Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# Prácticas de Seguridad Aplicadas a Escenarios de Autenticación

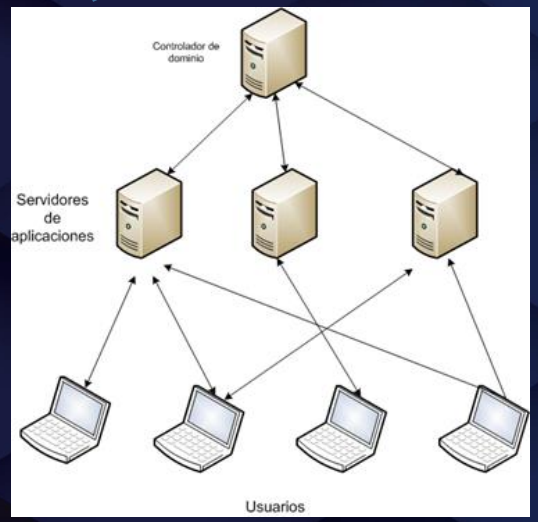
Congreso Internacional de DESARROLLO DE SOFTWARE

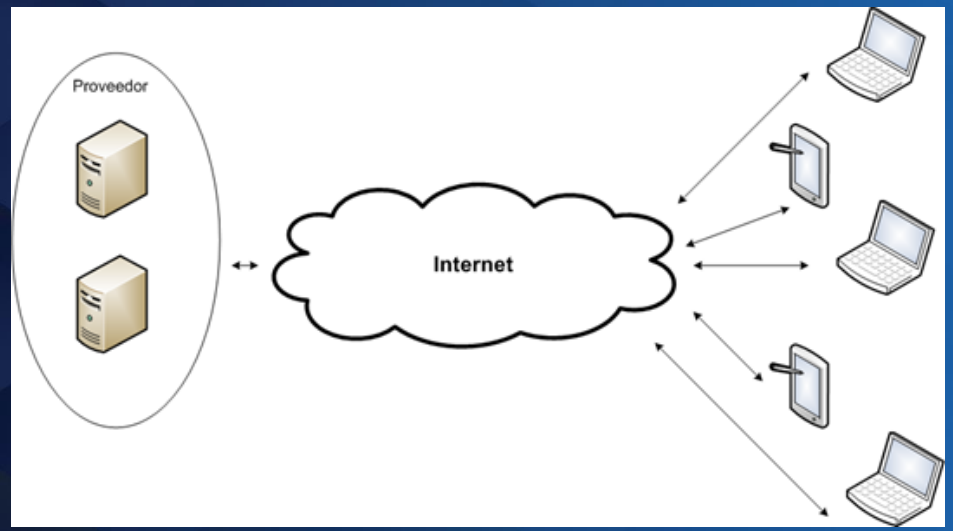
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# INTRODUCCIÓN




Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# OBJETIVO DEL ESTUDIO

## Escenarios Analizados

- Servicios sobre una Red Corporativa
- Servicios Publicos en Internet
- Servicios Corporativos en la Nube

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# OBJETIVO DEL ESTUDIO

## Análisis de requisitos
## Requisitos comunes a todos los escenarios

- Requisitos de Seguridad
  - Manejo de Contraseñas
  - Seguridad Física
  - Separación de Ambientes
  - Firewall de Aplicación
  - Cuentas de Servicio
  - Single Sign On
  - VPN
  - SSL
  - Certificados Digitales
  - Múltiple Factor
- Requisitos Funcionales y Operativos
  - Alta Disponibilidad
  - Conexiones de Respaldo
  - Backups
  - Gestión de Usuarios
  - Logs  y Auditoria
  - Manejo de fallas de servicio
  - Plan de recuperación de desastres

