Prácticas de Seguridad Aplicadas a Escenarios de Autenticación

Jadán, Andrés

2013

Ceed. 1502/0967

Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Prácticas de Seguridad Aplicadas a Escenarios de Autenticación

Autor: Ing. Andrés Jadán.
Director: Ing. Hugo Pagola

COHORTE 2013

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su Creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

Ing. Andrés Santiago Jadán Montero

DNI: 95144281

Pasaporte: 0103563805

DEDICATORIA

Dedico este trabajo a mi amada esposa, por su apoyo y ánimo que me brinda día con día para alcanzar nuevas metas, tanto profesionales como personales.

A mi padre por haberme brindado la oportunidad de tener una educación y siempre creer en mí, todo lo que he logrado se lo debo a él.

Resumen

La autenticación en los sistemas informáticos se encarga de verificar la identidad de un usuario que está solicitando acceso a un servicio para con esto proceder a autorizar o no el uso de los servicios.

Existen varios esquemas de autenticación en la actualidad los cuales son implementados según sea el nivel de seguridad requerido y el tipo de sistema informático.

Sin importar el esquema que se vaya a utilizar es necesario asegurar que este tenga un funcionamiento óptimo ajustándose a los requisitos operativos, funcionales y de seguridad que sean requeridos por el sistema informático o la organización involucrada.

El objetivo de este trabajo es analizar escenarios en los que se aplica un esquema de autenticación y presentar un catálogo de buenas prácticas que puedan ser usadas para llevar a cabo una implementación segura de cada esquema.

Palabras Claves

Autenticación, Dominios, Buenas Prácticas, Estándares, Usuarios, Identidad, Federación de Identidad, Recomendaciones.

Contenido

1 Introducción

En la actualidad la seguridad de los sistemas informáticos es de vital importancia para las organizaciones. En estos sistemas se maneja información que representa un activo importante para la organización y que por lo tanto debe ser custodiada y asegurada.

Para que un sistema brinde seguridad en el manejo de esta información es necesario que cumpla con los siguientes aspectos:

- Confidencialidad
- Integridad
- Disponibilidad

Un factor de gran importancia para el cumplimiento de estas tres dimensiones es la autenticación.

La autenticación se puede definir como "*Verificación de la identidad de una persona, usuario o proceso, para así acceder a determinados recursos o poder realizar determinadas tareas*"[1]

Para asegurar la ***confidencialidad*** de la información la autenticación trabaja conjuntamente con un proceso de autorización, y de esta forma solamente se permitirá el acceso a la misma a usuarios autorizados.

También es clave en el aseguramiento de la **integridad** de la información ya que mediante los procesos de autenticación y autorización se asegura que solamente los usuarios identificados y autorizados accedan a modificar la información existente.

Existen varios mecanismos, protocolos y tecnologías que permiten implementar en forma segura la autenticación dentro de un sistema.

La finalidad de este trabajo es analizar escenarios de autenticación y sugerir implementaciones adecuadas para cada caso, brindando un conjunto de recomendaciones para realizar una implementación segura.

El primer escenario analizado se refiere a una organización en la que se requiere autenticar y autorizar a sus empleados para el uso de los servicios prestados en su red corporativa.
En el segundo escenario planteado, se analizan servicios prestados a terceros mediante un portal WEB a través de internet con usuarios nominales.
Por ultimo en el tercer escenario se analiza el caso en el que una organización cuenta con servicios corporativos prestados por un proveedor externo en la nube.

Se realizaron tres pruebas de concepto utilizando tecnologías actuales lo cual fue un auxiliar para el relevamiento del catálogo de recomendaciones que se presenta en el capítulo 5.

2 Descripción de los Escenarios

2.1 Servicios sobre una red corporativa

Dentro de una empresa u organización de cierto tamaño es necesario implementar un esquema centralizado de autenticación para sus empleados, para ello es de vital importancia implementar un proveedor de autenticación.

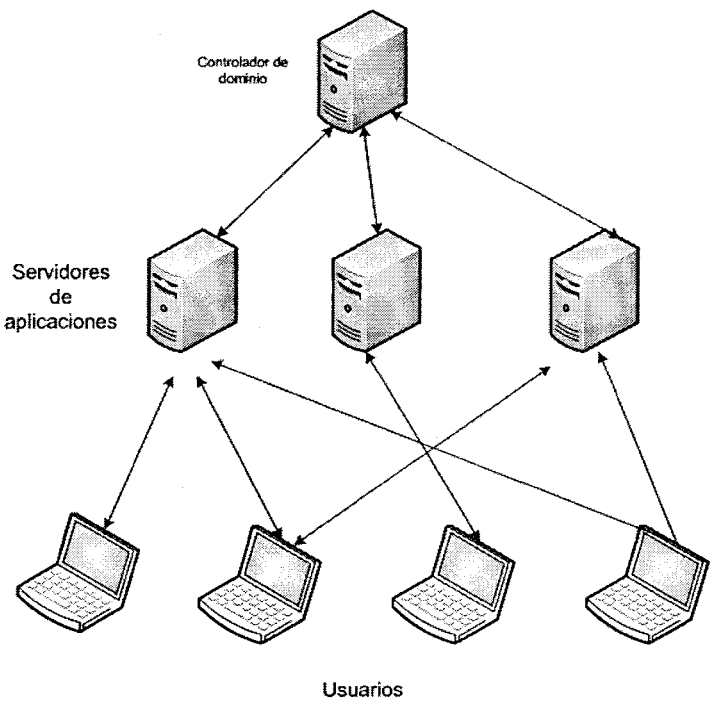

Figura 1 Dominio corporativo

El servidor de autenticación se encargara de autenticar los usuarios dentro de su dominio emitiendo credenciales para que puedan acceder a los servicios disponibles en la organización.

Este esquema de autenticación puede ser usado para disminuir el número de credenciales manejadas por el usuario, por ejemplo, en el caso de active

directory el usuario puede usar las mismas credenciales para ingresar a su terminal, acceder a su correo y a otras aplicaciones compatibles con los sistemas Microsoft, esto es conocido como single sign on.

2.2 Servicios públicos en Internet

En la actualidad la gran mayoría de los servicios son prestados a través de la web.

Estos servicios pueden ser de uso anónimo como por ejemplo noticias o servicios en los que se necesita autenticar a un cliente ejemplo servicios bancarios.

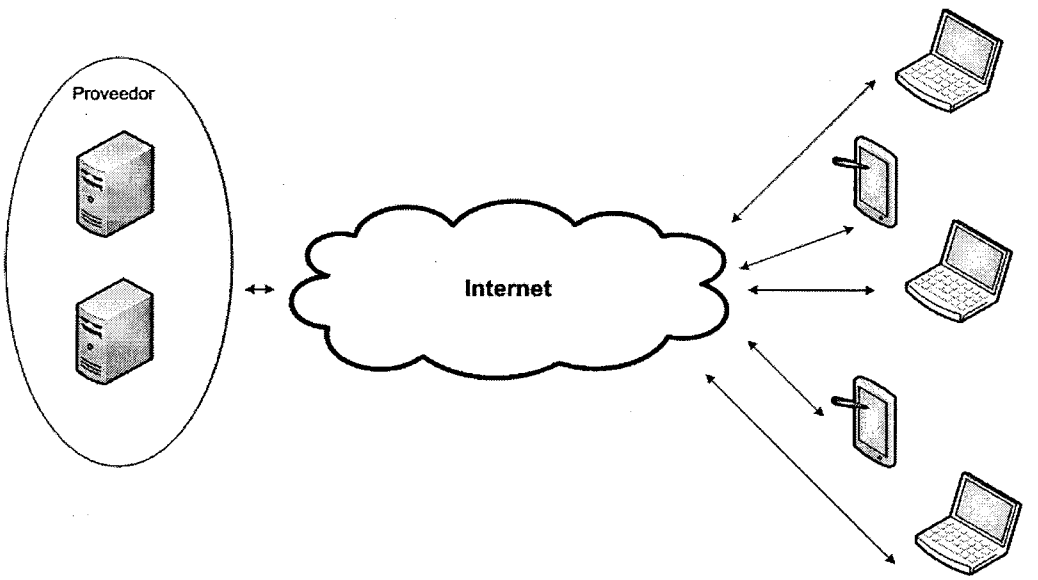

Figura 2 Servicios Web

Para realizar la autenticación de los usuarios a través de la web son utilizados varios métodos diferentes dependiendo de la implementación del servicio web.

Estos métodos van desde una implementación básica manejando toda la información en texto plano a una autenticación realizada mediante certificados digitales con lo que se establece un canal encriptado asegurando la información.

Este tal vez es el escenario en el que la autenticación sea un aspecto que ocupa mayor importancia que en los demás ya que aquí los servicios de una organización se encuentran expuestos a una red insegura.

2.3 Servicios corporativos en la Nube

Este escenario describe a una empresa que tiene un contrato de servicios con una tercera parte a través de internet, un ejemplo de este escenario es google y su servicio de mail corporativo.

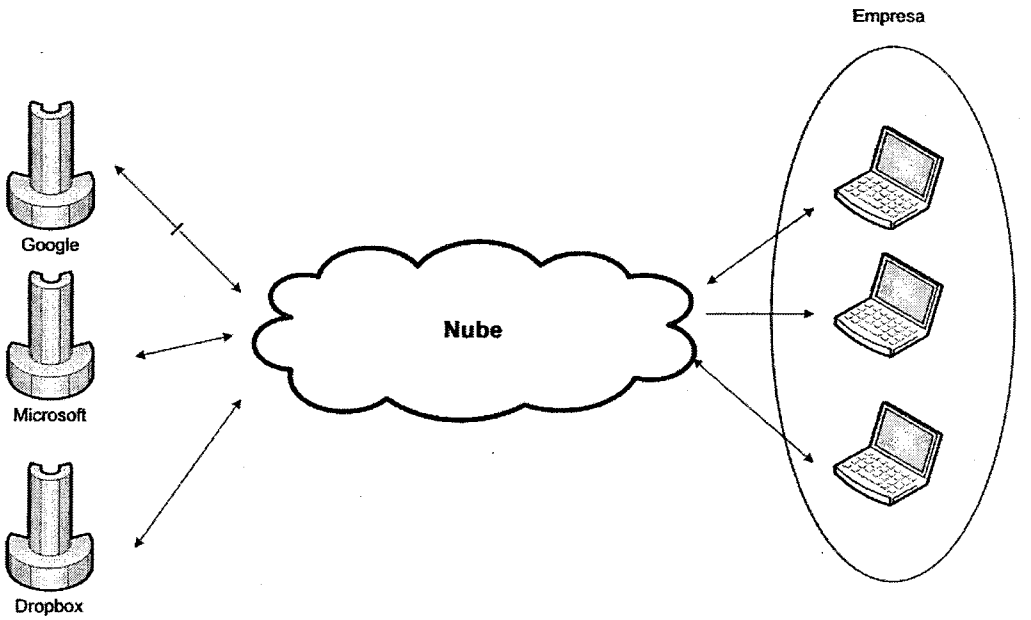

Figura 3 Servicios en la nube

A diferencia de los servicios consumidos normalmente a través de internet este escenario plantea un contrato entre las partes que define las condiciones de servicio y seguridad.

El proveedor deberá asegurar que los servicios contratados solamente sean accedidos por la empresa que los contrato y también asegurara un nivel de servicio mínimo.

El nivel de servicio será determinado por las necesidades específicas de la empresa y estará estipulado en el contrato.

En este escenario se pierde todo el control técnico sobre la autenticación de los usuarios ya que esto será realizado por el proveedor del servicio.
Todos los requisitos funcionales, operativos y de seguridad están a cargo del proveedor del servicio pero el consumidor debe estar involucrado en la definición de los mismos.

