



4^o

Coloquio de proyectos
de Becarios en Seguridad Informática

Migración de servicios de correo y LDAP

Campuzano Barajas José Daniel
Morales Perales Nayely

Agenda



Objetivo

Actualizar el sistema operativo junto con los servicios de correo electrónico Postfix y autenticación OpenLDAP.



Propósito

Cumplimiento con las políticas del SGSI.

Evitar la obsolescencia de los sistemas.

Seguridad preventiva.

Descripción del Proyecto

- Instalación previa.
 - Servidor de correo Postfix.
 - LDAP
- Migración.
 - Actualización de los paquetes asociados a los servicios.

Servidor de Correo Antecedentes

Postfix SMTP (TLS)

ClamAV

SpamAssassin

IMAP (SSL)

Dovecot

Interfaz web Horde (HTTPS)

Repositorio de llaves públicas.

LDAP Antecedentes

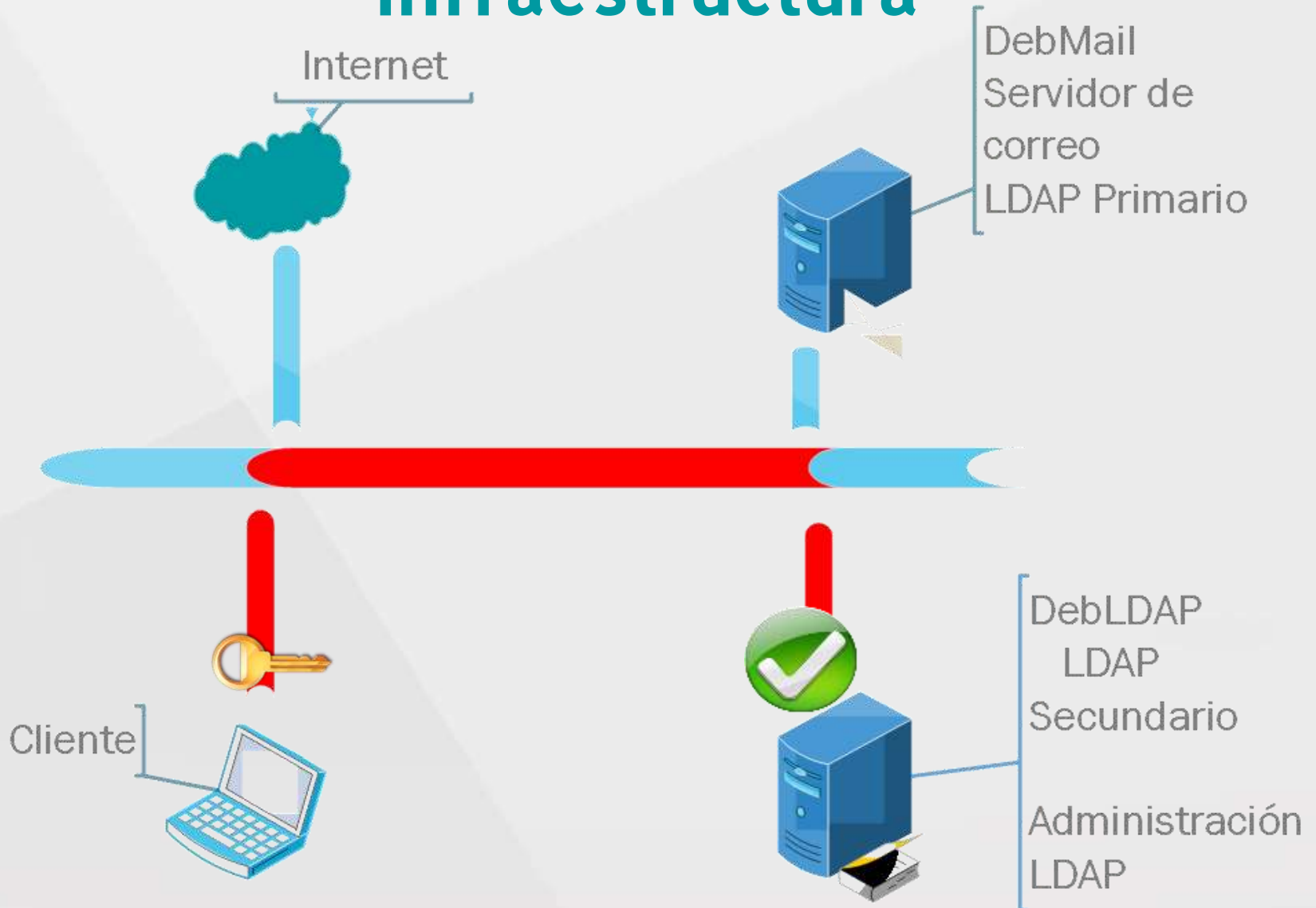
LDAP Principal

- Servidor de correo

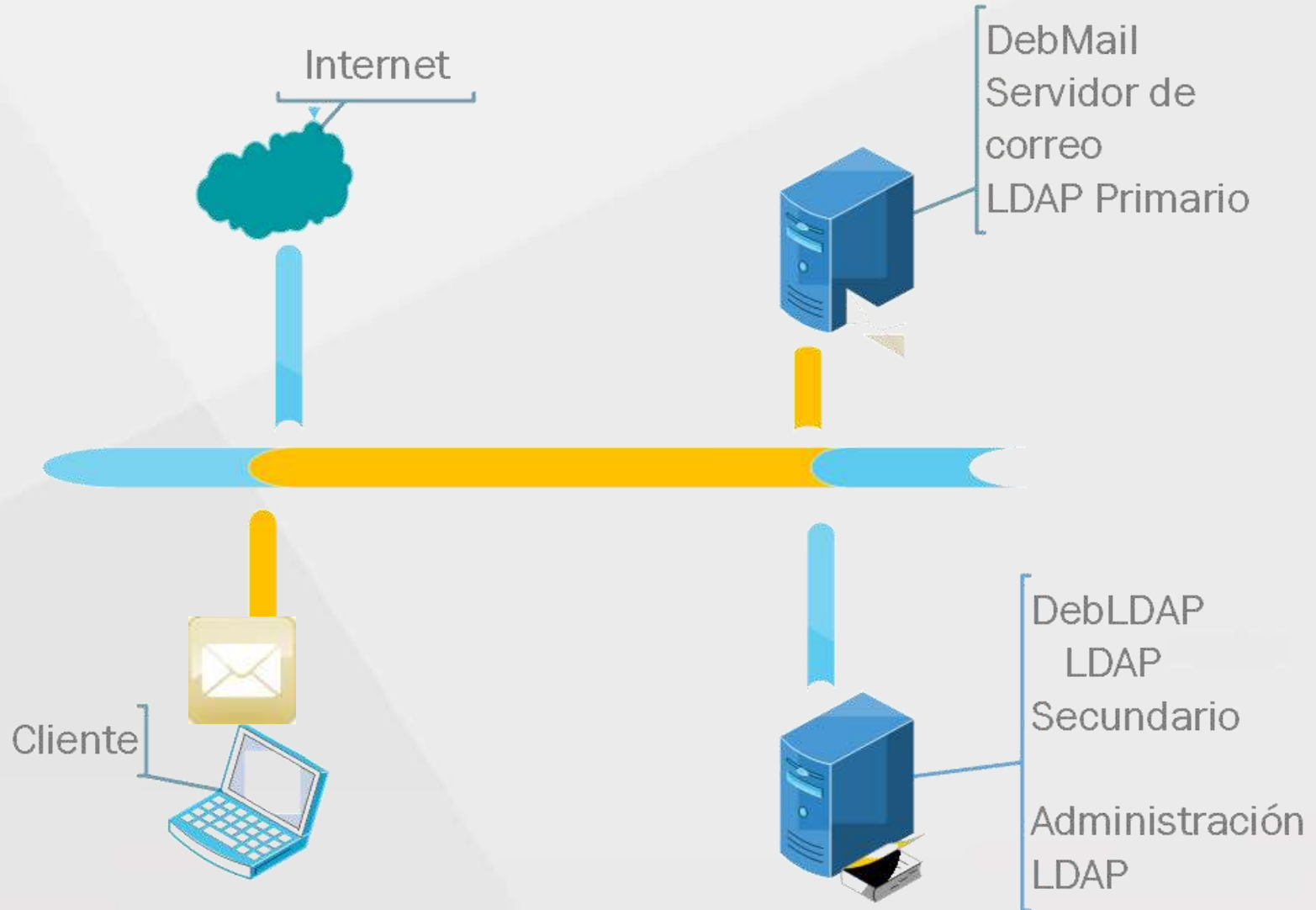
LDAP Secundario

- Autenticación
- Réplica
- Administración de cuentas de usuarios
- Reseteo de contraseñas