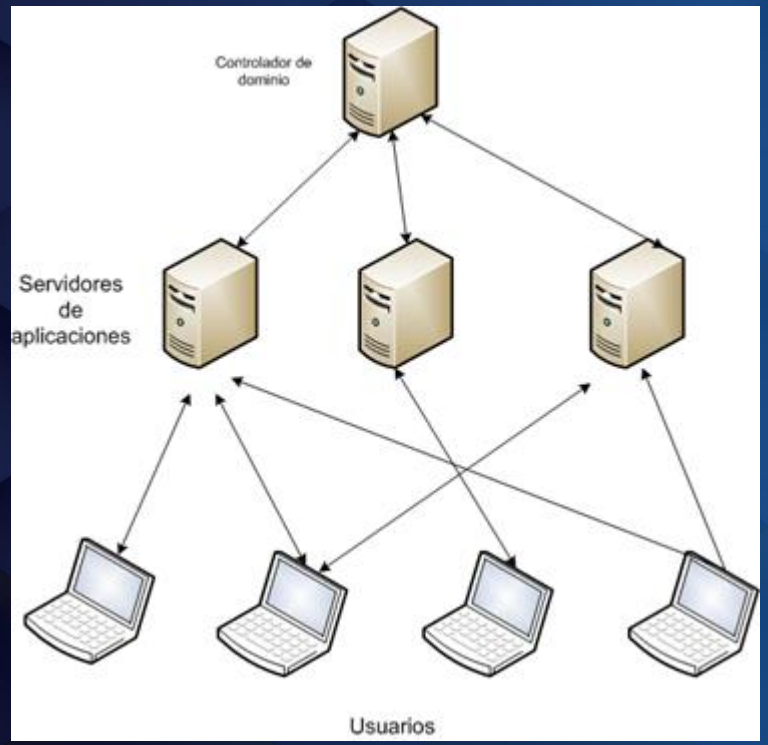
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Análisis de requisitos
## Requisitos para Servicios sobre una red Corporativa




Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

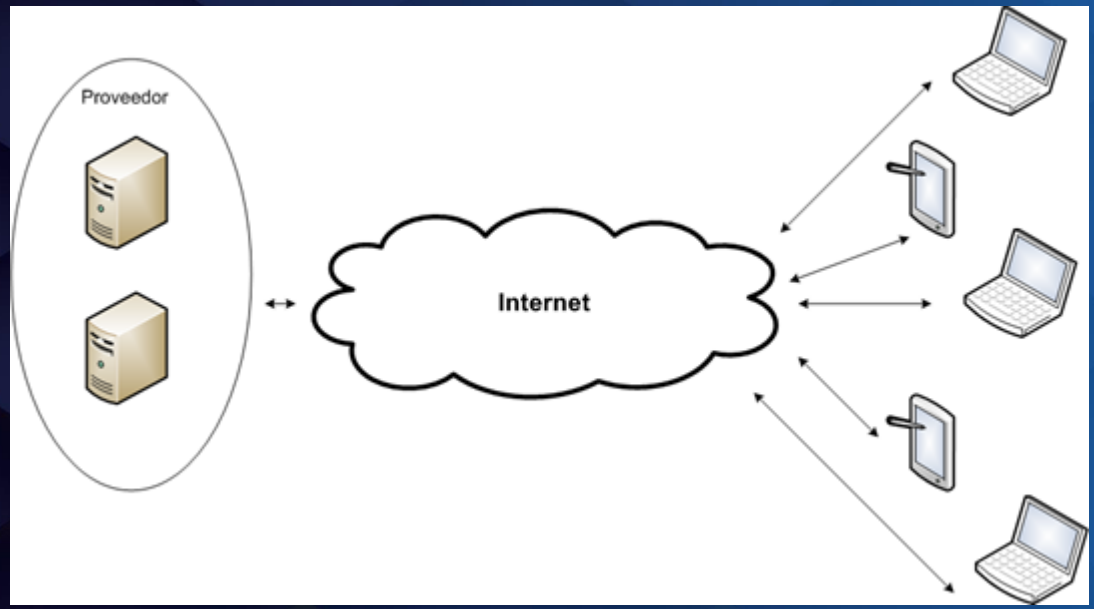
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Análisis de requisitos