Para la empresa lo más importante será la continuidad en su funcionamiento por lo que es de gran importancia que el proveedor brinde un nivel de disponibilidad de acuerdo a las necesidades de la empresa.

También hay que considerar el escenario en que una empresa cuente con servicios de varios proveedores y necesite interactuar entre ellos, en este caso será necesario contar con un esquema de single sign on o federación de identidad.

Como se ha explicado en este escenario la parte técnica de la operación de los servicios queda fuera de las manos de las organizaciones que se convierten en consumidores de servicios.
La herramienta disponible para controlar las implementaciones está en los acuerdos de nivel de servicio que deben de ser incluidos en el contrato de prestación del servicio.

Para guiar a las organizaciones en el proceso de establecer los acuerdos de nivel de servicio el consejo del consumidor de servicios en la nube ofrece documentos de referencia para la implementación.[2]

Uno de los documentos disponibles es la guía práctica para acuerdos de servicios consumidos a través de la nube en la que se establecen los principales puntos a observar:[3]

- Entender los roles y responsabilidades.

- Evaluar políticas a nivel de negocio.
- Entender las diferencias entre el modo servicio e implementación.
- Identificar objetivos críticos de rendimiento.
- Evaluar requerimientos de seguridad y privacidad.
- Identificar requerimientos de gestión del servicio.
- Prepararse para manejar fallas del servicio.
- Entender el plan de recuperación de desastres.
- Desarrollar un efectivo proceso de gobierno.
- Entender el proceso de salida

3 Análisis de Requisitos

Para obtener el catálogo de recomendaciones que propone este trabajo se realizó un análisis de los escenarios de autenticación descritos identificando los requisitos necesarios para obtener una implementación segura y confiable

A continuación se describen estos requisitos divididos por los que aplican a todos los escenarios y requisitos particulares de cada uno.

3.1 Requisitos comunes a todos los escenarios

Existen requisitos que son comunes a todos los escenarios planteados, que deben cumplir las implementaciones de autenticación para garantizar su funcionalidad y operatividad.

3.1.1 Requisitos Funcionales y Operativos

3.1.1.1 Alta Disponibilidad

Se debe garantizar la disponibilidad del servicio de autenticación Dependiendo el nivel de disponibilidad que se requiera hay diversas opciones tecnológicas disponibles.

En implementaciones de servicios que tienen que estar disponibles a los clientes todo el tiempo (7x24). El servidor de autenticación debe tener una disponibilidad en lo posible del 100%.
Para ello se propone utilizar un esquema denominado de Alta Disponibilidad del servicio.

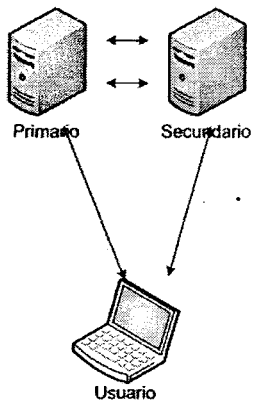

Figura 4 Implementación de Servidor Primario y Secundario

Para brindar esta continuidad de servicio es recomendable usar una arquitectura de servidor primario y secundario en la que ambos servidores primario y secundario trabajen en modo activo.

Este esquema de dos servidores debe ser transparente para el usuario y procesar las autenticaciones de forma balanceada o por desborde, en este último caso si el primario se encuentra saturado o no disponible el secundario tomará la operación.

Ambos servidores deben estar replicados y sus bases de configuración y repositorio de usuarios deben ser centralizadas o estar también replicadas.

Para escenarios que no requieran un nivel de disponibilidad tan alto como el descrito se recomienda un esquema de servidor secundario pasivo.
El servidor pasivo será una copia del servidor primario, se encontrara apagado o fuera de línea y se activará cuando el primario no pueda brindar el servicio.

Con esta implementación se obtiene un menor nivel de disponibilidad ya que es necesario que el personal de TI se encargue de activar el equipo secundario.

3.1.1.2 Conexiones de Respaldo

Para garantizar la disponibilidad del servicio de autenticación dentro de la implementación se debe considerar la inclusión de conexiones de red redundantes para los servidores.

Las solicitudes deben ser dirigidas mediante un balanceo a través de las conexiones redundantes o en un esquema de fail over usando el canal secundario en caso de fallar el primario.

3.1.1.3 Backups

De manera complementaria para asegurar la disponibilidad del servidor de autenticación se debe implementar un esquema de backup con respaldos periódicos de los servidores de identidad y de aplicaciones.

Los backups serán usados como contingencia para realizar la recuperación de los servidores por lo que deben de ser realizados con la periodicidad que exija la criticidad del servicio.

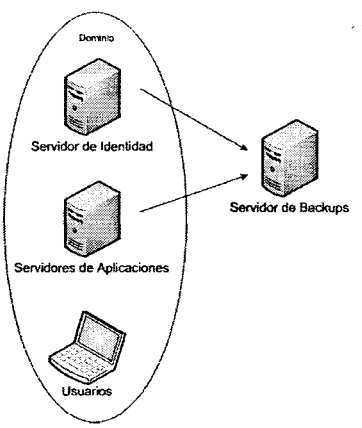

Figura 5 Implementación Servidor Backup

Para que el servidor de backups pueda funcionar correctamente debe ser configurado con los permisos necesarios para acceder a los servidores, se

debe tener cuidado en los privilegios otorgados a este servidor para evitar accesos indebidos a información de la organización.
Para que el proceso sea llevado a cabo correctamente es necesario que la organización defina una política para los mismos. En esta política se establecerá periodicidad, datos a respaldar, medio de almacenamiento y manejo de los mismos.

3.1.1.4 Time Server

Independientemente del protocolo que se haya elegido para la implementación las credenciales emitidas contaran con un atributo de caducidad.
Este atributo es incluido para evitar que un atacante que obtenga una credencial anterior pueda obtener acceso al sistema, cada vez que se reciba una credencial caducada se solicitara al usuario volver a autenticarse.

Para que no exista la posibilidad de que las credenciales sean rechazadas erróneamente debido a una diferente configuración horaria se debe implementar un time server dentro de la organización al que todos los servidores se conectaran para establecer su configuración.

3.1.1.5 Gestión de Usuarios

Generar una política de gestión de usuarios para el esquema de autenticación de una organización permite definir procesos y practicas orientadas a mantener la integridad de la implementación y de sus datos de usuario.

En la política de gestión deben ser establecidos los siguientes procesos:

- Creación de nuevos usuarios.
- Creación de roles de usuarios

- Asignación y cambio de roles a usuarios.
- Activación y desactivación de cuentas.
- Reseteo de contraseñas.

Todos los procesos deben estar documentados y aprobados por las autoridades de la organización.

La estandarización de estos procesos es necesaria para mantener un control sobre la calidad de los datos de los usuarios y los cambios que se apliquen sobre ellos con la finalidad de obtener una configuración segura y confiable.

Debe existir un proceso de concientización sobre estos procesos dirigido a todos los miembros de la organización.

3.1.1.6 Logs y Auditoria

Los procesos de gestión de usuario y sus accesos deben tener definidos controles internos que garanticen la integridad y confidencialidad de la información de usuarios.
La organización debe llevar a cabo auditorías internas y de corresponder según la importancia del servicio externas sobre el servicio de autenticación.

La aplicación de una auditoria sobre una implementación se realiza para validar sus prácticas y procesos, comparándolos con estándares y normas que apliquen a la organización.
La finalidad de este proceso es la de encontrar posibles fallas o inconsistencias por lo que el resultado de la auditoria permite a la organización validar la integridad de sus sistemas.

La auditoría de un esquema de autenticación brinda a la organización la capacidad de identificar posibles fallas en el proceso o prácticas indebidas que generen un riesgo para la seguridad de los sistemas.[4]

Una de las herramientas que son usadas durante el proceso de auditoria son los logs en los que se registra todas las acciones ejecutadas dentro de un sistema.
Es necesario que la implementación del esquema de autenticación incluya el registro de logs de las acciones administrativas y de los procesos de gestión de credenciales de usuarios especialmente en el caso de sistemas de autogestión.
Se debe registrar todos los casos de autenticación exitosa y fallida, además de registrar todos los cambios de configuración que se realicen.

Los registros de los logs deben tener una marca de tiempo para poder establecer correctamente la secuencia de eventos.

3.1.1.7 Manejo de fallas de servicio

La organización debe contar con un proceso de manejo de contingencias en caso de presentarse una falla en el servicio de autenticación.

Este proceso debe incluir las siguientes definiciones

- Mecanismo de reporte de falla de servicio.
- Responsables de reportar fallas de servicio.
- Proceso de activación de servidores secundarios en el caso que se mantenga una configuración activo/pasivo.
- Proceso para volver a configuración original.
- Responsables de procesos.

3.1.1.8 Plan de recuperación de desastres

El plan de recuperación de desastres que definido por la organización debe considerar el proceso de recuperación de los servicios de autenticación de manera prioritaria para mantener el acceso seguro a los sistemas.

Los requisitos mínimos que deberá observar el plan para restablecer el servicio de autenticación son los siguientes.

- Servidores involucrados.
- Ubicación de respaldos.
- Ubicación física de servidores de contingencia.
- Servicios prioritarios.
- Responsables del proceso

3.1.2 Requisitos de Seguridad

3.1.2.1 Evaluar políticas a nivel de negocio

La organización debe realizar un análisis de las políticas que gobiernan sus procesos, estas políticas pueden ser internas o externas como por ejemplo el cumplimiento de la norma SOX.

La definición del esquema de autenticación debe realizarse en base a los resultados del análisis realizado con la finalidad de obtener una configuración segura y que cumpla con los objetivos del negocio.

3.1.2.2 Manejo de Contraseñas

Debe establecerse una política dentro de la organización que abarque las recomendaciones de los estándares de seguridad y necesidades de la empresa.

El uso inadecuado de las contraseñas puede aumentar el riesgo de que una vulnerabilidad sea explotada y que los recursos de la organización sean accedidos de manera indebida.

El uso de contraseñas está sujeto a múltiples consideraciones como su formación, caracteres permitidos y el algoritmo de encriptación que se usara para almacenarlas.

La fortaleza de una contraseña se basa en su longitud y complejidad como lo indica la NIST en su publicación especial "*800-118 Guide to Enterprise Password Management*", la contraseña será más resistente a ataques según se aumente su longitud y se añadan set de caracteres permitidos para su formación.[5]

Tomando en cuenta esto se puede fortalecer la contraseña extendiendo su longitud o agregando set de caracteres permitidos para su formación.

También hay que tomar en cuenta regulaciones de organismos externos como es el caso del banco central de la república Argentina que en una de sus comunicaciones establece que la longitud mínima de las contraseñas será de 8 caracteres y requiere el almacenamiento de un historial de las ultimas 12 contraseñas para que no puedan volver a ser usadas.[6]

También se debe tomar en cuenta la complejidad que representara para los usuarios una contraseña demasiado larga o con demasiados requisitos de caracteres especiales.

Las contraseñas deben de ser almacenadas de manera segura, no se recomienda almacenarlas en texto plano si no en forma de hash, para esto se debe hacer uso de un algoritmo fuerte como SHA-3

3.1.2.3 Seguridad Física

Es necesario proteger la integridad física de todos los servidores involucrados, esto incluye asegurar su correcta instalación para evitar fallas y protegerlos de posibles desastres o de accesos indebidos.

Se deben seguir todas las recomendaciones especificadas en la ISO 27002 que especifica controles para proteger las instalaciones de la organización, cada control dependerá de los riesgos identificados y el valor de los elementos que se están protegiendo.[7]

Como aspectos básicos a tomar en cuenta se identifican los siguientes:

- Protección ante fenómenos naturales.
- Controles de acceso a las instalaciones mediante un PIN o tarjeta magnética.
- Registro de acceso a las instalaciones.
- Detección de intrusos (vigilancia de audio, video, etc.).
- Equipamiento para el control de incendios.
- Control de ambiental.
- Protección ante fallas de alimentación eléctrica.
- Protección física de los canales de comunicación.
- Mantenimiento preventivo de instalaciones y equipos.

