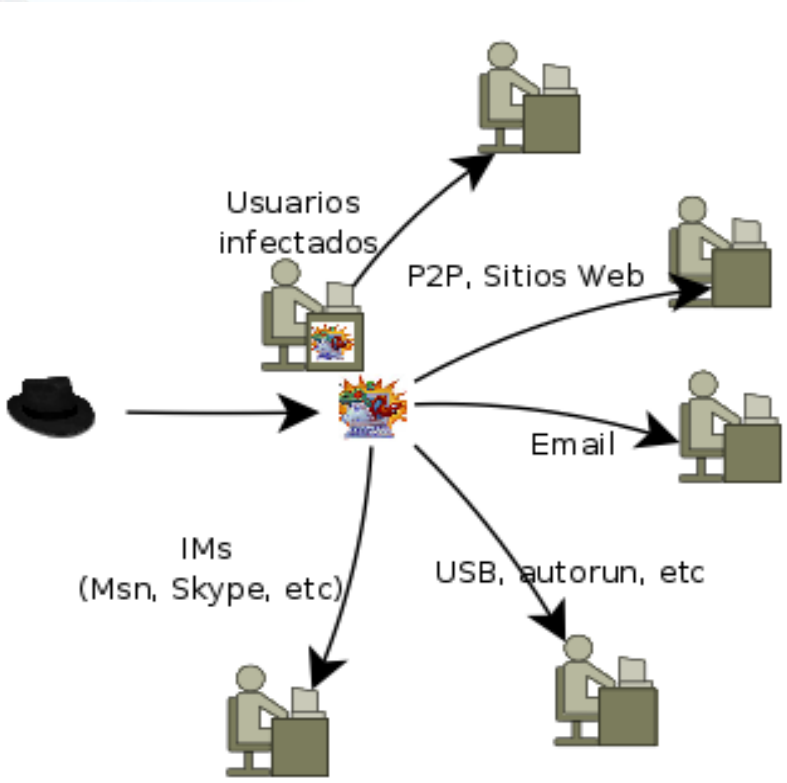
- Conjunto de computadores controlados por una entidad externa (botmaster) con la ayuda de un ”software autónomo y automático” (bot) instalado en dichos computadores.

Botnets

- Objetivo: apropiarse de la capacidad computacional de usuarios indefensos y utilizarla para los fines que el botmaster defina:
  - Campañas de SPAM
  - Ataque a otros sitios
  - Distribución del bot
  - Ataques de fuerza bruta
  - Uso comercial

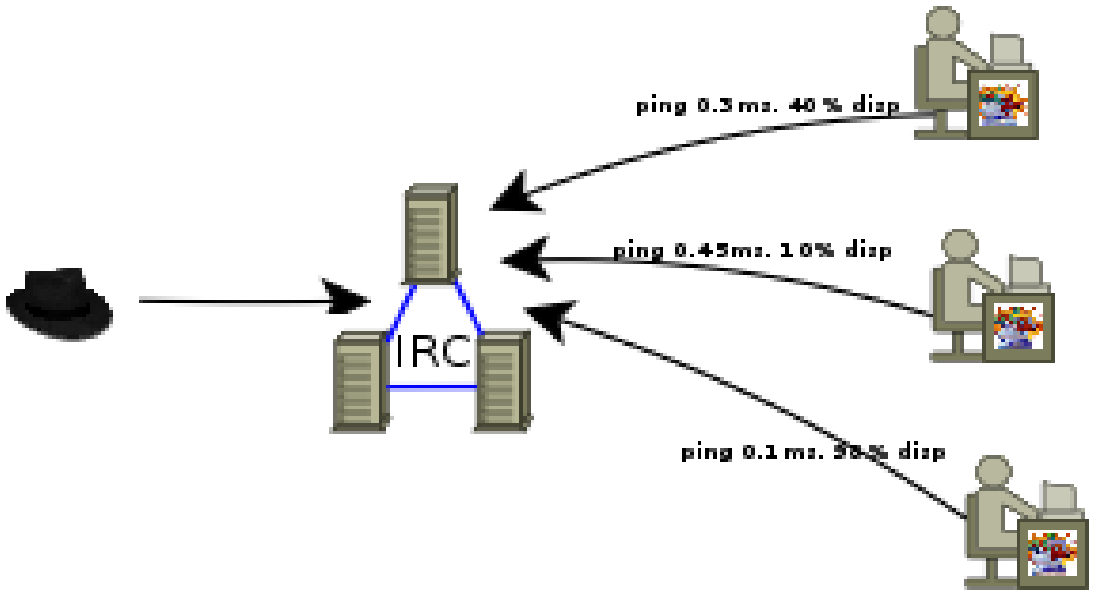
Botnets

- Como funciona?
  - 1) el botmaster propaga un virus con el software del bot incorporado.