## Requisitos para Servicios públicos en Internet




Congreso Internacional de DESARROLLO DE SOFTWARE

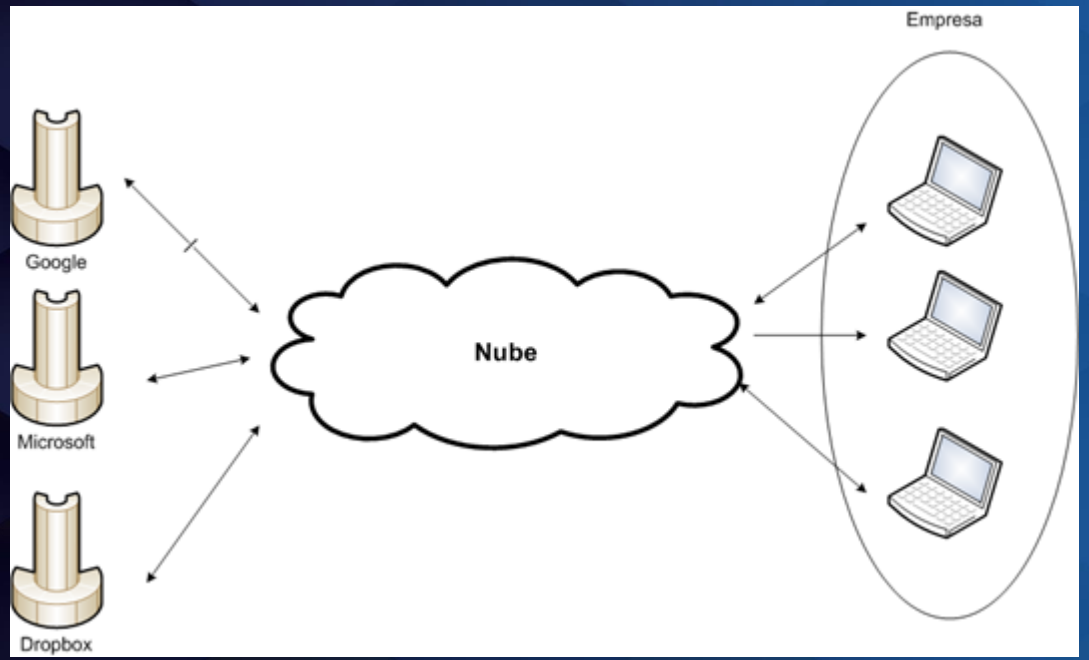
Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Análisis de requisitos
## Requisitos para Servicios Corporativos en la Nube




Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA



# Prueba de Concepto de los escenarios

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

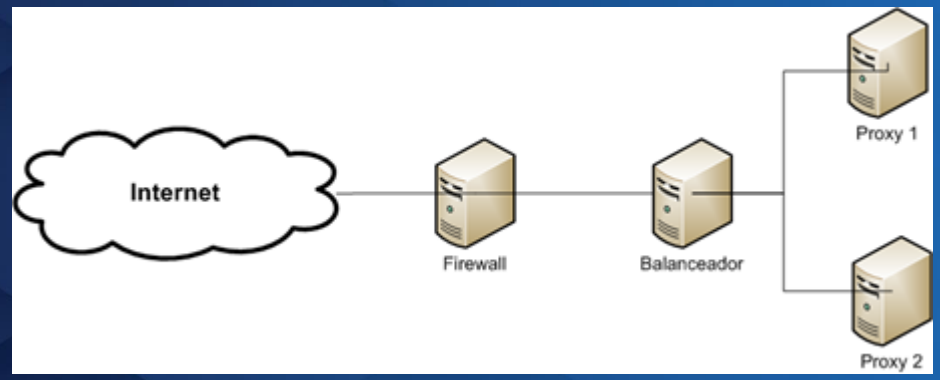
## Servicio Corporativo con doble Factor: CA Strong Authentication

| | |
|---|---|
| **Prueba de concepto** | **Autenticación con doble factor para acceso de escritorios virtuales CITRIX** |
| **Escenario Aplicado** | Servicios sobre una red Corporativa |
| **Software Involucrado** | • Windows Server 2012<br>• MS SQL Server 2012<br>• CA Strong Authentication 8.1<br>• Citrix Server<br>• Tomcat<br>• Apache |
| **Descripción** | Servicio de escritorios virtuales accedido por usuarios externos |

