



# Seguridad en el Ámbito Académico: La Universidad de Los Andes

Nicolás Ruiz  
<nicolas@ula.ve>

# Seguridad ULA

- Diferencias con ISPs y redes corporativas
- Necesidades, Amenazas y soluciones.



# Qué los hace especial

- El requerimiento del usuario es simple: acceso total a la red.
- La red evolucionó “bottom-up”.
- El usuario es “dueño” de su equipo cliente.
- Autoridades prefieren no imponer limitaciones.



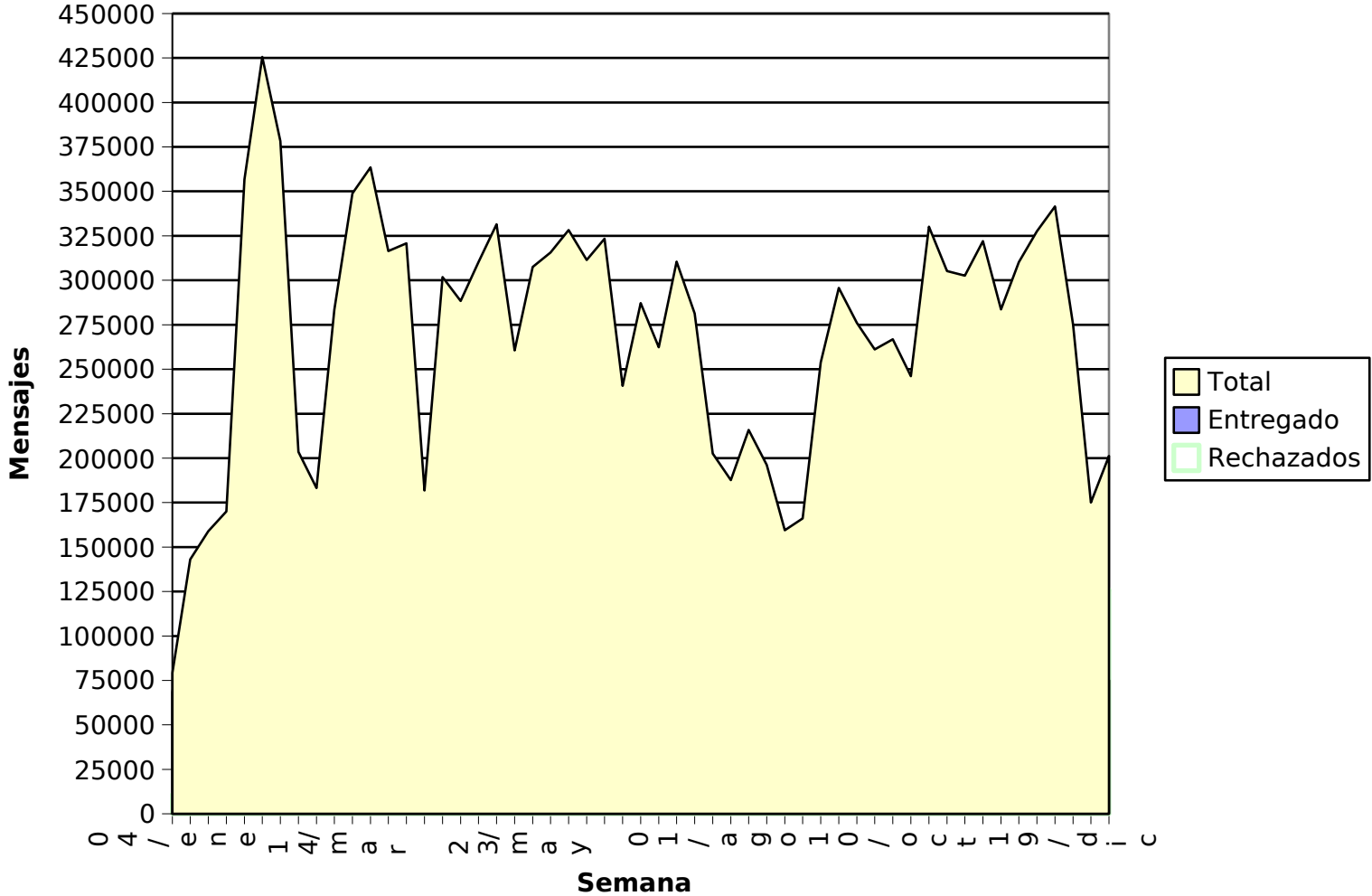
# Spam y Malware via Correo

- Etiquetado de Spam y filtrado de Malware (y ejecutables en general) desde primera mitad del 2004.
- Servidor de Correo: Sendmail.
- Antivirus: ClamAV.
- Antispam: Spamassassin.
- Varios Blacklists.
- Clientes acceden via HTTPS, IMAP sobre SSL, POP3 sobre SSL.