En un esquema de autenticación los equipos más importantes a proteger serán los que funcionen como servidores de autenticación y repositorios de usuarios.
Se debe tener especial cuidado sobre los equipos que contengan el repositorio de usuarios ya que teniendo acceso a estos equipos un intruso podría obtener los listados de usuarios y el hash de sus contraseñas.

3.1.2.4 Separación de Ambientes

Cuando una organización expone servicios a una red externa aumenta el riesgo de intrusiones a su red interna ya que los servicios externos pueden servir como puerta de entrada.

Estas intrusiones afectan a los escenarios que tienen servicios publicados en el internet y también a las empresas con una red corporativa ya que la misma podría estar formada por varias extranet de sus diferentes sucursales a las que se conecta mediante internet.

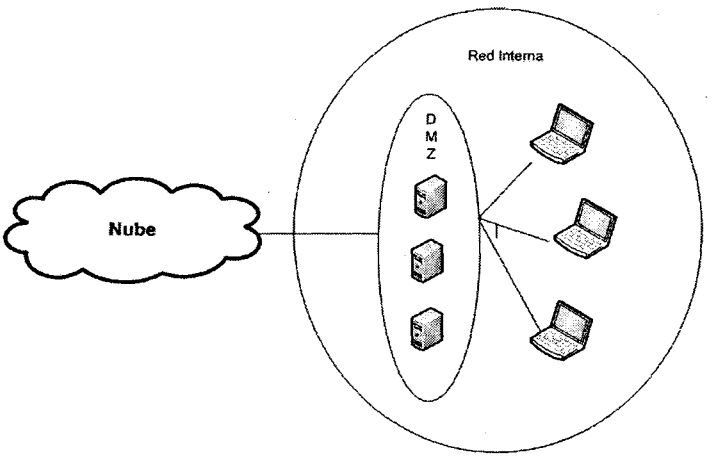

Figura 6 Separación de Ambientes

Para mitigar este riesgo es necesario que todos los servidores de identidad se encuentren ubicados en una DMZ separados de la red interna, con esto se limita el alcance que podría tener un intruso.[8]

3.1.2.5 Firewall de Aplicación

Es necesario implementar medidas de protección sobre el tráfico de red que se genera en el proceso de autenticación ya que un atacante puede introducir código malicioso.

Se recomienda implementar un firewall con capacidad de analizar el tráfico de aplicaciones específicas analizando los paquetes recibidos y enviados y comparándolos con paquetes comunes con la finalidad de encontrar irregularidades.[9]

3.1.2.6 Cuentas de Servicio

Para que se ejecuten los servicios de autenticación dentro de los servidores generalmente se necesitan cuentas de servicio, las que son habitualmente creadas durante la instalación del software.
Es conocido que algunos sistemas del mercado definen estas cuentas con contraseñas por defecto. Es muy importante modificar estas contraseñas ya que si no son modificadas a contraseñas fuertes se puede producir una vulnerabilidad que puede ser aprovechada por los atacantes.

Un ejemplo son los ataques al protocolo Kerberos llamados ataques de boleto plateado y de boleto dorado en el que se aprovecha cuentas de servicio con claves conocidas para fabricar credenciales y obtener acceso a los sistemas.[10][11]

Al momento de crear una cuenta de servicio se debe definir claramente los privilegios que se requieren para el funcionamiento de la aplicación para evitar el uso indebido de la cuenta[12] [13]

Se recomienda tomar en cuenta los siguientes aspectos para asegurar las cuentas de servicio

- De ser posible usar cuentas locales de los equipos en los que se ejecute el servicio.
- Las cuentas usadas deben de ser de tipo básico.
- En el caso de ser necesario cuentas de dominio para ejecutar los servicios evitar usar usuarios con privilegios administrativos.

- La cuenta de servicio solamente deberá tener permisos de escritura/lectura limitados a los archivos o directorios necesarios para prestar el servicio.

3.1.2.7 Single Sign On

El uso de diferentes contraseñas para ingresar a cada sistema aumenta el número de credenciales que tendrá que manejar el usuario, lo que genera el riesgo de que el usuario tenga un manejo inadecuado de las contraseñas.

Implementar un esquema de single sign on para ingresar a las aplicaciones dentro de la organización mitiga este riesgo ya que da la posibilidad de que el usuario maneje una única credencial con una contraseña fuerte.

3.1.2.8 VPN

En el caso de que la organización cuente con diferentes sucursales separadas geográficamente será necesario establecer una conexión entre ellas.
Esta conexión se podrá realizar mediante un canal dedicado implementado por la organización o a través de un proveedor de internet.

Si es que la conexión se establece directamente por internet se pone en riesgo a la organización ya que sería vulnerable a ataques como el conocido man in the middle.
Para mitigar este riesgo todas las conexiones entre sucursales o con proveedores externos deben ser realizadas mediante conexiones VPN

Para implementar la VPN de la organización se sugiere adoptar las recomendaciones de la NIST que establece los requerimientos técnicos y de seguridad a considerar antes de una implementación VPN[14]

3.1.2.9 SSL

La mayoría de los servicios en la actualidad son presentados a los usuarios mediante páginas web, para este tipo de servicios hay que considerar ataques al protocolo HTTP desde la red interna de la empresa.

Para mitigar este riesgo todas los servicios que se vayan a consumir mediante un navegador web deben de ser presentados usando el protocolo HTTPS para esto la organización deberá contar con los certificados que cumplan con las recomendaciones de seguridad.

3.1.2.10 Certificados Digitales

En el caso de una conexión sobre un canal inseguro como internet los certificados digitales son usados para establecer un canal de comunicación seguro entre el proveedor del servicio y el usuario.

Para una implementación de este tipo es necesario de la intervención de una tercera parte ajena al cliente y el proveedor de servicio, la cual estará encargada de emitir los certificados digitales para cada uno de los participantes de la conexión.

Para considerar seguro el certificado la autoridad certificante debe entregar certificados que cumplan con los establecido en el estándar x.509v3.[15]

Otro aspecto que define la confiabilidad del certificado digital es el tipo de algoritmos usados en el esquema PKI para el cifrado y para hash, actualmente se recomienda[16]:

Algoritmo Cifrado: Recomendamos el uso de Curvas Elípticas ECC-1 de 160 bits o RSA 2048 bits y 4096 para la AC.

Algoritmo de Hash: sha2 512 o eventualmente sha3 de 1024 bits

3.1.2.11 Múltiple Factor

En un esquema que usa la combinación de usuario y contraseña para el proceso de autenticación existe el riesgo de que estos datos puedan ser obtenidos por un atacante.

En sistemas en los que se requiere un nivel más alto de seguridad se debe incluir un segundo factor de autenticación para aumentar la complejidad de las credenciales.

Es recomendable usar varios factores para comprobar la identidad de los usuarios con la finalidad de asegurar el sistema y evitar ataques que suplanten la identidad de usuarios.

Los factores usados para realizar la autenticación se pueden dividir de la siguiente forma[17]:

- Información que conoce el usuario: es información que el usuario conoce como su id o su nombre de usuario, esto se puede combinar con una contraseña.
- Elementos que posee el usuario: son elementos entregados al usuario, se usan credenciales digitales o llaves usb que generan one time passwords.

- Factores Inherentes: por ejemplo la aplicación de una tecnología de reconocimiento facial de los usuarios.
- Ubicación: Se realiza mediante el rango de IPs desde el que se solicita el acceso o en el caso de un dispositivo móvil se hace uso de su GPS integrado, este factor ya es usado por google que envía una alerta si es que se tiene un intento de ingreso en una ubicación poco usual.
- Tiempo: puede aplicarse en casos que el uso de un servicio este limitado a un rango horario o para permitir el ingreso a usuarios de cierta zona horaria.

3.2 Requisitos para Servicios sobre una red Corporativa

3.2.1 Requisitos Funcionales y Operativos

3.2.1.1 Estandarización de los Protocolos de Autenticación

Una organización se encuentra constantemente evolucionando por lo que requerirá nuevas aplicaciones o servicios para satisfacer sus necesidades. Para solventar esto la organización generara proyectos de desarrollo o iniciara procesos de adquisición de tecnología a proveedores externos.

Se debe definir dentro de la organización una política acerca de los protocolos de autenticación que podrán ser usados.
Esta limitación permitirá a la organización llevar de mejor manera la administración de los servicios de autenticación ya que se manejara un número acotado de protocolos.

La definición de un número limitado de protocolos brinda la oportunidad de preparar al personal de la organización en la administración de los mismos. Al mantener un programa de capacitación se logra optimizar las operaciones ya que se cuenta con personal entrenado para gestionar los servicios.

Además esta definición permite a la organización asegurarse de que solamente sean usados protocolos confiables y comprobados evitando así la inclusión de vulnerabilidades en desarrollos futuros.

3.2.2 Requisitos de Seguridad

3.2.2.1 Evaluar políticas a nivel de negocio

La organización debe implementar los requisitos mencionados dentro de los requisitos de seguridad que aplican a todos los escenarios.

Cada uno de los requisitos debe de ser analizado e implementado basándose en los objetivos de la organización y de los estándares que apliquen a la actividad de la misma.

3.3 Requisitos para Servicios públicos en Internet

3.3.1 Requisitos Funcionales y Operativos

3.3.1.1 Conexiones de Respaldo

En este escenario los usuarios no se encuentran en la misma red que el servidor y acceden a los servicios a través de internet por lo que es necesario garantizar un nivel adecuado de disponibilidad del servicio.

Para asegurar la disponibilidad del servicio es necesario contar con una conexión de salida a internet de respaldo, lo recomendable será tener al menos dos conexiones de proveedores diferentes.

3.3.1.2 Gestión de Usuarios

Este tipo de implementaciones incluye una gran cantidad de usuarios consumidores de un servicio, por lo que resulta costoso para una organización el mantenimiento una gestión centralizada de credenciales.

Debido a esto es necesario implementar un esquema de autogestión de credenciales para el usuario que requiera mínima intervención del personal de la organización.

La implementación de la herramienta de autogestión debe ser realizada de manera que sea fácil de usar y que permita al usuario solventar todos sus requerimientos

Debe existir una política de auto gestión de credenciales definida e implementada en el sistema de autenticación que debe incluir los siguientes procesos:

- Creación de nuevos usuarios.
- Cambio de Contraseñas
- Baja de Usuarios.
- Recuperación de nombre de usuario y contraseña.

Todas las operaciones que se lleven a cabo deben de ser debidamente registradas en un log para análisis futuros.

Para que un usuario pueda realizar todas estas operaciones es necesario implementar un segundo factor el que puede ser su dirección de correo electrónico que será utilizado para confirmar su identidad.

3.3.2 Requisitos de Seguridad

3.3.2.1 Implementación de Autenticación Básica

Existen implementaciones web en las que para realizar el proceso de autenticación se envía las credenciales del usuario en texto plano, de esta manera cualquier atacante puede interceptar y obtener las credenciales.

Se debe evitar enviar las contraseñas en texto plano, para esto los desarrolladores deben usar un algoritmo de hash seguro o un protocolo de autenticación en el que sus paquetes de información viajen encriptados.

De esta manera la contraseña del usuario no podrá ser obtenida en el caso de que el tráfico de la aplicación haya sido interceptado.

3.4 Requisitos para Servicios Corporativos en la Nube

3.4.1 Requisitos Funcionales y Operativos

3.4.1.1 Entender los roles y responsabilidades

La norma ISO 17789 establece una arquitectura de referencia para el cloud computing definiendo tres roles principales:

- Consumidor de servicios en la nube.
- Proveedor de servicios en la nube.
- Cloud Partner.