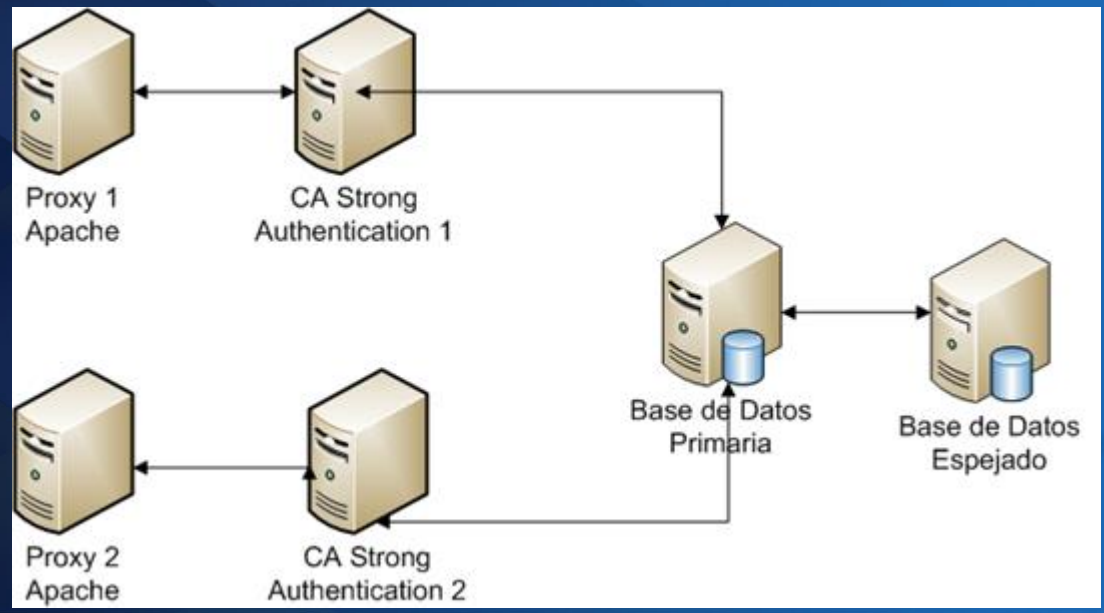
# RESULTADO Y DISCUSIONES

## Servicio Corporativo con doble Factor: CA Strong Authentication

**Acceso desde Internet**




**Arquitectura**



Instituto