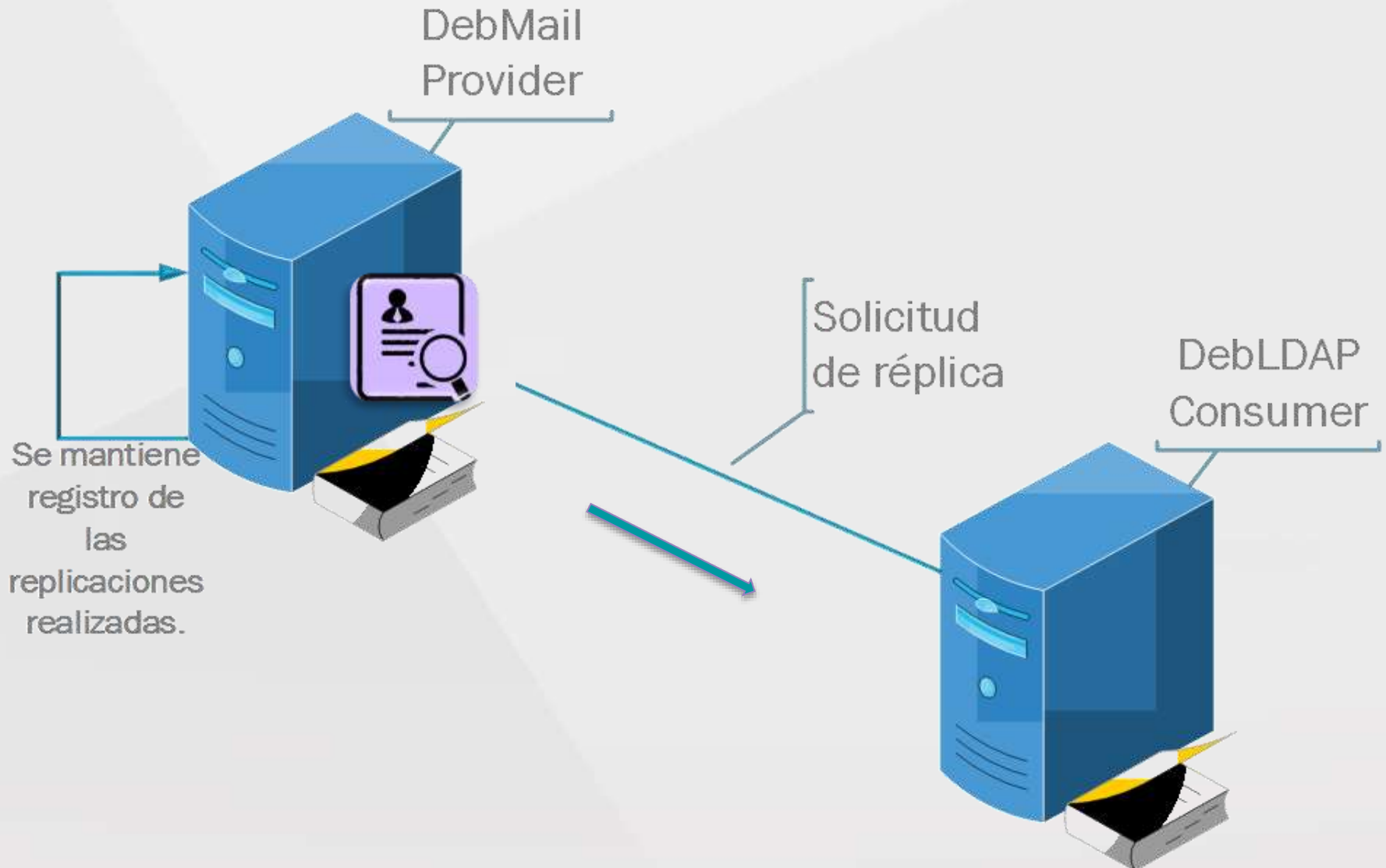
Infraestructura



Infraestructura



Módulo para replicación



LDAP Account Manager



LDAP Account Manager LAM configuration

LAM Login

User name: admin
Password:
Language: English (Great Britain)