En la ISO se encuentran a detalle los roles y sub roles existentes con sus respectivas responsabilidades.[18]

Para llevar un control sobre la calidad de la implementación la organización debe tener en cuenta lo siguiente:

- Establecer un responsable que informe sobre incumplimientos de requisitos establecidos en el SLA.
- Implementar un mecanismo para monitorear el cumplimento de los niveles de servicio.
- La organización puede delegar la auditoria del cumplimiento de los niveles de servicio a un auditor asociado.

3.4.1.2 Identificar objetivos críticos de rendimiento

Para definir los niveles de servicio en el contrato es necesario identificar los procesos y servicios críticos de la organización y los niveles de servicio requeridos para cada uno.

Se deben definir indicadores claves de rendimiento (KPI) para cada uno los servicios de la organización y el mecanismo para evaluarlos.

Como mecanismo para lograr los niveles de servicio deseados de parte del proveedor de servicio la organización puede otorgar incentivos de acuerdo al cumplimiento del SLA.

3.4.1.3 Identificar requerimientos de gestión del servicio

Para facilitar sus procesos administrativos la organización debe disponer de herramientas que le permitan gestionar el servicio, estas herramientas deben de ser puestas a disposición por el proveedor.

Se considera que para llevar un mejor control del servicio de autenticación la organización debe contar con las siguientes herramientas:

- Herramienta de auditoría sobre las acciones que se realizadas sobre el sistema.
- Herramientas de gestión sobre el sistema, en el caso de un escenario de autenticación es necesario contar con una herramienta de gestión de credenciales de usuarios (creación, eliminación, desactivación, asignación de perfiles, etc.).
- Para la gestión de la autenticación también es necesario una herramienta de monitoreo y reporte con estadísticas de uso del servicio.

3.4.1.4 Finalización de los servicios

Es vital que el contrato defina claramente el proceso a seguir en caso de una terminación del servicio.
El proceso finalización de los servicios deberá ser lo más ordenado posible para evitar un corte abrupto y que el proveedor se quede con los datos de la organización.

En este caso el proveedor del servicio debe entregar la base de datos de las credenciales de los clientes a la organización y retirar esta información de sus servidores.
La organización para continuar con sus actividades debe planear una implementación de un nuevo servicio de autenticación mediante otro proveedor o usando su propia infraestructura.

3.4.1.5 Manejo de fallas del servicio

Siendo el servicio de autenticación crítico para el acceso a los demás sistemas de la organización el proveedor del servicio debe asegurar que siempre estará disponible.

Se debe requerir que el proveedor tenga implementado un plan de contingencia en caso de fallas acorde al nivel de disponibilidad requerido por la organización.

3.4.1.6 Plan de recuperación de desastres

Puede existir el caso en el que la organización tenga que recurrir a su plan de recuperación de desastres, este plan debe incluir los pasos necesarios para rehabilitar el acceso a los servicios del proveedor.

Este plan de recuperación desastres debe ser definido conjuntamente con el proveedor y la organización estableciendo las responsabilidades de cada entidad en el proceso.

3.4.2 Requisitos de Seguridad

3.4.2.1 Evaluar requerimientos de seguridad y privacidad

La organización debe definir el nivel de seguridad que considere adecuado para sus actividades y definirlo desde el inicio del contrato en el SLA de acuerdo.
Deben estar definidos en el mismo los mecanismos que tendrán que ser usados por el proveedor para proteger las credenciales de los usuarios.

Se recomienda tomar en cuenta lo siguiente:

- Toda la información de los usuarios debe ser almacenada de manera segura haciendo uso de un algoritmo de encriptación fuerte.

- La organización también debe definir los datos de los usuarios que son entregados al proveedor. No se deberá incluir información personal del usuario a menos que sea necesario para el servicio.

- El acuerdo de servicio debe incluir cláusulas de confidencialidad entre las partes.

4 Prueba de Concepto de los escenarios

4.1 Descripción

Para complementar este trabajo se realizó una prueba de concepto sobre escenarios de autenticación aplicando diferentes tecnologías.

La primera prueba realizada trata sobre una implementación de autenticación con inclusión de un segundo factor de autenticación para el sistema de escritorios remotos virtuales implementados con un servidor CITRIX.
La implementación se realizó haciendo uso del producto de la empresa CA Technologies llamado CA Strong Authentication.

La segunda prueba de concepto consta de la implementación de un CMS de una organización para lo que fue usado DRUPAL sobre un servidor apache y una base de datos MYSQL.

Dentro de esta implementación se usa la autenticación de usuarios propia del CMS y se añade un segundo factor de autenticación para los usuarios con rol administrador. Como se puede ver en la siguiente figura la autenticación al sitio web de la organización se realiza a través de un módulo instalado dentro del CMS.

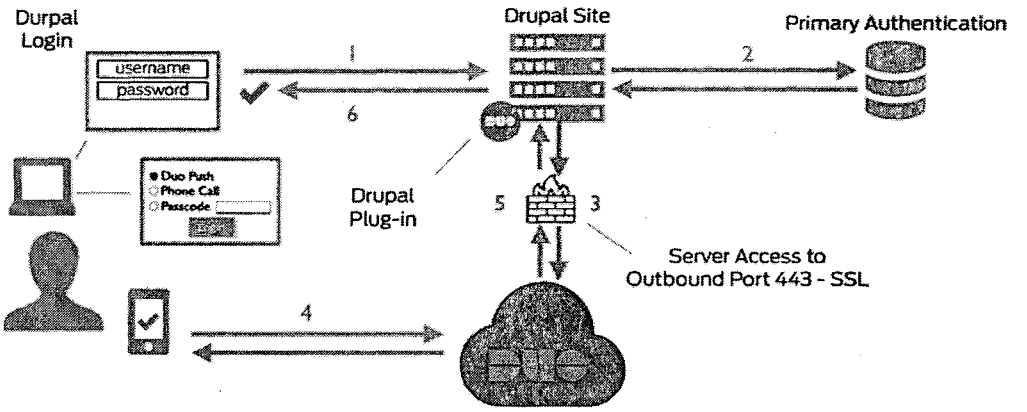

Figura 7 Esquema de implementación de DUO con CMS drupal[19]

Este módulo genera una petición de acceso que deberá será respondida por el usuario en una aplicación de su dispositivo móvil.

La tercera prueba de concepto es una implementación de federación de identidad entre dos organizaciones que manejan dominios distintos.

La federación de identidad se realizó con la herramienta ADFS 2.0 de Microsoft y para fortalecer el proceso de autenticación se agregó un segundo factor de autenticación usando el software DUO Security.

4.2 Implementación

4.2.1 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 • MS SQL Server 2012 • CA Strong Authentication 8.1 • Citrix Server • Tomcat • Apache
Descripción	Servicio de escritorios virtuales accedido por usuarios externos

La organización en la que se realizó la implementación es una multinacional que cuenta con una infraestructura de gran tamaño y gran cantidad de usuarios por lo que requiere una implementación de alta disponibilidad y con seguridad acorde a los datos que se manejan.

Para que la organización tenga un mayor control sobre el nivel de disponibilidad se decidió implementar el servicio usando infraestructura propia de la organización, en este caso se eligió la herramienta CA Strong Authentication.

"*CA Strong Authentication es un sistema de autenticación versátil que puede ayudarlo a implementar y administrar una amplia gama de métodos de autenticación, desde contraseñas hasta tokens de software de dos factores o credenciales de hardware. También puede proporcionar métodos de autenticación tales como SMS, correo electrónico o entrega de contraseñas de un solo uso (OTP) por mensajes voz.*"[20]

La organización cuenta con un servicio de escritorios virtuales (Citrix) en el que para acceder los usuarios se autentican usando sus credenciales LDAP.

El objetivo es agregar un segundo factor de autenticación para este servicio mediante el servidor CA Strong Authentication, esta herramienta de la compañía CA brinda la capacidad de implementar múltiples métodos de autenticación de una manera centralizada.

La implementación se realizó sobre una plataforma Microsoft usando Windows server 2012, además de esto para realizar la instalación es necesario contar con:

- Proxy Apache
- Servidor de aplicaciones Tomcat.
- Servidor de Base de Datos.

Para el servidor de base de datos el sistema presenta varias opciones pero la recomendada es Microsoft SQL Server que se debe encontrar en un equipo separado para asegurar la disponibilidad.

En la base de datos se almacenan las configuraciones del sistema y la información de las credenciales de los usuarios, para asegurar la disponibilidad la organización implemento un sistema de espejado de base de datos.

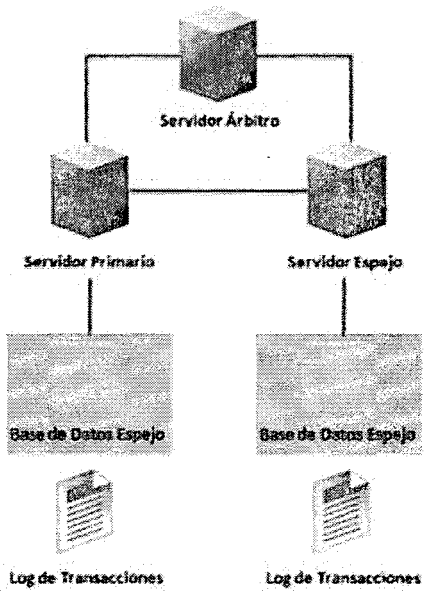

Figura 8 Espejado de Base de Datos[21]

Todos los servidores involucrados en la provisión del servicio de segundo factor de autenticación se encuentran desplegados en zonas DMZ separados de la red interna.

Debido a que el servicio de segundo factor de autenticación esta publicado hacia el internet se realizó la implementación de dos servidores apache que actúan como proxys inversos como se puede ver en la siguiente figura.

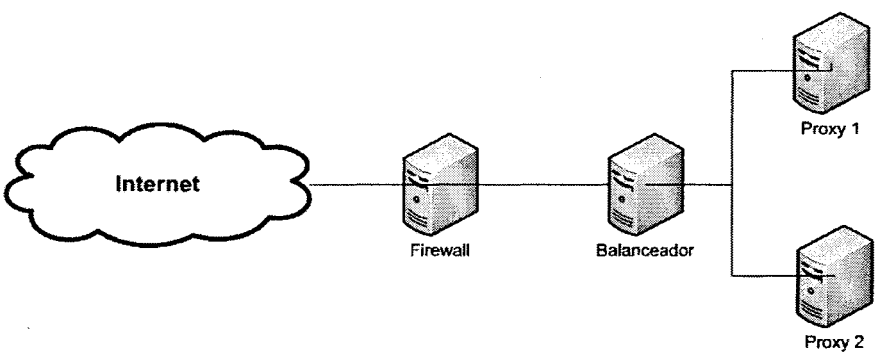

Figura 9 Esquema de Implementación de Firewall y Proxy de la Organización

Los servidores apache son usados para proteger las aplicaciones de administración del servicio de segundo factor y solamente publicar hacia el internet los servicios necesarios para la autenticación de los usuarios.

En los servidores se instalaron certificados digitales provistos por la organización para mantener conexiones seguras a través de SSL.

Para asegurar la disponibilidad de la implementación se incluyó en la infraestructura servidores primarios y secundarios para todos los elementos de la siguiente manera.

