Optimización y aseguramiento de sitios web institucionales

Ing. Ernesto Pérez Estévez, Mg.
CSIRT CEDIA

Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia
www.cedia.edu.ec

Conferencista

- Ernesto Pérez Estévez
- CSIRT CEDIA

- Utilizando tecnologías de Software Libre desde 1995
- ~20 años trabajando con servidores de alojamiento y ambientes de alta concurrencia.

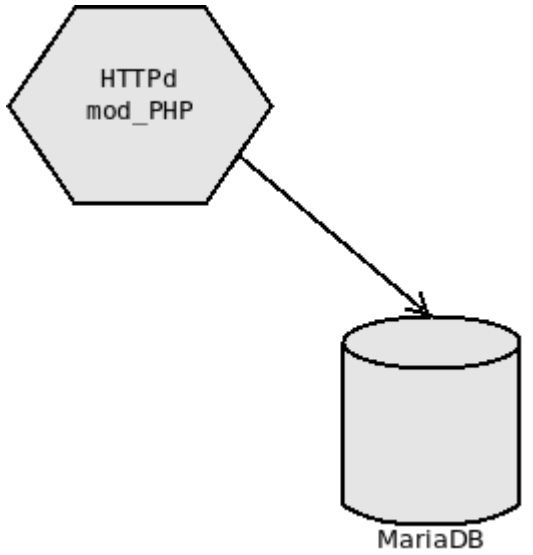
Agenda

- Instalación típica y problemas comunes
- Sobre soluciones técnicas
- Sobre el sitio web en sí
- Protecciones al sitio web
- Preparación ante emergencias
- Conclusiones

Instalación típica de sitio web

- Linux CentOS-7 o CentOS-6
- HTTPD de Apache
- PHP (Acostumbran REMI)
- MariaDB o MySQL
- Joomla o Wordpress

Problemas comunes

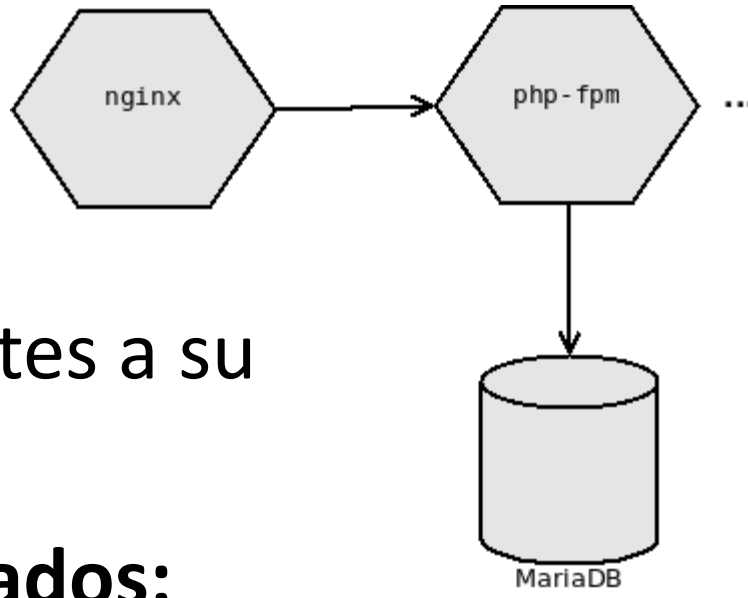


- Todos los servicios instalados por defecto
- Apache:
  - esquema de levantar hijos por cada petición (prefork)
  - propenso a recibir un ataque de DDOS
  - PHP como módulo de apache (mod_php)
- Respuestas lentas de MariaDB
- Alto consumo de recursos disco, procesador, RAM
- No uso de SSL

Soluciones tradicionales

- Aumentar recursos (RAM, CPU)
- Cambio a esquemas o sistemas difíciles de dominar en corto tiempo
- Mover a un sistema de cobro por uso de recursos