LDAP server: ldap://deb@mail.seguridad.mx
Server profile: lam

LDAP Account Manager - 4.7.1 (Logged in as: admin > seguridad > unam > mx) Tree view Tools Help Logout

Users Groups Hosts Samba domains

User count: 8

Select all	User name	First name	Last name	UID number	GID number
<input type="checkbox"/>	bseguridad	becuno	seguridad	10000	10000
<input type="checkbox"/>	dcampuzano	daniel	campuzano	10003	10000
<input type="checkbox"/>	dvalverde	diego	valverde	10005	10000
<input type="checkbox"/>	ncarami	naome	carami	10006	10000
<input type="checkbox"/>	nmorales	nayely	morales	10004	10000

Módulo de autenticación de usuarios



Ventajas

- **Control de acceso global**
- **Rápida lectura de registros**
- **Política de contraseñas**

Self Service Password

Autoservicio de Reseteo de Contras...

Autoservicio de Reseteo de Contraseñas



Su nombre de cuenta es requerida

Ingrese su contraseña anterior y elija una nueva.
Si necesita ayuda, contacte al administrador

Cuenta

Contraseña anterior

Contraseña nueva

Confirme contraseña nueva

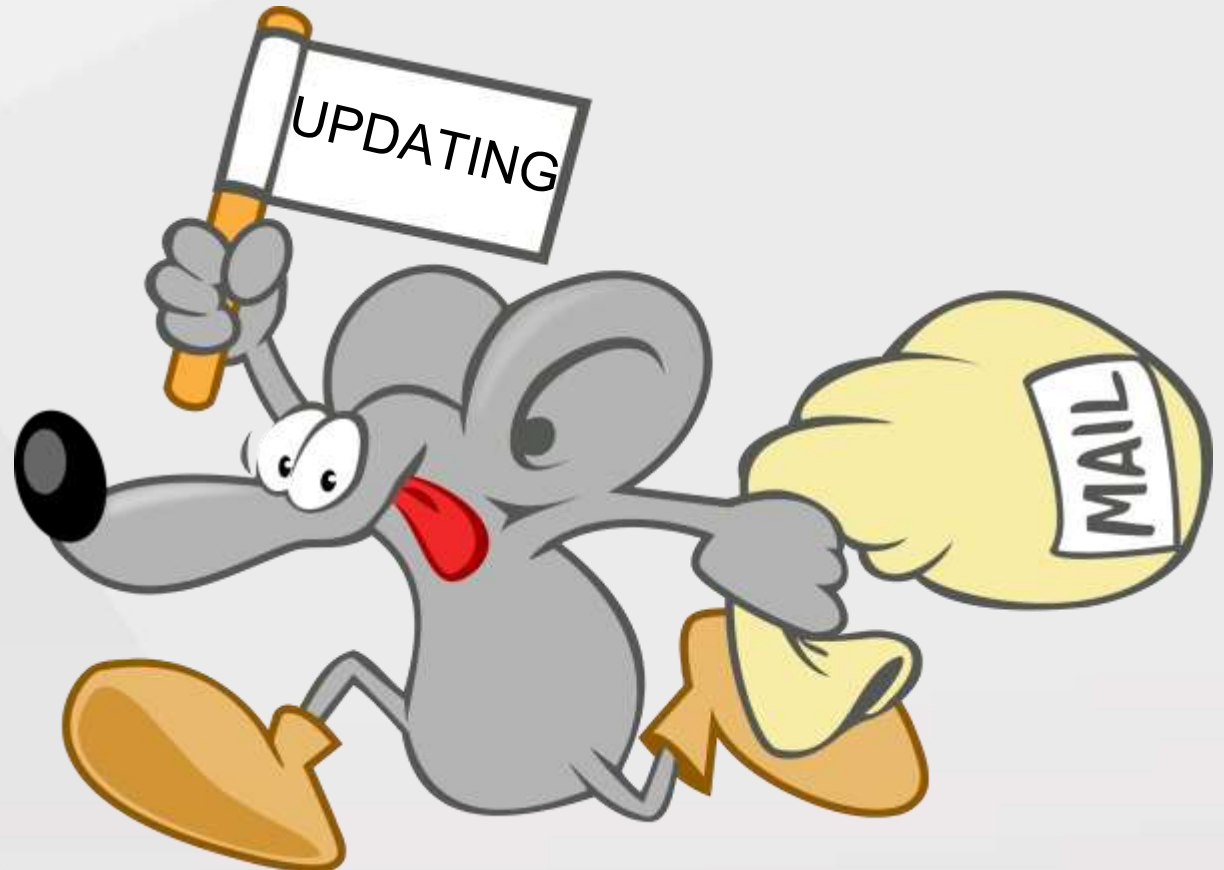
Enviar

Migración: Debian 8

- Actualización de paquetes de Debian 6
- Adaptación de configuraciones.
 - LDAP (Primario y réplica)
 - Correo electrónico
- Mantener cuotas
 - Usuarios
 - Tamaño de archivos adjuntos.

Migración servidor de Correo

Actualización de *Postfix*



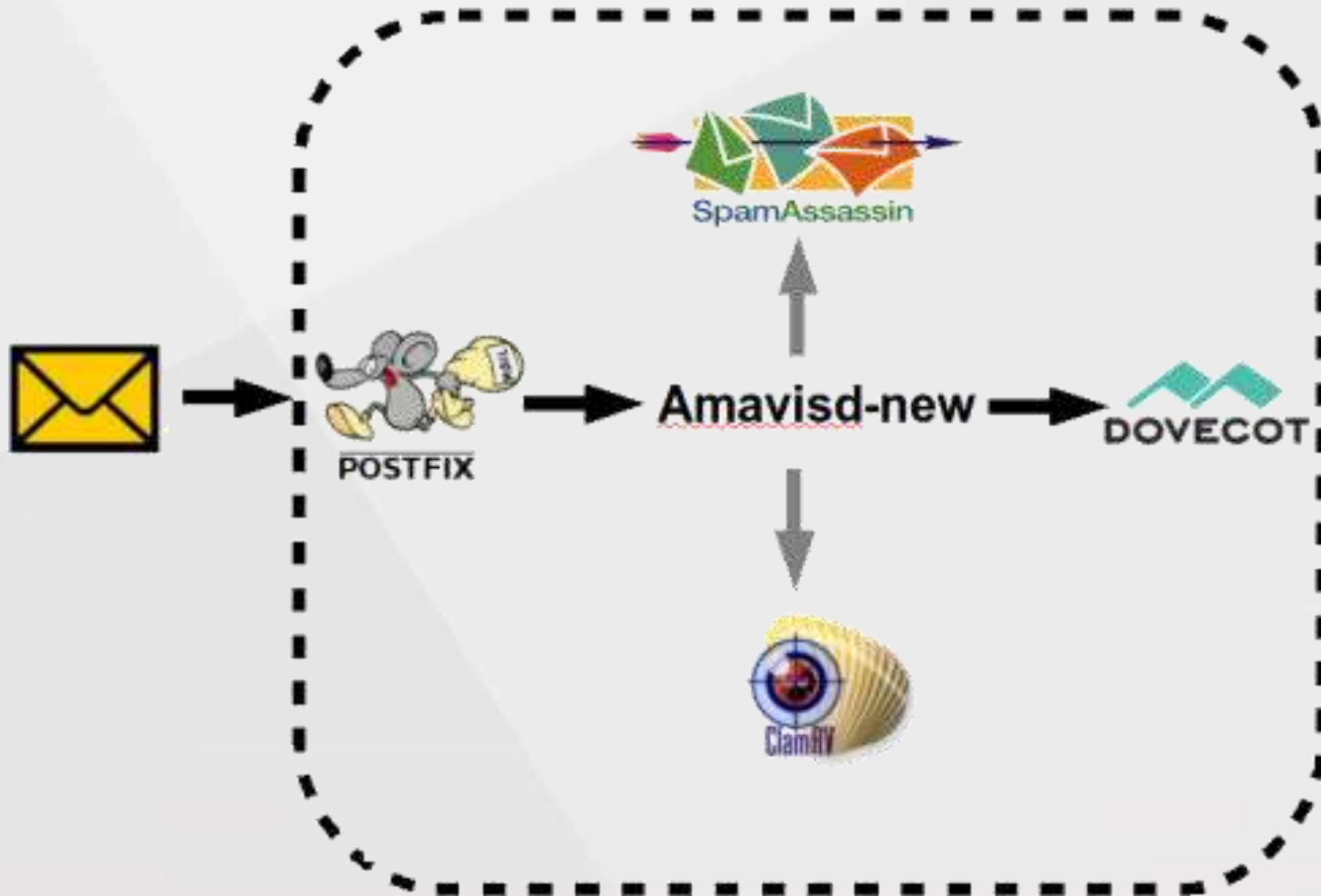
Migración de servidor IMAP

Actualización de *dovecot*.