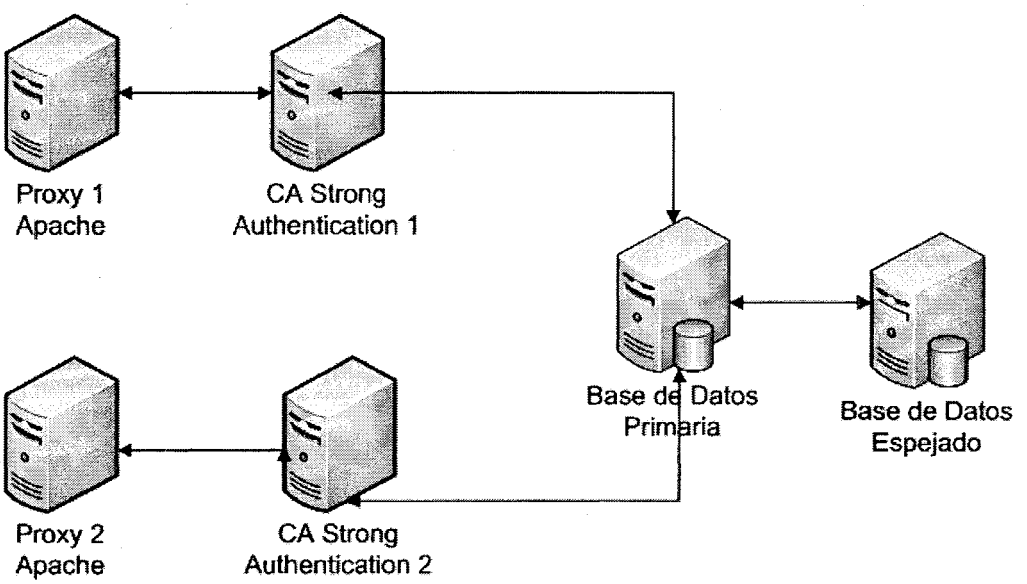

Figura 10 Implementación Alta Disponibilidad

Tanto las configuraciones primaria y secundaria se encuentran activas y cuentan con configuraciones idénticas, la organización habilito el servicio de dos balanceadores uno para el servicio SSL de los proxy Apache y el otro para el servicio RADIUS que provee CA Strong Authentication para realizar la autenticación del segundo factor.

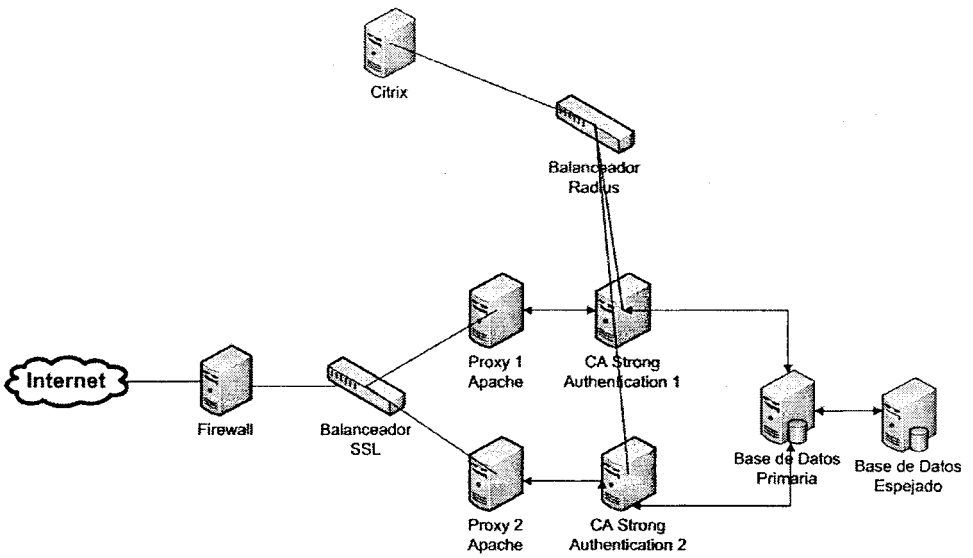

Figura 11 Esquema de Servicio de Autenticación

Dentro del servidor de autenticación Arcot Webfort se creó un nuevo esquema para la organización en la que se establece los siguientes parámetros:

- Servicio LDAP con el que se realizara la autenticación de los usuarios de dominio.
- Tipo de credenciales que le serán otorgadas al usuario, en este caso se usó una credencial OTP (One time Password).
- Grupo de usuarios a los que se les permite crear nuevas credenciales.
- Parámetros propios de la credencial como: longitud, validez, etc.

Una vez configurado el servidor para que los usuarios puedan crear sus credenciales en el servidor deben de seguir el siguiente proceso

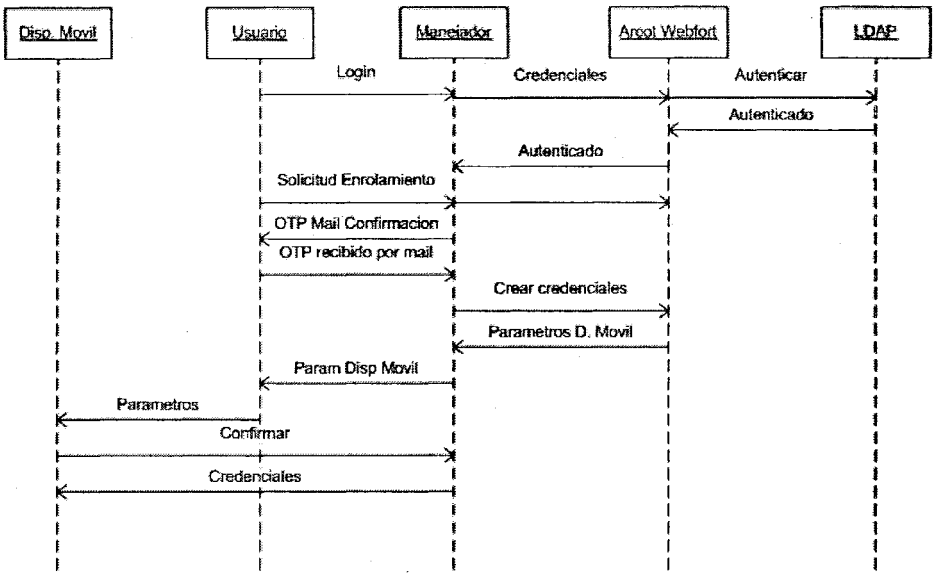

Figura 12 Proceso registro de OTP en dispositivo móvil

Una vez terminado el proceso el usuario puede generar un OTP de 6 dígitos desde una aplicación en su dispositivo móvil que junto con su contraseña de dominio le darán acceso a un escritorio remoto virtual de CITRIX.

Para que la plataforma CITRIX pueda realizar la autenticación del segundo factor es necesario agregar a su configuración la dirección del balanceador de servicio RADIUS que se ha implementado en la infraestructura.

El balanceador dirige las solicitudes de autenticación hacia los dos servidores de Strong Authentication disponibles los cuales se encargan de autenticar el OTP del usuario.

4.2.2 Servicio Publico en internet: Portal CMS Drupal

Prueba de concepto	Autenticación de usuarios de un sitio web implementado con el CMS DRUPAL
Escenario Aplicado	Servicios públicos en internet
Software Involucrado	• Windows Server 2012 • MYSQL • DRUPAL • DUOS • APACHE/PHP
Descripción	Portal web accedido por usuarios externos

Para implementar este escenario se fue usado un servidor virtual con las siguientes características:

- Sistema Operativo: Windows Server 2008 R2
- Servidor web Apache con PHP habilitado
- Base de Datos MySQL

Para la implementación se usaron las últimas versiones del software del servidor de aplicaciones y de base de datos, para el CMS se utilizara la última versión estable de DRUPAL.

En el servidor se realizó una instalación básica del paquete del CMS DRUPAL usando la distribución básica y no una distribución personalizada con módulos adicionales instalados.

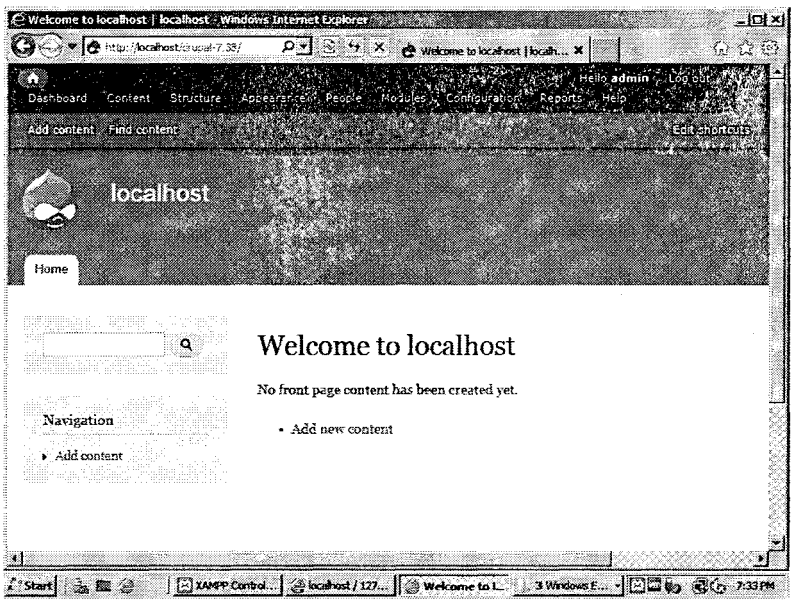

Figura 13 Homepage sitio DRUPAL

Para agregar un nuevo factor de autenticación es necesario instalar un nuevo módulo al sitio de DRUPAL lo que se realizó dentro del apartado Modules que se encuentra en la sección de administración del portal.

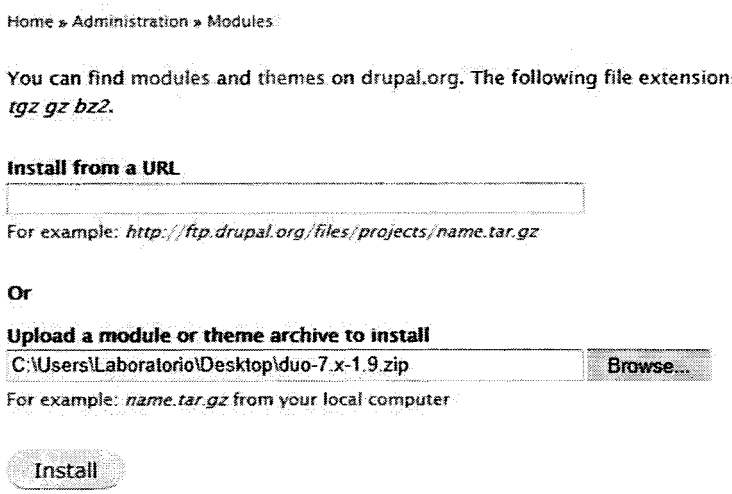

Figura 14 Instalación extensión DUO

Antes de configurar el módulo de autenticación doble factor se debe acceder a la interfaz de administración web del proveedor del servicio y registrar la aplicación la que se aplica el segundo factor, el proveedor entrega las claves compartidas necesarias para la comunicación