Soluciones efectivas

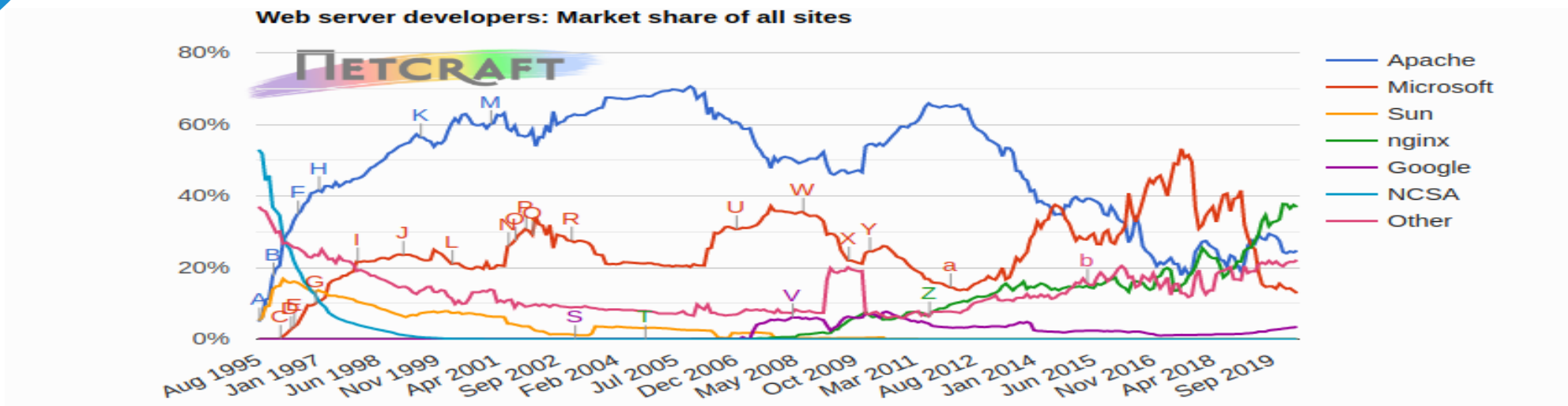


- Servidor web performante: **nginx**, con ligeros ajustes a su configuración tradicional

PHP separado del web: **php-fpm** con **ajustes mesurados:**

- cantidad de hijos y timeouts
- no instalar modulos de PHP innecesarios, sólo los que moodle solicite
- usar rpm de php de **CentOS-SCL** (rh-php73*)
- Instalar/activar optimizador/acelerador: **opcache, apcu**

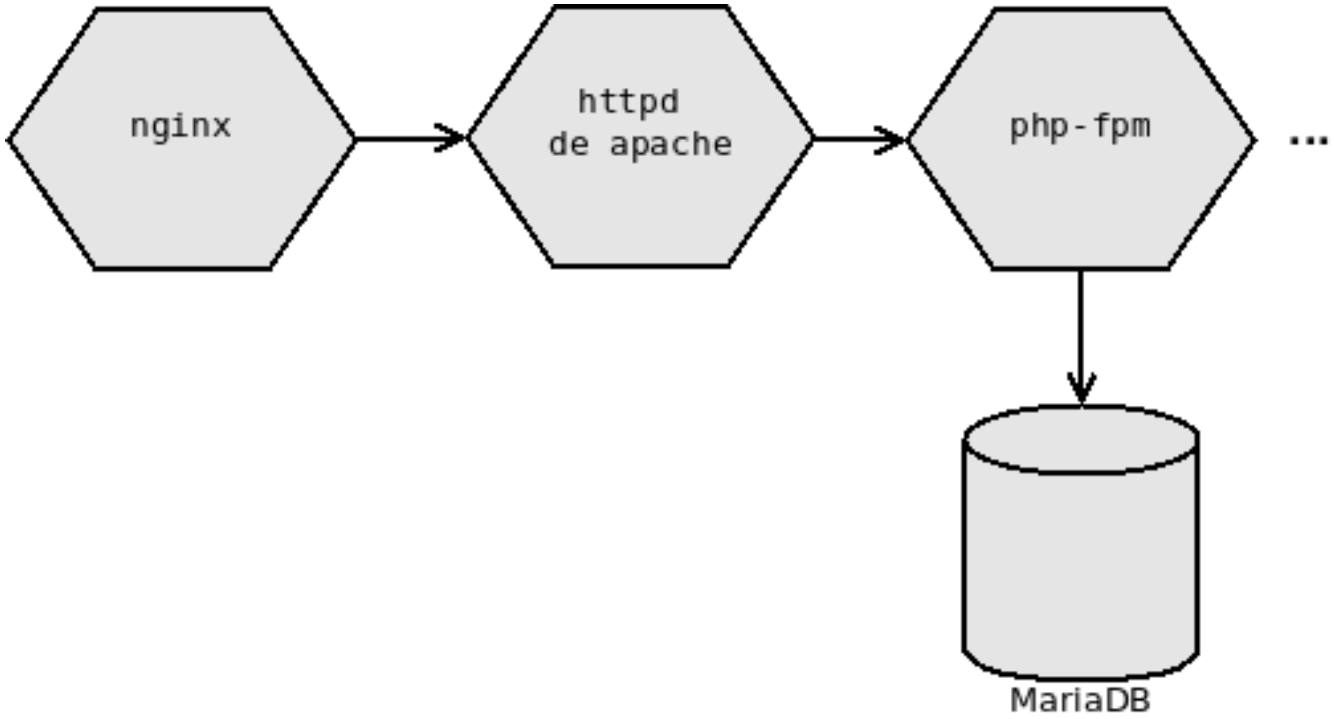
Soluciones efectivas



Developer	March 2020	Percent	April 2020	Percent	Change
nginx	473,308,955	37.47%	459,886,788	36.91%	-0.57
Apache	306,114,673	24.24%	308,143,708	24.73%	0.49
Microsoft	170,567,386	13.50%	160,121,865	12.85%	-0.66
Google	41,227,959	3.26%	42,648,748	3.42%	0.16