Superior Tecnológico del Azuay

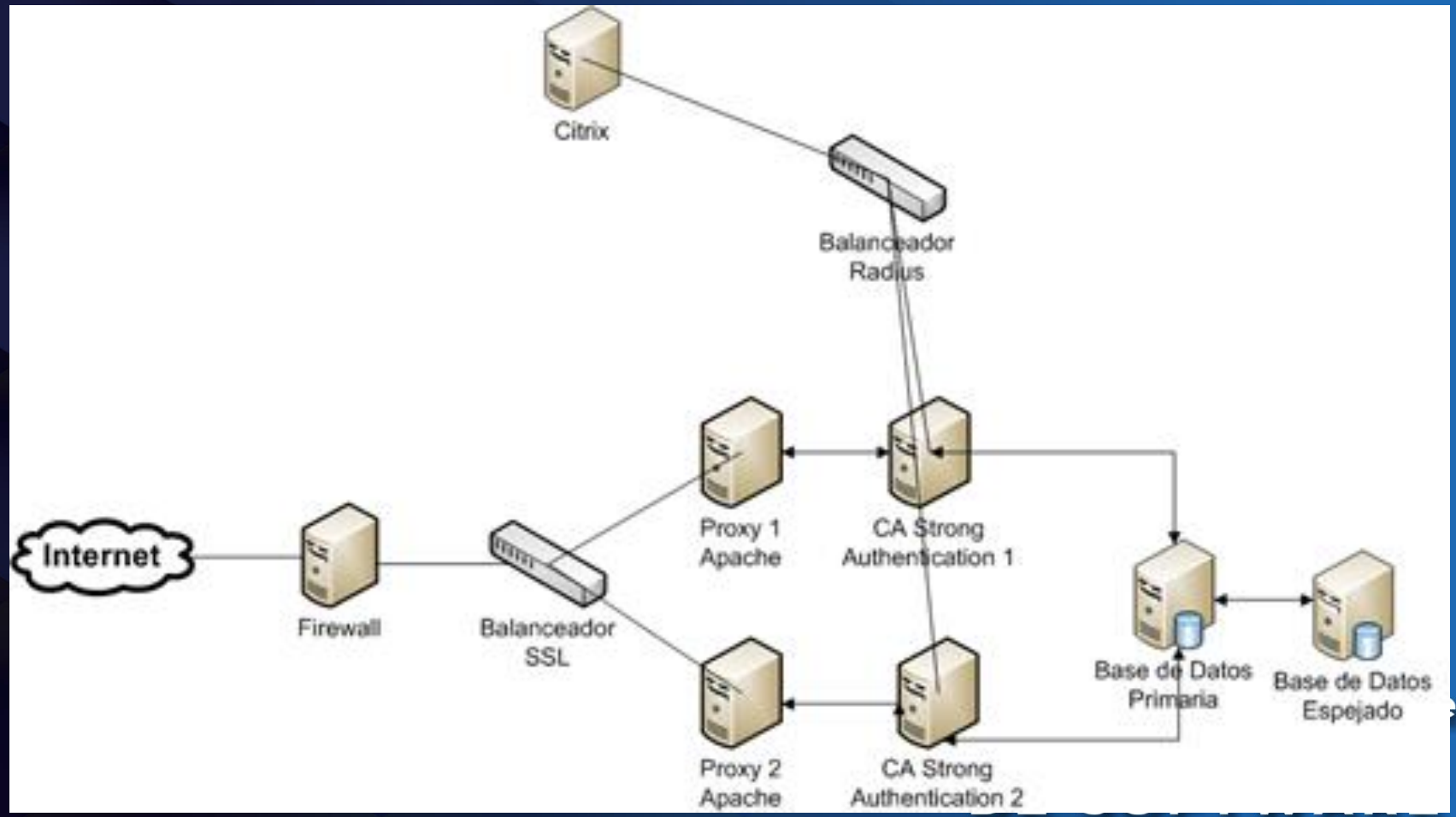
CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Servicio Corporativo con doble Factor: CA Strong Authentication