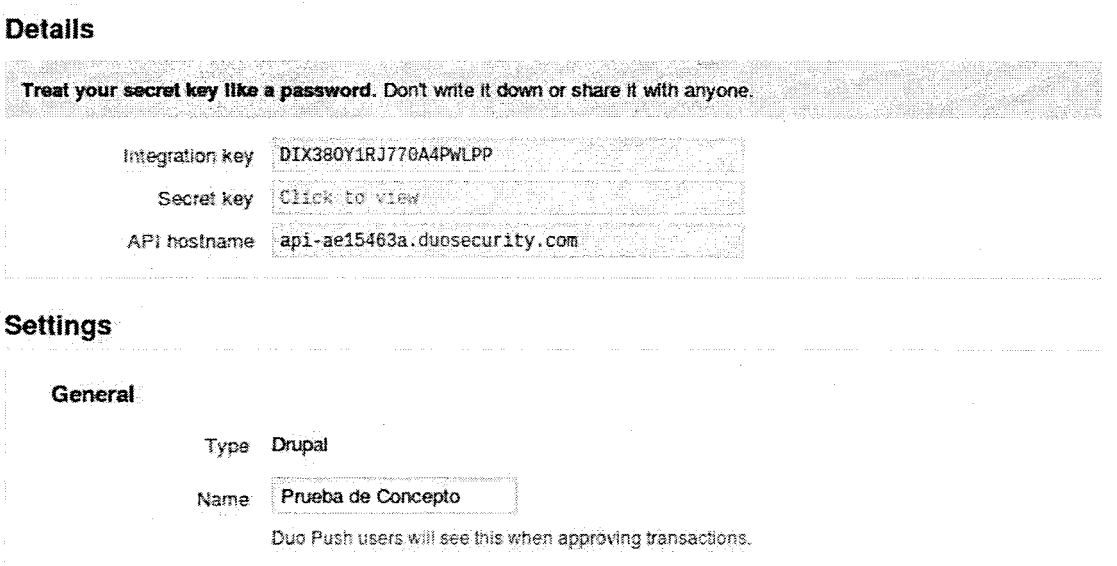

Figura 15 Claves de integración entregadas por el proveedor

Estas claves deben ser incluidas en la configuración del módulo instalado dentro del CMS

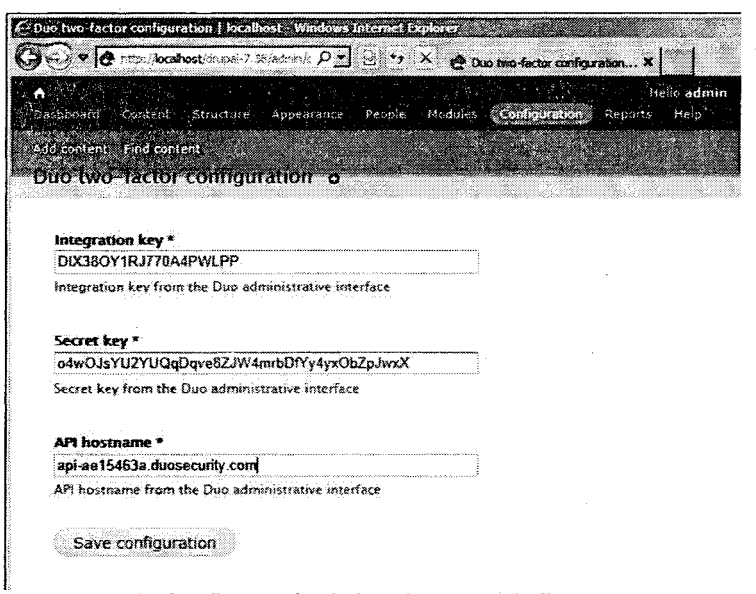

Figura 16 Configuración de las claves en el cliente

Una vez finalizada la configuración del módulo es necesario cerrar sesión y volver a ingresar las credenciales del administrador para realizar el proceso de enrolamiento.

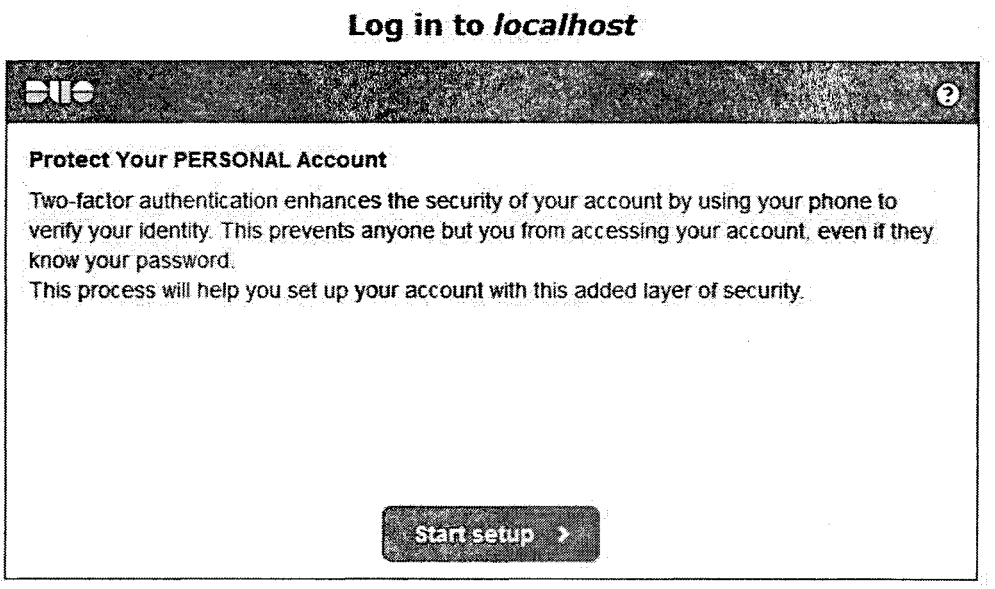

Figura 17 Login después de la Configuración

Para el enrolamiento se eligio la opción de realizarlo a través de un teléfono móvil en este caso un Iphone 4

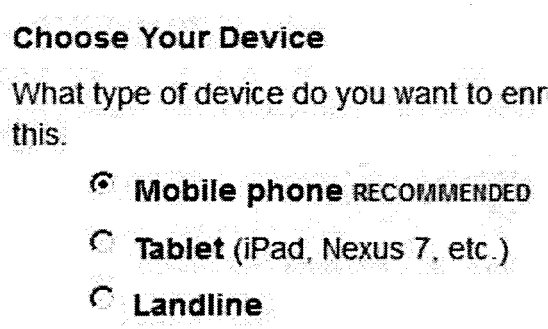

Figura 18 Enrolamiento de Smartphone

El sistema entrega un código de barras que debe ser escaneado con la aplicación instalada en el Smartphone.

Una vez terminado este proceso la aplicación informara al usuario que ha sido enrolado en el sistema.

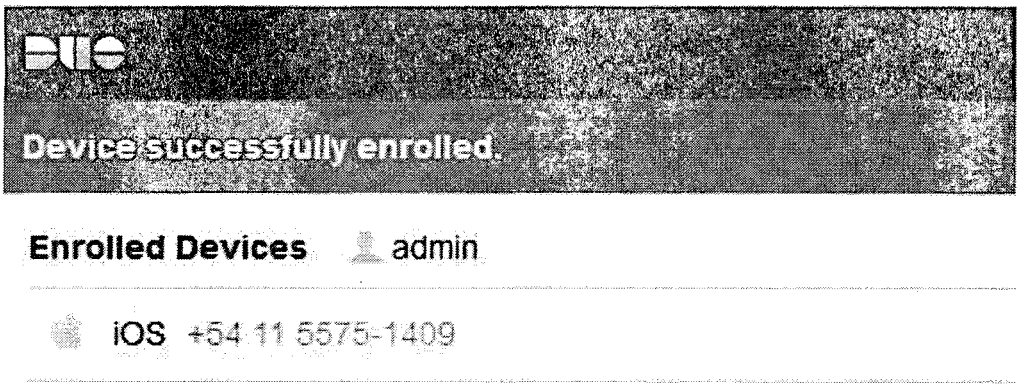

Figura 19 Información del nuevo dispositivo enrolado

A partir de este momento el usuario para ingresar a la consola de administración del CMS tiene que ingresar su usuario y contraseña y autorizar el acceso desde la aplicación móvil instalada en su Smartphone en la que recibirá la siguiente notificación

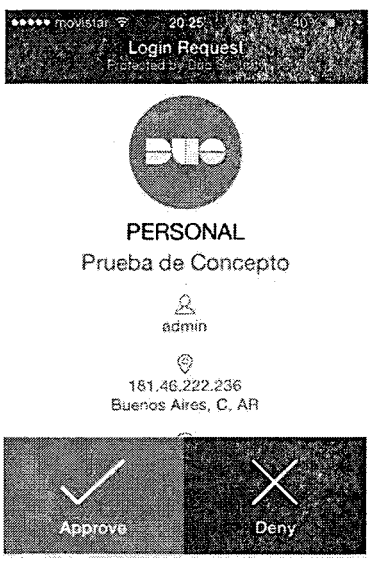

Figura 20 Interfaz en el dispositivo móvil

4.2.3 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 • Active Directory • ADFS 2.0 • DUOS
Descripción	Federación de identidad entre dos organización implementando un segundo factor de autenticación

Nota: Este escenario es una versión extendida del discutido en el trabajo final de especialización[22].

La implementación de esta prueba de concepto de federación de identidad se define de la siguiente manera: Dos empresas llamadas EMPRESA1 y EMPRESA2 han comenzado un proyecto de colaboración. Para llevar a cabo el proyecto la EMPRESA1 pone a disposición su sitio de intranet como repositorio de documentos.

Las dos empresas cuentan con dominios implementados en Active Directory en el que tienen registrados sus usuarios, decidiéndose que los usuarios ingresen al sitio de intranet de la EMPRESA1 con las credenciales que manejan en sus respectivos lugares de trabajo.

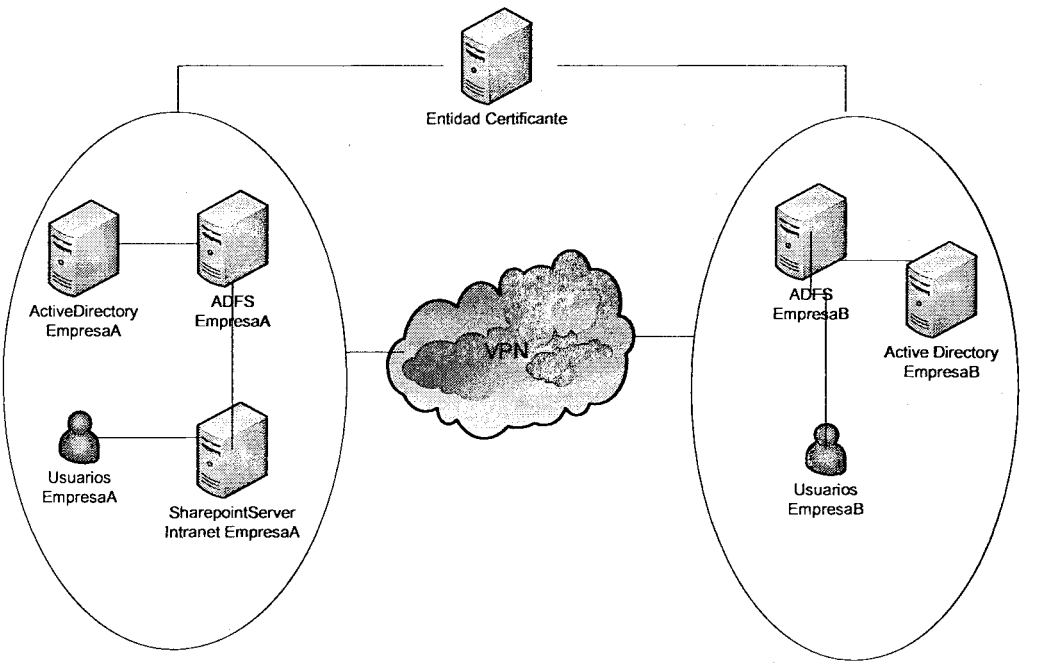

Figura 21 Esquema Prueba de Concepto ADFS 2.0

El recurso compartido entre las organizaciones es provisto por un servidor Microsoft Office Sharepoint Server 2007 que fue configurado para aceptar las credenciales generadas por los servidores que actúan como proveedores de autenticación.

La prueba de concepto se llevó a cabo utilizando máquinas virtuales sobre la plataforma vmware versión 10.