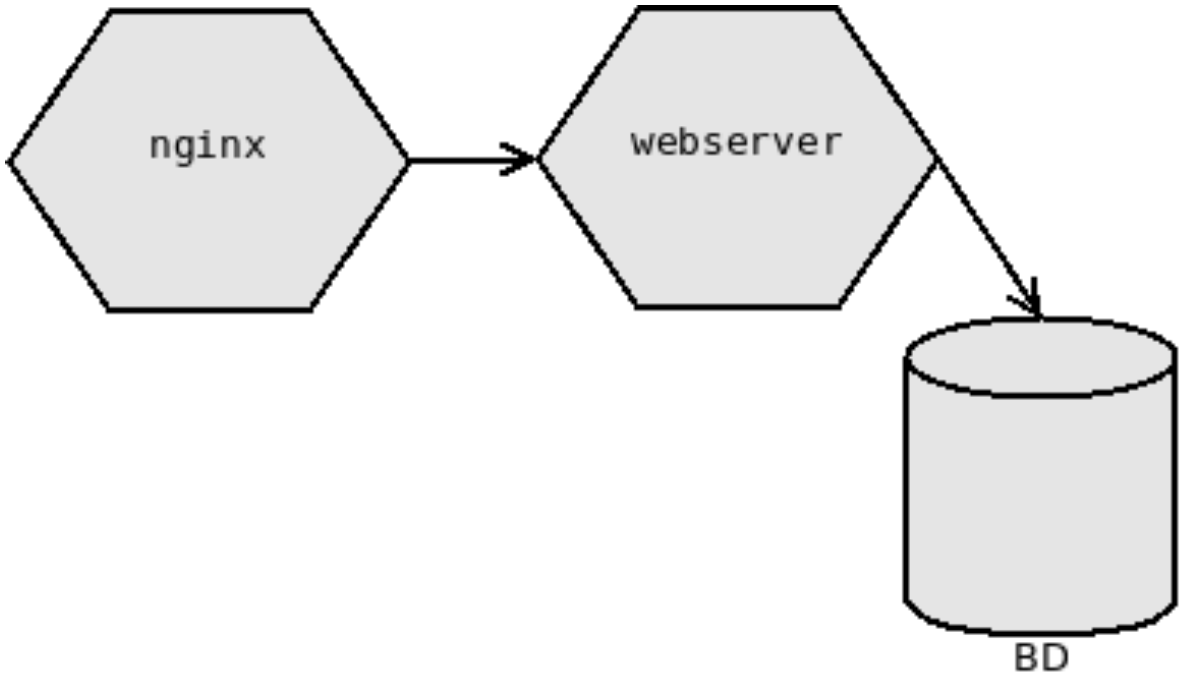
Variante proxy reverso

- **nginx → apache → php-fpm**



Variante proxy reverso

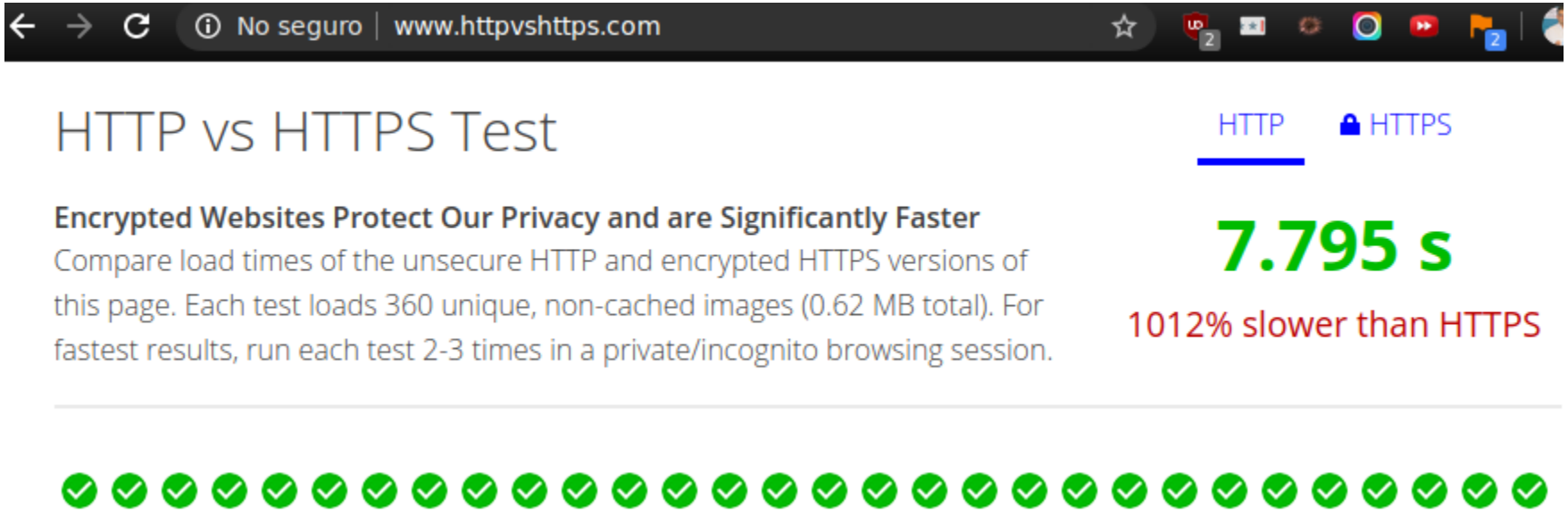
- **nginx → webserver**



...

Soluciones efectivas

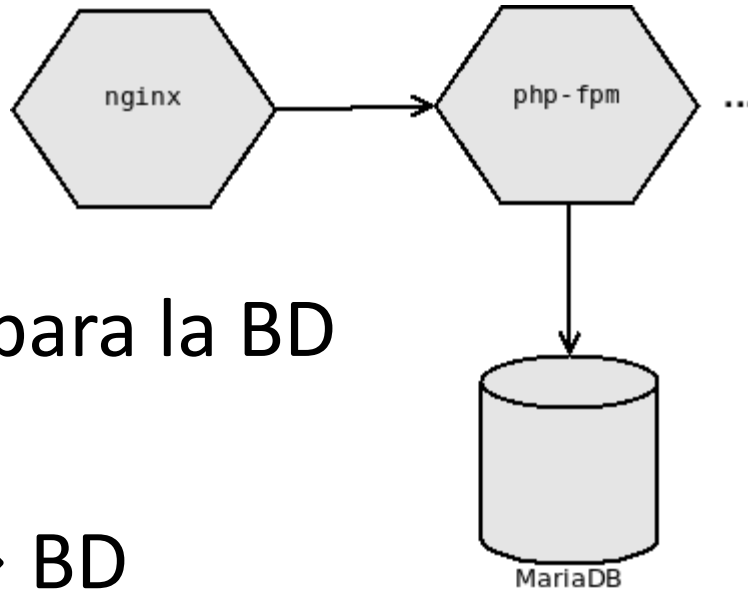
- **LetsEncrypt** para SSL



Soluciones efectivas

- **Sistema antiddos**
- **WAF : Web Application Firewall**
- **Monitoreo de uptime del sitio**
- **Monitoreo de cambios en el sitio**

Soluciones efectivas



- MariaDB → **query cache**, parámetros sensibles para la BD
  - Para ello podemos usar mysqltunner-Perl
- **Deshabilitar las conexiones persistentes** PHP → BD
- Revisar **estado de tablas** de la BD diariamente
- **Eliminar servicios innecesarios (y puertos innecesarios)**
- **Eliminar paquetes innecesarios** (ej: mlocate)

Sobre el sitio web en sí

- Casi todos (todos) se desarrollan dinámicos
- Tamaño del sitio web
- Compresión de páginas web
- Caché de otro contenido (imágenes, css, etc)

Protecciones mínimas sugeridas

- Proteger URL de administración
- Actualizar sitio continua y frecuentemente (en el contrato)
- Actualizar sistema operativo continua y frecuentemente
- Separar sistemas del sitio principal (sitios de reservas de laboratorios o espacios, sistemas académicos, lms)

Ser precavido

- Es el sistema que da la cara por la organización
- Debe respaldarse frecuentemente, ej:
  - rsnapshot
- Tener pequeño sitio estático alterno para emergencias

Conclusiones

- Manejar un server web es más que instalarlo... y ya.
- Al igual que cualquier sistema universitario, requiere de atención y cuidado continuo.

- En CEDIA estamos para apoyarlos

¿Preguntas?

Ing. Ernesto Pérez Estévez, Mg.

CSIRT CEDIA

ernesto.perez@cedia.org.ec

https://csirt.cedia.org.ec