**Arquitectura**



Instituto Superior Tecnológico del Azuay

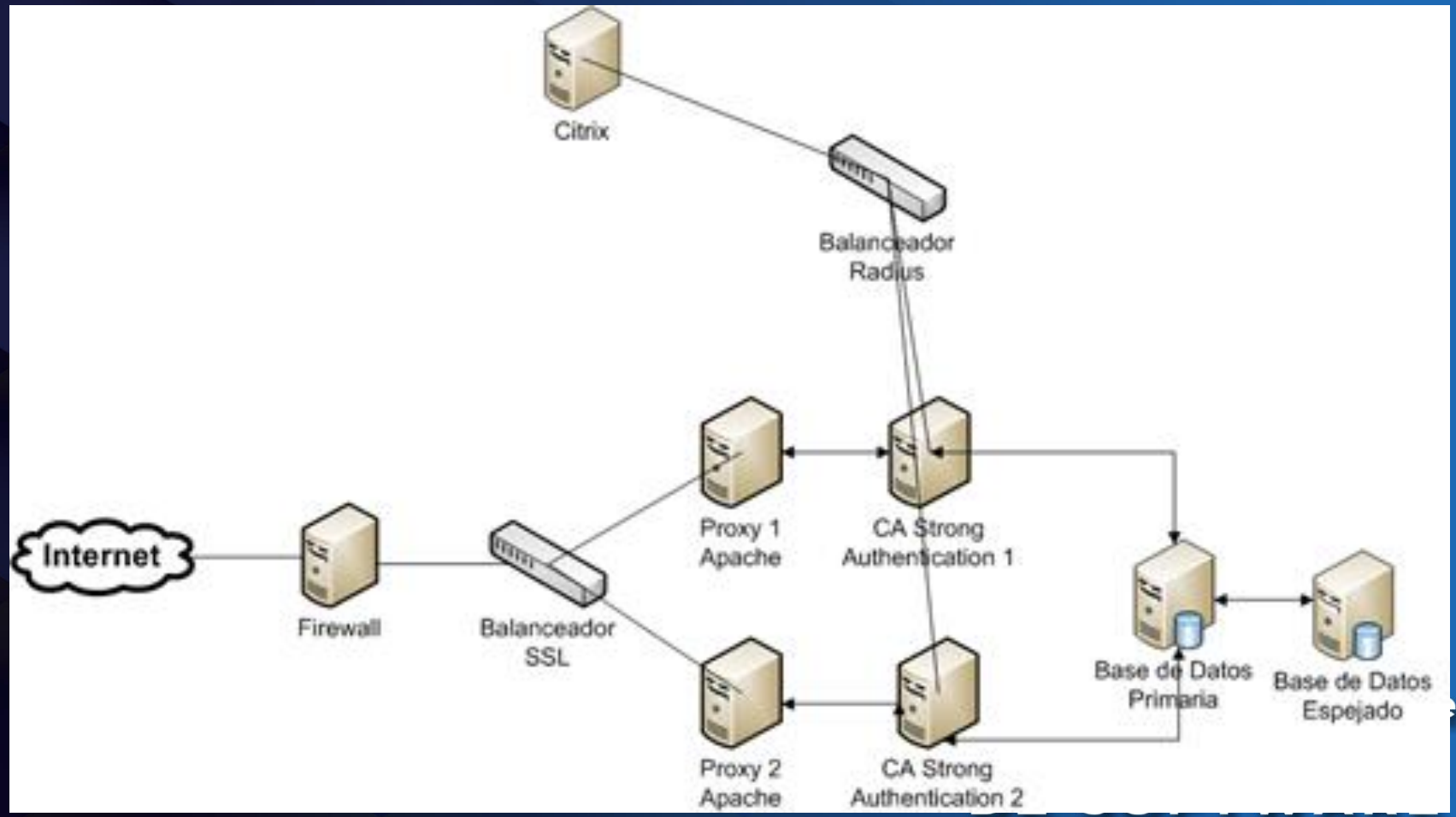
CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Servicio Corporativo con doble Factor: CA Strong Authentication

**Arquitectura**



Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Servicio Corporativo en la nube: Federación con ADFS 2.0

| | |
|---|---|
| **Prueba de concepto** | **Federación de identidad entre dos organizaciones** |
| **Escenario Aplicado** | Servicios corporativos en la nube |
| **Software Involucrado** | • Windows Server 2012<br>• Active Directory<br>• ADFS 2.0<br>• DUOS |
| **Descripción** | Federación de identidad entre dos organización implementando un segundo factor de autenticación |