Previo a realizar las configuraciones para el funcionamiento de la federación de identidad los servidores virtuales fueron preparados de la siguiente manera

- Servidores de Dominio
  - Dominio Empresa1
    - Nombre: ADEMPRESA1
    - Dominio: empresa1.com.ar
    - Sistema Operativo: Windows Server 2008 R2

        - Servicios Instalados
            - Active Directory Domain Services
            - DNS
            - IIS
        - IP: 192.168.0.100
    - Dominio Empresa2
        - Nombre: ADEMPRESA2
        - Dominio: empresa2.com.ar
        - Sistema Operativo: Windows Server 2008 R2
        - Servicios Instalados
            - Active Directory Domain Services
            - DNS
            - IIS
        - IP: 192.168.0.200
- Servidor Web
    - Nombre: INTRANET
    - Dominio: adempresa1.com.ar
    - Sistema Operativo: Windows Server 2003 Enterprise Service Pack 2
    - IIS (habilitado ASP.NET 2.0)
    - Microsoft Office SharePoint 2007 (Se usó esta versión ya que consume menos recursos)
- Certificados Digitales
    - Para la emisión de los certificados se utilizó los servicios de certificación de Windows server generando certificados para cada servidor con una llave RSA 1024.
    - Cada equipo tendrá instalado su certificado digital y el de los demás equipos en los repositorios correspondientes.
    - Instalar el certificado de la Entidad Certificante en el repositorio TRUSTED CERTIFICATION AUTHORITIES.
- DNS

- Se debe agregar una zona de búsqueda para resolver los nombres de los equipos del dominio externo.
- Zona de búsqueda reversa, necesario para la correcta comunicación durante el proceso de solicitud/emisión de tokens.

Como servidores de autenticación se usó Active Directory Federation Services en su versión 2.0, para la prueba de concepto se instaló este servicio en el servidor de dominio de cada empresa, en una implementación real debe ser instalado en servidores separados.

En el servidor Web Sharepoint 2007 que actúa como proveedor de recursos se ha creado un sitio para compartir documentos, se accederá al sitio mediante protocolo SSL con la siguiente dirección:

https://intranet.empresa1.com.ar.

En el servidor de autenticación es necesario crear una relación de confianza con el servidor de recursos, esto se realizara en el servidor de identidad en la zona llamada Relying Party Trust.

Para completar la configuración de esta relación de confianza se establece la manera en la que se comunicaran los atributos al servidor de recursos.

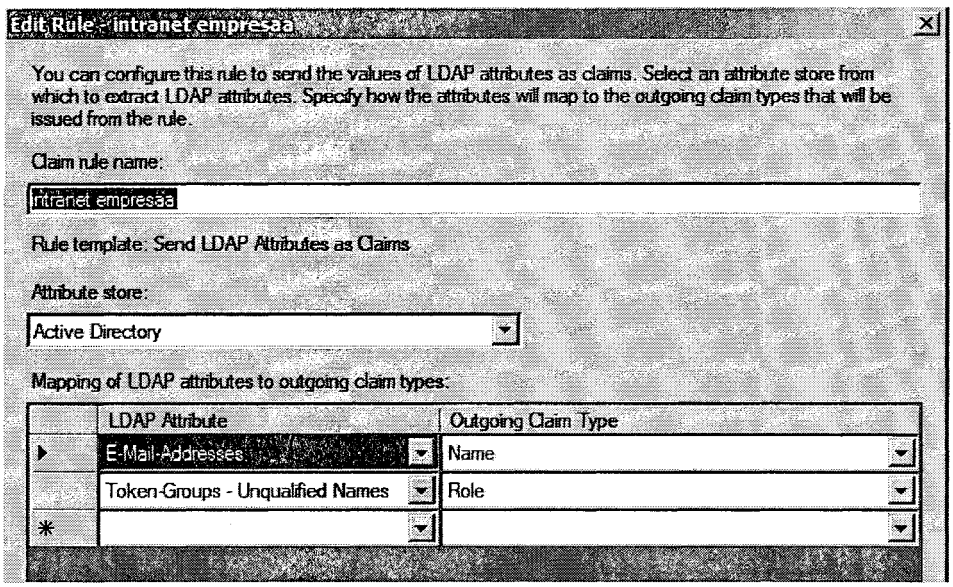

Figura 22 Configuración reglas ADFS EMPRESAA

En la imagen anterior se puede observar la configuración de los atributos que se envían al proveedor de recursos, en este caso se han especificado dos atributos por parte del proveedor de recursos (Name, Role)

Para el atributo Name se indica que será enviada la dirección de correo completa del usuario con la finalidad de identificar el nombre del usuario y el dominio al que pertenece de la forma *usuario1@empresa1.com.ar*.

Para el atributo Role requerido por el servidor de recursos se utilizara el nombre del grupo al que pertenezca el usuario, en este caso solamente los usuarios que pertenezcan al grupo Intranet podrán tener acceso al recurso.

Una vez realizadas estas configuraciones cuando se acceda al sitio SSL de la intranet de la EMPRESA1 el sitio se redirigirá a un formulario de login provisto por el servidor de identidad.

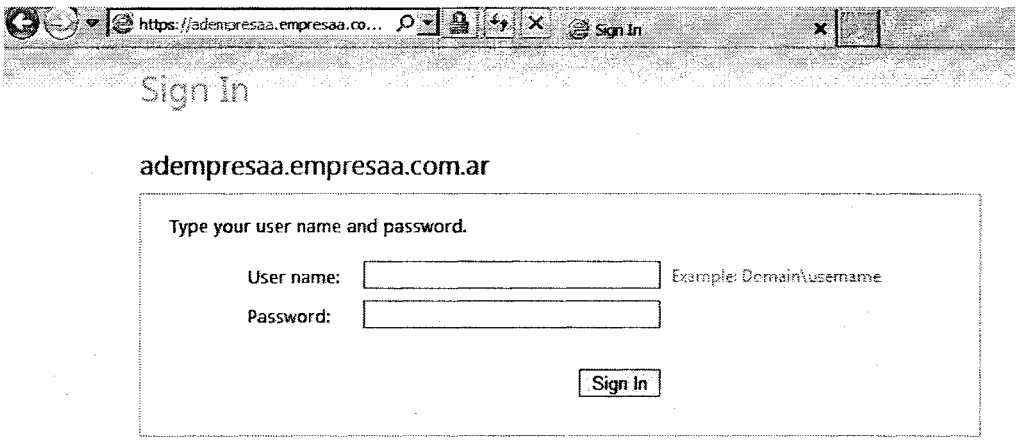

Figura 23 Interfaz login servidor ADFS

Con esto se completa el proceso de log in y el servidor de recursos procede a autorizar a los usuarios que pertenezcan al grupo Intranet y se les presenta la página de inicio del sitio.

Para que los usuarios del dominio EMPRESA2 puedan acceder al sitio se configurara la relación de confianza entre los dos servidores de identidad.

Se agregó al servidor de identidad de la EMPRESA2 en la zona de Claims Provider Trusts en la cual se encuentran los servidores que proveen la autenticación de usuarios, en esta zona se encuentra por defecto el active directory del dominio.

Al agregar la nueva relación se puede configurar la forma en la que serán recibidos los atributos del proveedor, en este caso se configuro un filtro para el atributo de dirección de correo electrónico para permitir solamente direcciones que pertenezcan al dominio empresab.com.ar

Para finalizar en el servidor de identidad de EMPRESA2 se debe agregar al servidor de identidad de EMPRESA1 en la zona de Relying Party Trust.

La relación de confianza establecida permite que el servidor de identidad de EMPRESA2 se encargue del proceso de autenticación de los usuarios de su dominio y comunique los atributos especificados al servidor de autenticación de EMPRESA1 que solamente se encargara de pasar estos atributos al servidor de recursos que se encuentra en su dominio.

El escenario implementado solventa la necesidad de dos organizaciones de compartir sus recursos simplificando el proceso de administración de los usuarios.

Para incluir un segundo factor a la autenticación de usuarios se ha decidido implementar un segundo factor de autenticación mediante el software DUO Security.

Esta herramienta deberá ser desplegada sobre cada uno de los servidores de autenticación ADFS 2.0 de la siguiente manera.

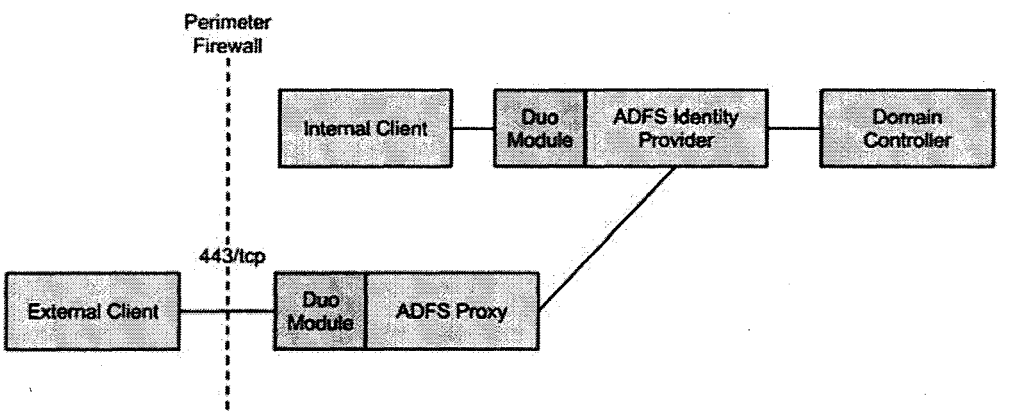

Figura 24 Implementación DUO sobre ADFS 2.0 [23]

Una vez implementado el modulo del segundo factor de autenticación cada uno de los usuarios debe seguir un proceso de enrolamiento dentro del sistema de DUO Security para lo que debe contar con un dispositivo con *IOS* o Android.

Debido a que la implementación incluye servicios de un proveedor externo se deben establecer requisitos de seguridad dentro del acuerdo de nivel de servicio:

- Establecer mediante un SLA un nivel de servicio que el proveedor de servicio tiene brindar.
- Todo el intercambio de información debe realizarse mediante el protocolo SSL.
- Acuerdo de confidencialidad de los nombres de los usuarios que sean enrolados dentro del sistema.
- Establecer un mecanismo para desactivar el segundo factor de autenticación en caso de falla del proveedor.

4.3 Resultados

La primera implementación se realizó en una organización multinacional de gran tamaño con gran cantidad de usuarios.
La implementación sigue las políticas propias de la organización ubicando los servidores en zonas DMZ y publicándolos a internet a través de conexiones protegidas por la infraestructura de seguridad existente en la organización.

Mediante la implementación de la infraestructura mostrada en la prueba de concepto se ha logrado brindar a la organización un servicio de autenticación seguro y de alta disponibilidad.

Al trabajar con la herramienta CA Strong Authentication 8.1 se pudo conocer el proceso para implementar un segundo factor de autenticación haciendo uso de infraestructura propia de la organización.
El haber realizado esta implementación permitió conocer en la práctica los requisitos de alta disponibilidad y seguridad de una organización de este tipo.

La segunda prueba de concepto se realizó sobre una infraestructura de menor tamaño a la anterior contando con un solo servidor que contiene al CMS.
Para la autenticación de usuarios principal se usó el mecanismo propio del CMS que hace uso de un usuario y contraseña.

Ya que el CMS usado en esta prueba de concepto usa un tipo de autenticación básica con la inclusión de un segundo factor de autenticación se logró aumentar la seguridad del mecanismo.
En la tercera prueba de concepto se implementó un esquema de autenticación entre dos organizaciones el que se realizó tomando en cuenta las recomendaciones para generar un esquema de federación de identidad seguro y confiable.

Se identificó que en la pruebas de concepto 2 y 3 la disponibilidad del servicio de segundo factor depende enteramente de un proveedor externo lo que significara que si el proveedor no se encuentra disponible no se podrá acceder a los servicios (sitio web DRUPAL, servicios corporativos organizaciones).