Cambio en la estructura de los archivos de configuración.



Protección Anti-virus y Anti-spam



Horde 5

The screenshot shows the Horde 5 administration interface. The browser address bar displays `http://coneos8.seguridad.unam.mx/horde/admin/config/`. The page header includes the Horde logo, version 5.2.2, and navigation menus for Mail, Calendar, Address Book, Tasks, Notes, and Others. A sidebar on the left lists various system components like Configuration, Users, Groups, Permissions, Locks, Alarms, Sessions, PHP Shell, SQL Shell, and CLI. The main content area features a 'Check for newer versions' button and a table listing installed applications and their database schema status.

Application	Database
Horde Groupware Webmail Edition 5.2.2	
Address Book (turba) 4.2.2	✓ SQL DB schema is ready
Bookmarks (traan) 1.1.1	✓ SQL DB schema is ready
Calendar (ironolith) 4.2.2	✓ SQL DB schema is ready
content 2.0.4	✓ SQL DB schema is ready
File Manager (gallem) 3.0.3	✓ SQL DB schema is ready
Filters (ingo) 3.2.1	✓ SQL DB schema is ready
Horde (horde) 5.2.1	
Mail (im) 5.2.3	✓ SQL DB schema is ready
Notes (horde) 5.2.1	✓ SQL DB schema is ready
Tasks (nag) 4.2.1	✓ SQL DB schema is ready
timeobjects 2.1.0	

Repositorio de llaves

Keyserver CSI - UNAM / CERT

Subir Clave

Listar todas las claves

Descargar bloque de claves

Buscar una llave pública

Cadena de búsqueda:

¿Cómo deseas realizar la búsqueda?

- Busca por nombre o dirección de correo electrónico
- Busca por nombre o dirección de correo electrónico *y muestra el índice de claves y subclaves*
- Buscar por el hash de la llave pública
- Buscar por el hash de la llave pública *y obtén bloque de claves*

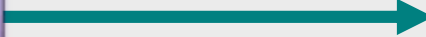
Limpiar

Enviar



Migración de base de datos de LDAP

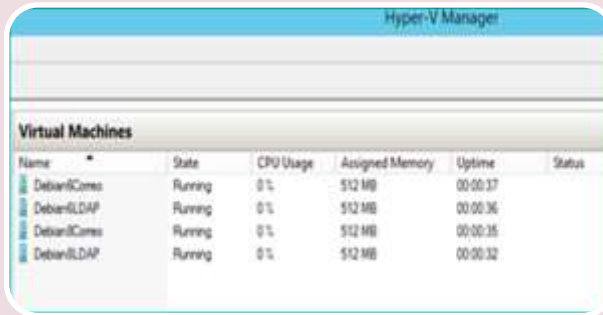
Deb6mail
-slapcat



Deb8mail
-slapadd



Resultados



Hyper-V Manager

Virtual Machines					
Name	State	CPU Usage	Assigned Memory	Uptime	Status
Debian8Cores	Running	0%	512 MB	00:00:37	
Debian8LDAP	Running	0%	512 MB	00:00:36	
Debian8Cores	Running	0%	512 MB	00:00:35	
Debian8LDAP	Running	0%	512 MB	00:00:32	



Ambientes
funcionales

- Debian 6
- Debian 8

Metodología
de la
migración
documentada.

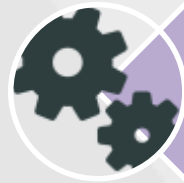
Conclusiones



Cumplimiento de las políticas
SGSI



Mitigar riesgos de seguridad



Mejora de funcionalidad.



Ambiente controlado de pruebas
para evitar fallos a gran escala

GRACIAS

Campuzano Barajas José Daniel

jose.campuzano@cert.unam.mx

Morales Perales Nayely

nayemoralesp@gmail.com