Congreso Internacional de DESARROLLO DE SOFTWARE

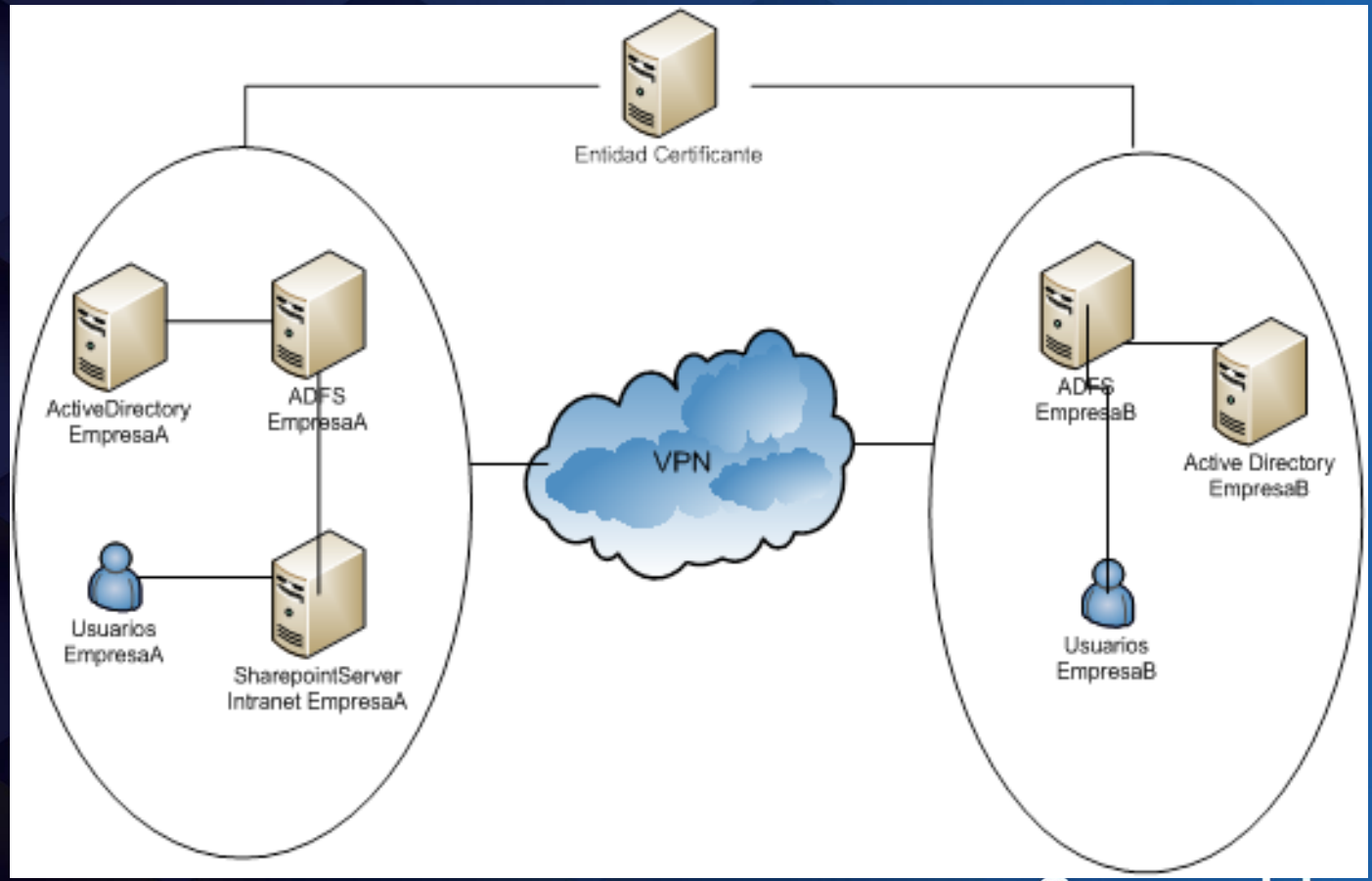
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Servicio Corporativo en la nube: Federación con ADFS 2.0




Congreso Internacional de DESARROLLO DE SOFTWARE

# RESULTADO Y DISCUSIONES

## Catalogo de Recomendaciones

Para todos los escenarios

**Funcionales y Operativas**

| | |
|---|---|
| **RG-FO-01** | Servidor Secundario |
| **RG-FO-02** | Comunicaciones |
| **RG-FO-03** | Backup<br><br>Política de backups periódicos<br><br>Seguridad física.<br><br>Almacenamiento Offsite |
| **RG-FO-04** | Time Server |
| **RG-FO-05** | Gestión de Usuarios |
| **RG-FO-06** | Auditoría y Control Interno del proceso |
| **RG-FO-08** | Manejo de Fallas de Servicio |
| **RG-FO-09** | Plan de Recuperación de Desastres |

# RESULTADO Y DISCUSIONES

## Catalogo de Recomendaciones

Para todos los escenarios

**Funcionales y Operativas**

| | |
|---|---|
| **RG-FO-01** | Servidor Secundario |
| **RG-FO-02** | Comunicaciones |
| **RG-FO-03** | Backup<br><br>Política de backups periódicos<br><br>Seguridad física.<br><br>Almacenamiento Offsite |
| **RG-FO-04** | Time Server |
| **RG-FO-05** | Gestión de Usuarios |
| **RG-FO-06** | Auditoría y Control Interno del proceso |
| **RG-FO-08** | Manejo de Fallas de Servicio |
| **RG-FO-09** | Plan de Recuperación de Desastres |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Recomendaciones para servicios sobre una red corporativa