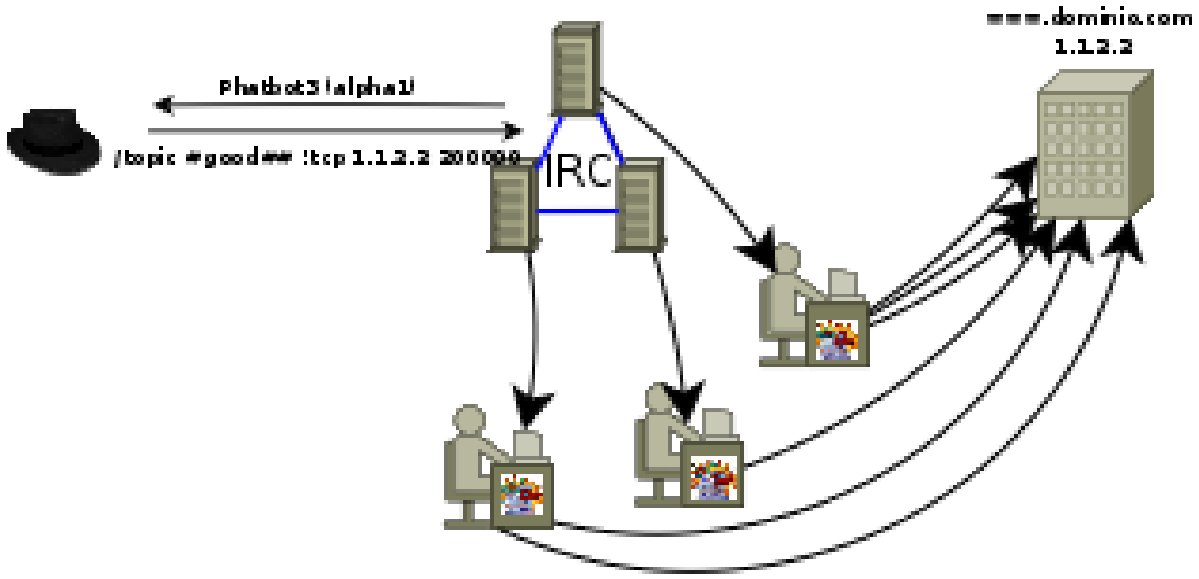
Botnets

- Cómo funciona?
  - 2) Los computadores infectados se conectan a una red de servidores (IRC, y en algunos casos web) controlada por el botmaster, se identifica y envía datos respecto de la calidad de enlace y disponibilidad.



Botnets

- Cómo funciona?
  - 3) El botmaster obtiene datos y da ordenes por medio de la red de servidores. Los computadores infectados ejecutan las ordenes que aparecen usualmente por PRIVMSG o TOPIC de IRC. Luego, comienzan a atacar.



Botnets

- Caso local
  - Lunes 5 de Mayo, ataque distribuido de denegación de servicio al host 74.54.58.76.
  - 79 estaciones UC participando en el ataque.
  - Al día siguiente se encuentran otras 141 estaciones de la UC infectadas intentando conectarse a la botnet.
  - La botnet contaba con casi 40 mil nodos online.
    - Capacidad de procesamiento estimada: 97 Tera Hertz
    - Capacidad de envío de datos : 45,6 Tera Bits / segundo

Botnets

- Consecuencias
  - Agotamiento de recursos de comunicación en los orígenes y el destino.
  - Pérdida de rendimiento en los equipos infectados.
  - Involucramiento en incidentes y sus consecuencias (listas negras, bloqueos, mala reputación, eventuales problemas legales, etc).