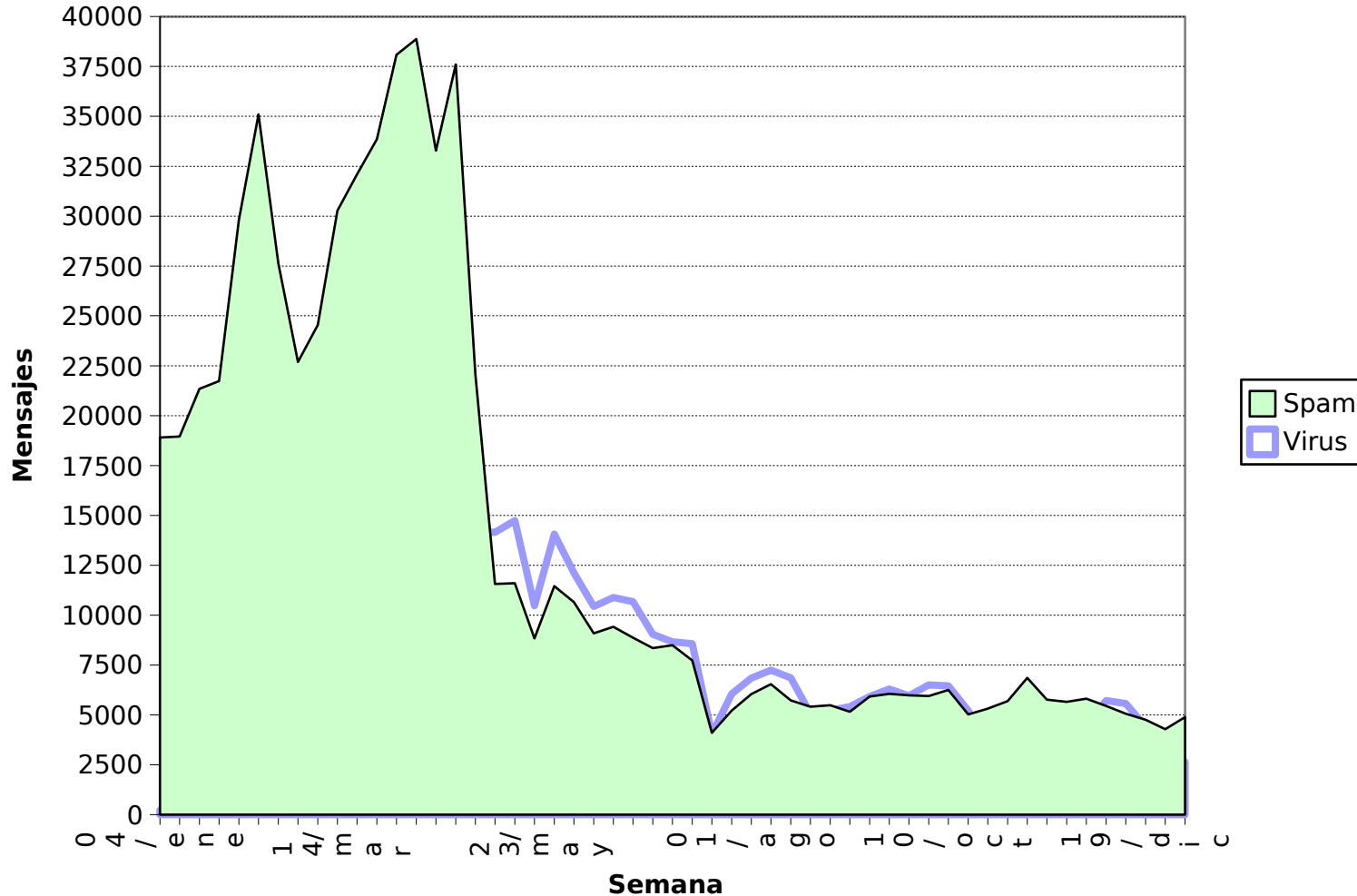
# Correo (por semana)

### Mensajes Procesados



# Mensajes con Virus/Spam

Mensajes con Virus / Spam



# Firewall/Antivirus en los clientes

- Históricamente: garantizar conectividad de red.
- Actualmente: conectividad, actualizaciones, firewall, antivirus.
- Filtrado en el servidor de correo y el antivirus/firewall en el cliente bajó el número de clientes infectados bajó de aprox. 60 a 2.



# Firewall de borde

- Se permiten conexiones a servicios locales y remotos bien conocidos (Destino es un “well known port”).
- Los usuarios pueden (y suelen) solicitar excepciones.
- No son buenos para avisar que las reglas ya no son necesarias.



# Firewall de borde (cont)

- Estadísticas Mayo 2006
  - Reglas Estáticas: 536
  - Reglas Dinámicas: 22692
  - Reglas Dinámicas activadas en un periodo de 25 días: 1002 (4.4%)
  - 16 reglas estáticas generan 18816 reglas dinámicas (1176 c/u (21\*56))
- Crecimiento de Reglas estáticas: 63% en un año.