### Funcionales y Operativas

| | |
|---|---|
| **RRC-FO-01** | Gestión de Usuarios<br>Implementar un sistema de gestión de credenciales de usuarios disponible para la mesa de ayuda y administradores del sistema |
| **RRC-FO-02** | Protocolos de Autenticación<br>Generar una política definiendo el protocolo a usar por las aplicaciones de la empresa y la forma de implementarlo.<br><br>Implementar programas de capacitación en administración y desarrollo en los protocolos definidos en la estandarización |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

Recomendaciones para servicios sobre una red corporativa

**Seguridad**

| | |
|---|---|
| **RRC-RS-01** | **Evaluar políticas a nivel de negocio**<br>Realizar un relevamiento previo a la implementación del esquema de autenticación que considere los siguientes aspectos:<br>• Normas que aplican a la actividad de la organización.<br>• Estándares de seguridad de la información.<br>• Análisis de criticidad de los servicios.<br>• Tecnologías a usar y posibles vulnerabilidades en su implementación. |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

Recomendaciones para servicios sobre una red corporativa

**Seguridad**

| | |
|---|---|
| **RRC-RS-01** | **Evaluar políticas a nivel de negocio**<br>Realizar un relevamiento previo a la implementación del esquema de autenticación que considere los siguientes aspectos:<br>• Normas que aplican a la actividad de la organización.<br>• Estándares de seguridad de la información.<br>• Análisis de criticidad de los servicios.<br>• Tecnologías a usar y posibles vulnerabilidades en su implementación. |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Recomendaciones para servicios públicos en Internet

**Funcionales y Operativas**

| | |
|---|---|
| **RPI-FO-01** | **Conexiones de Respaldo**<br>La organización deberá contar con al menos dos proveedores diferentes para asegurar alta disponibilidad de ser requerida |
| **RPI-FO-02** | **Autogestión de Usuarios**<br>Implementar un sistema de autogestión de credenciales, protegido por una conexión SSL y solicitar que el usuario verifique su dirección de correo para realizar cualquier acción.<br><br>Las acciones de los usuarios deben de quedar registradas en logs de auditoria. |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Recomendaciones para servicios públicos en Internet

**Seguridad**

| | |
|---|---|
| **RPI-RS-01** | **Autenticación Básica**<br>Las credenciales de usuario deben ser intercambiadas entre cliente y servidor de manera segura haciendo uso de un algoritmo de encriptación fuerte. |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Recomendaciones para servicios corporativos en la Nube

**Funcionales y Operativas**

| | |
|---|---|
| **RCN-FO-01** | Definir Roles |
| **RCN-FO-02** | Políticas de Negocio |
| **RCN-FO-03** | Identificar Objetivo Critico |
| **RCN-FO-04** | Proceso de cierre de contrato |
| **RCN-FO-05** | Fallas de Servicio |
| **RCN-FO-06** | Plan de recuperación de desastres |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Recomendaciones para servicios corporativos en la Nube

**Funcionales y Operativas**

| | |
|---|---|
| **RCN-FO-01** | Definir Roles |
| **RCN-FO-02** | Políticas de Negocio |
| **RCN-FO-03** | Identificar Objetivo Critico |
| **RCN-FO-04** | Proceso de cierre de contrato |
| **RCN-FO-05** | Fallas de Servicio |
| **RCN-FO-06** | Plan de recuperación de desastres |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# RESULTADO Y DISCUSIONES

## Recomendaciones para servicios corporativos en la Nube

**Seguridad**

| | |
|---|---|
| **RCN-RS-01** | **Requerimientos de Seguridad y Privacidad**<br>Definir la información que no se compartirá con el proveedor (información personal del usuario) y establecer un acuerdo de confidencialidad con el proveedor. |
| **RCN-RS-02** | **Convenio de Confidencialidad**<br>El contrato de prestación de servicios deberá incluir un convenio de confidencialidad entre las partes y establecer el proceso de borrado seguro de los datos por parte del proveedor cuando se termine el contrato. |

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA



# Conclusiones

Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

- Ingresa a:
- www.cidecuador.com
- Al finalizar este evento podrás encontrar esta presentación en su respectiva página web.

Congreso Internacional de
DESARROLLO DE SOFTWARE