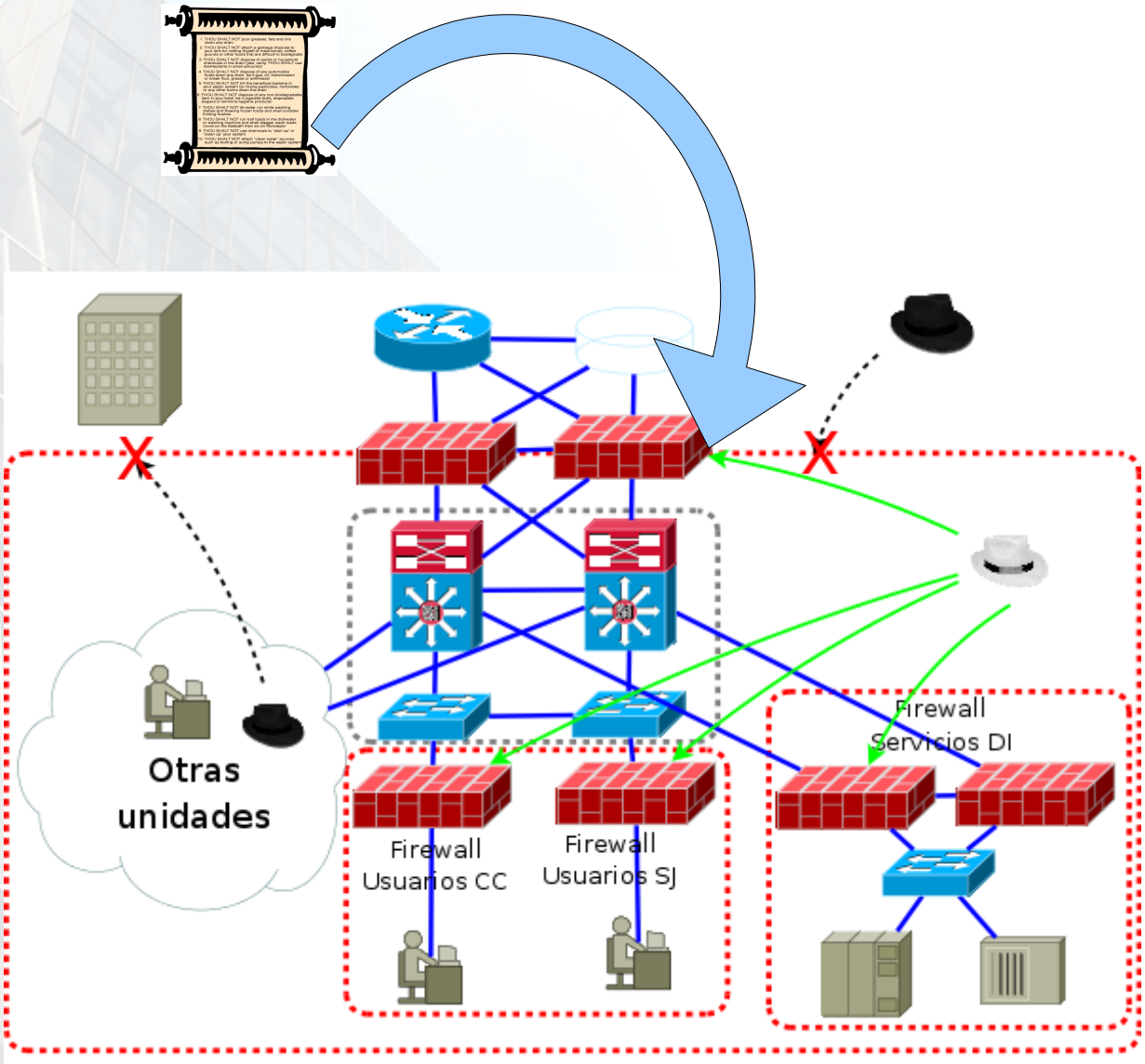
PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

DIRECCIÓN DE INFORMÁTICA

Política de uso de recursos computacionales y de comunicaciones

120 años
EN EL CORAZÓN DE CHILE

Política de uso de recursos computacionales y de comunicaciones



Política de uso de recursos

Pontificia Universidad Católica de Chile

- Define las normas de uso para los recursos computacionales que la Universidad dispone para la comunidad.
- Va en directa relación con sus objetivos y la normativa legal vigente.
- Considera el acceso libre a la información.
- Prohibe el uso de los recursos con fines que no guarden relación a los objetivos de la Universidad.

Dirección de Informática

120 años en el corazón de Chile

Política de acceso a internet

Pontificia Universidad Católica de Chile

Dirección de Informática

- Permitidos
  - Navegación Web (puertos 80, 8080, 443)
    - WebMail o correo web (Gmail, Live, yahoo!, etc).
    - Foros, blogs, prensa, Facebook, Youtube, MySpace etc.
    - Smtp autentificado.
  - Mensajería instantánea (MSN, Gtalk, Skype)

Política de acceso a internet

Pontificia Universidad Católica de Chile

Dirección de Informática

- No permitidos
  - Aplicaciones no web
    - Ares
    - Kazaa
    - Bittorrent
    - Juegos online
    - etc.
  - Envío de correo usando servidores de correo no pertenecientes a la UC (uso de SMTP puro para SPAM).
- Posibilidad de excepciones (justificadas).

120 años en el corazón de Chile

Consultas

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

DIRECCIÓN DE INFORMÁTICA

120 años
EN EL CORAZÓN DE CHILE