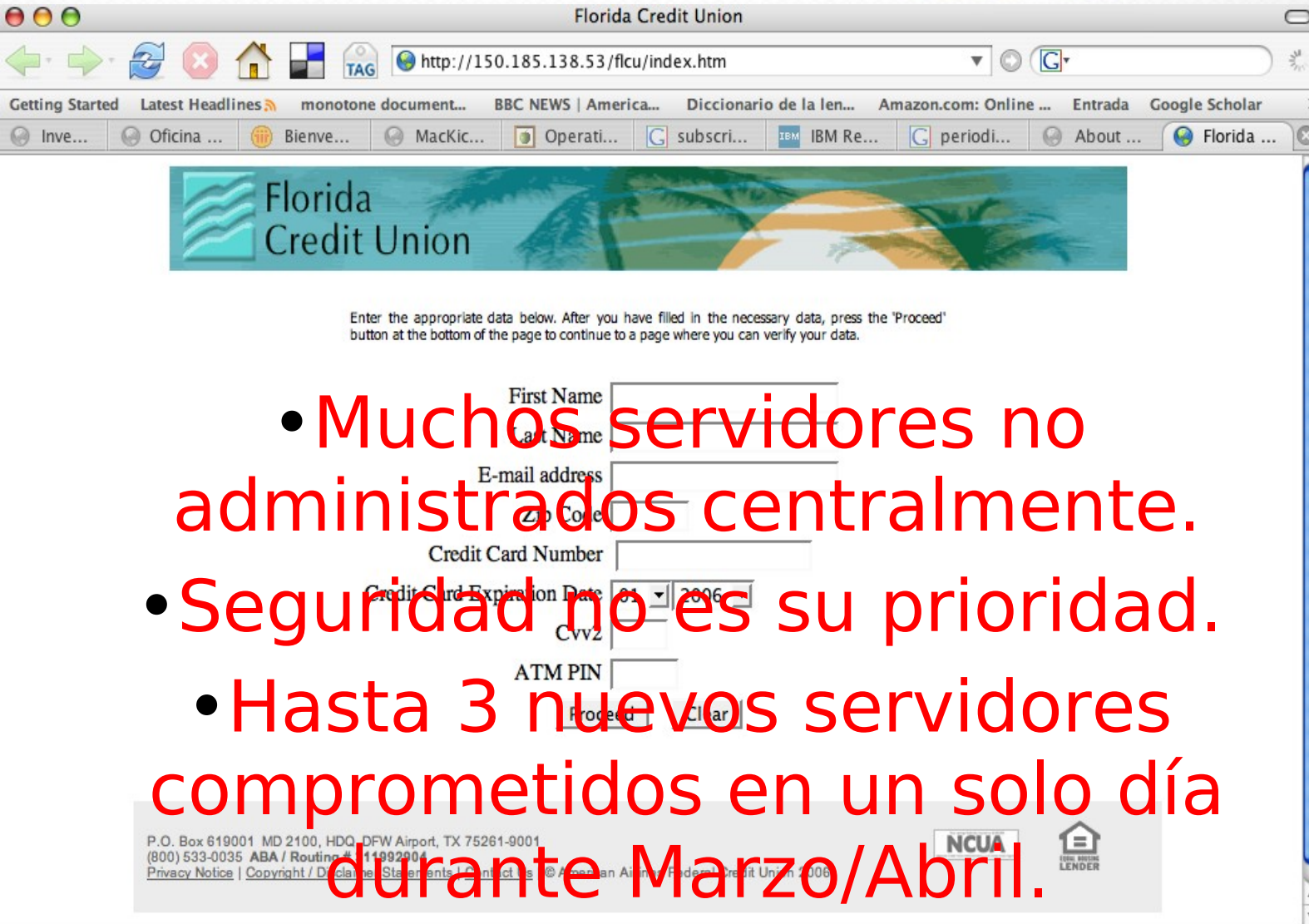


# Port Scanning y DDoS

- Suelen ser detenidos en los firewalls de borde.
- Algunos ataques son tan violentos que se necesita cooperación de los routers.



# Inyección PHP



Florida Credit Union

http://150.185.138.53/flcu/index.htm

Getting Started Latest Headlines monotone document... BBC NEWS | America... Diccionario de la len... Amazon.com: Online ... Entrada Google Scholar

Inve... Oficina ... Bienve... MacKic... Operati... subscri... IBM IBM Re... periodi... About ... Florida ...

Florida Credit Union

Enter the appropriate data below. After you have filled in the necessary data, press the 'Proceed' button at the bottom of the page to continue to a page where you can verify your data.

- Muchos servidores no administrados centralmente.
- Seguridad no es su prioridad.
- Hasta 3 nuevos servidores comprometidos en un solo día durante Marzo/Abril.

First Name

Last Name

E-mail address

Zip Code

Credit Card Number

Credit Card Expiration Date 01 2006

Cvv2

ATM PIN

Proceed Clear

P.O. Box 619001 MD 2100, HDQ DFW Airport, TX 75261-9001  
(800) 533-0035 ABA / Routing # 11992904  
Privacy Notice | Copyright / Disclaimer | Statements | Contact Us © American Airlines Federal Credit Union 2006

NCUA  
THE FEDERAL  
LENDER