Con el uso de un proveedor externo para implementar el segundo factor de autenticación se ha podido conocer los procesos necesarios para realizar su implementación y los requerimientos para mantener su disponibilidad y seguridad.

5 Catálogo de Recomendaciones

Las siguientes recomendaciones cubren los requisitos relevados en los tres escenarios analizados y en las pruebas de concepto realizadas.
Están separados según el escenario en que aplican y divididos en requisitos de seguridad y en requisitos funcionales y operativos.

5.1 Recomendaciones para todos los escenarios

5.1.1 Funcionales y Operativas

RG-FO-01	**Servidor Secundario** Implementar servidores secundarios activos para los servidores de identidad, el servidor secundario responderá en caso de no disponibilidad del primario de forma transparente al usuario.
RG-FO-02	**Comunicaciones** Los canales de comunicaciones deben ser seguros y redundantes. Para el caso de las redes externas se recomienda disponer de dos o más proveedores.
RG-FO-03	**Backup** Servidor de Backup para el repositorio de usuario y las configuraciones del servidor de identidad. Política de backups periódicos, la periodicidad será definida por la cantidad de transacciones e información que maneje la empresa. Almacenar los medios que contienen los Backups resguardando su seguridad física. Almacenarlos en un lugar Offsite alejado geográficamente del centro de cómputos.
RG-FO-04	**Time Server** Incluir un time server dentro de la arquitectura, la implementación del mismo debe considerar alta disponibilidad.

RG-FO-05	**Gestión de Usuarios** Implementar una política de gestión de usuarios acorde a las necesidades de la empresa. Como mínimo definir los siguientes procesos: • Creación de nuevos usuarios. • Creación de roles de usuarios • Asignación y cambio de roles a usuarios. • Activación y desactivación de cuentas. • Reseteo de contraseñas.
RG-FO-06	**Auditoría y Control Interno del proceso** Definir un esquema de auditoria interna para todos los procesos involucrados en la autenticación de usuarios. Determinar si es necesario la inclusión de una auditoria externa sobre los procesos de acuerdo a las necesidades de la organización.
RG-FO-07	**Logs de Auditoria** Los logs deben almacenar la siguiente información: • Todas las acciones administrativas • Procesos de gestión de credenciales de usuarios incluso en el caso de sistemas de autogestión. • Casos de autenticación exitosa y fallida, • Todos los cambios de configuración que se realicen. Los registros de los logs deben tener una marca de tiempo para poder establecer correctamente la secuencia de eventos.

RG-FO-08	**Manejo de Fallas de Servicio** Documentar el proceso a seguir en caso de falla en el servicio de autenticación, definiendo responsables y acciones a tomar. Este proceso debe incluir las siguientes definiciones • Mecanismo de reporte de falla de servicio. • Responsables de reportar fallas de servicio. • Proceso de activación de servidores secundarios en el caso que se mantenga una configuración activo/pasivo. • Proceso para volver a configuración original. • Responsables de procesos.
RG-FO-09	**Plan de Recuperación de Desastres** La organización debe diseñar un plan de recuperación de desastres. Para desarrollar el DRP de la organización se recomienda seguir guías estandarizadas como: • NIST 800-34 Contingency Planning Guide for Federal Information Systems • ISO 27031 Guidelines for information and communication technology readiness for business continuity

5.1.2 Seguridad

RG-RS-01	**Contraseñas** Política de contraseña basada en estándares internacionales y requerimientos de regulaciones nacionales o sectoriales. Se recomienda mínimamente usar una contraseña que cumpla con: • Longitud mínima 8 caracteres. • Al menos una letra mayúscula. • Un signo de puntuación. • Al menos un digito numérico entre 0 y 9. • No se podrá repetir ninguna de las 6 últimas contraseñas utilizadas. Nota: En algunos sectores las regulaciones pueden solicitar valores superiores como por ejemplo la 4609BCRA que impone las ultimas 12 contraseñas
RG-RS-02	**Seguridad Ambiental del centro de Cómputos** Los servidores deben encontrarse en un ambiente controlado con temperatura y humedad de acuerdo a las recomendaciones del fabricante.
RG-RS-03	**Control de Acceso del centro de cómputos** Implementar control de acceso a las instalaciones mediante un PIN o tarjeta magnética. Registrar fecha y hora de acceso a las instalaciones del personal
RG-RS-04	**Gestión de Contingencias** El datacenter debe tener implementado mecanismos de protección en caso de desastres..
RG-RS-05	**Control de Incendios** Implementar un sistema de control de incendios que proteja a las instalaciones en caso de incendio causando el menor daño posible a los equipos.

RG-RS-06	**Protección antes fallas de alimentación eléctrica** Tener disponibles generadores eléctricos para solventar la falla del servicio de parte del proveedor. La instalación eléctrica deberá proteger a los equipos de altas y bajas de tensión.
RG-RS-07	**Protección Física de los canales de comunicación** Todas las conexiones de red internas y externas deberán ser instaladas de manera que se resguarde su integridad física.
RG-RS-08	**Mantenimiento Preventivo** Definir un cronograma de mantenimiento preventivo para todos los equipos involucrados en la implementación.
RG-RS-09	**Separación de Ambientes** Todos los servidores que se encuentre expuestos a una red externa insegura deberán incluirse en una zona DMZ.
RG-RS-10	**Firewall** La organización debe implementar un firewall con capacidad de analizar trafico especifico del protocolo de autenticación que se esté usando para detectar posibles amenazas
RG-RS-11	**Certificados Digitales** Todos los certificados digitales usados deben cumplir con el estándar X.509 v3. **Algoritmo Cifrado:** Curvas Elipticas ECC-1 de 160 bits o RSA 2048 bits **Algoritmo de Hash:**: sha2 512 o eventualmente sha3 de 1024 bits

RG-RS-12	**Cuentas de Servicio** Como política para una implementación de cualquier tipo que los passwords de las cuentas de servicio serán aleatorios y se almacenaran usando ensobrado digital. Las cuentas deben tener las siguientes características: • Usar cuentas locales de ser posible. • Cuenta con perfil básico. • Cuenta de dominio sin privilegios administrativos. • Permisos de lectura/escritura acotados a archivos y directorios necesarios.
RG-RS-13	**Single Sign On** Implementar single sign on para reducir el número de credenciales. La implementación debe incluir la funcionalidad de single log out, se recomienda usar SAML
RG-RS-14	**VPN** Implementar conexiones VPN con las sucursales, usar las recomendaciones del vpn consortium y sus arquitecturas recomendadas.[24]
RG-RS-15	**SSL** Todo servicio que vaya a ser consumido mediante un navegador web deberá ser implementado con el protocolo SSL.
RG-RS-16	**Múltiple Factor** Se recomienda implementar un segundo factor para autenticar un usuario para agregar seguridad a la implementación. En el caso de transacciones delicadas como las bancarias o pago de servicios, establecer una verificación de segundo factor para autorizar la acción.

5.2 Recomendaciones para servicios sobre una red corporativa

5.2.1 Funcionales y Operativas

RRC-FO-01	**Gestión de Usuarios** 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** Generar una política definiendo el protocolo a usar por las aplicaciones de la empresa y la forma de implementarlo. Implementar programas de capacitación en administración y desarrollo en los protocolos definidos en la estandarización

5.2.2 Seguridad

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

5.3 Recomendaciones para servicios públicos en Internet

5.3.1 Funcionales y Operativas

RPI-FO-01	**Conexiones de Respaldo** La organización deberá contar con al menos dos proveedores diferentes para asegurar alta disponibilidad de ser requerida
RPI-FO-02	**Autogestión de Usuarios** 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. Las acciones de los usuarios deben de quedar registradas en logs de auditoria.

5.3.2 Seguridad

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

5.4 Recomendaciones para servicios corporativos en la Nube

5.4.1 Funcionales y Operativas

RCN-FO-01	**Definir Roles** Definir los roles y responsabilidades de cliente y proveedor de servicio en el SLA según la ISO 17789.
RCN-FO-02	**Políticas de Negocio** Identificar las políticas internas y externas (regulaciones del sector o gubernamentales) que afecten al proceso y definirlas en el SLA.
RCN-FO-03	**Identificar Objetivo Critico** Definir alta disponibilidad para el servicio de autenticación dentro del SLA.
RCN-FO-04	**Proceso de cierre de contrato** Definir el proceso de finalización del contrato con el proveedor definiendo obligaciones de cada una de las partes. Se debe definir un tiempo para este proceso de cierre adecuado a las necesidades de la organización.
RCN-FO-05	**Fallas de Servicio** • Definir un responsable del monitoreo del servicio. • Establecer un mecanismo de notificación al proveedor. • Definir en el SLA el tiempo máximo de falta de servicio. • Documentar proceso de recuperación de servicio.
RCN-FO-06	**Plan de recuperación de desastres** Definir conjuntamente con el proveedor el proceso de recuperación de desastres, definir responsables de proceso

5.4.2 Seguridad

RCN-RS-01	**Requerimientos de Seguridad y Privacidad** 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** 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.

6 Conclusiones

Durante el desarrollo de esta tesis se ha realizado una revisión de distintos escenarios de autenticación que se presentan en la actualidad. Este análisis permitió identificar los requisitos funcionales y de seguridad particulares a cada escenario.

Además se identificaron requerimientos comunes a todos y se han propuesto recomendaciones para implementar cada uno de los requerimientos. Para identificar los requerimientos y evaluar posibles recomendaciones fueron muy importantes los conocimientos obtenidos durante el estudio del posgrado, y la revisión de normas y estándares nacionales e internacionales tales como la ISO 17789. Esta norma es específica a los servicios prestados en la nube.

Para complementar el marco teórico se ha realizado una prueba de concepto con tres escenarios, el primero es un servicio de Internet basado en DRUPAL, el segundo es un escenario interno basado en Federación de Identidad con doble factor para la autenticación y el tercero es un escenario mixto de una organización que brinda un servicio basado en recursos internos a usuarios que acceden desde el exterior por internet. Estas maquetas se realizaron para aplicar las recomendaciones obtenidas durante el relevamiento.

Como resultado del relevamiento y de la prueba de concepto se puede observar que la disponibilidad es un factor de gran importancia en un esquema de autenticación. Si no está disponible este servicio todas las operaciones se verán interrumpidas.

Al revisar los resultados de la prueba de concepto se puede observar que la implementación de un esquema de autenticación dependerá de las características propias de cada organización y de los recursos con los que cuentan,

Para concluir es importante destacar que cada implementación se debe guiar en estándares y normas internacionales que se apliquen a los servicios que se quieran implementar.

Como ayuda en este proceso, en este trabajo se propone un catálogo de recomendaciones que entiendo sirven de base para lograr una implementación segura y confiable.

7 Bibliografía

[1] «¿Cuál es la definicion de Autentificación?» [En línea]. Disponible en: http://www.alegsa.com.ar/Dic/autentificacion.php. [Accedido: 21-abr-2015].

[2] «Cloud Standards Customer Council Resource Hub». [En línea]. Disponible en: http://www.cloud-council.org/resource-hub.htm#practical-guide-to-cloud-service-agreements-version-2. [Accedido: 20-jul-2015].

[3] «CSCC_Practical_Guide_to_Cloud_Service_Agreements_Version_2.0.pdf». .

[4] «ITAF-3rd-Edition_fmk_Eng_1014.pdf». .

[5] «NIST SP 800-118, Guide to Enterprise Password Management (DRAFT) - draft-sp800-118.pdf». .

[6] «Aplicación de "Envío de Comunicaciones y Comunicados" - a4609.pdf». .

[7] «Physical and environmental security (ISO 17799-27002) Privacy / Data Protection Project (c)2002-2005». [En línea]. Disponible en: http://privacy.med.miami.edu/glossary/xd_iso_phys_env_sec.htm. [Accedido: 15-jun-2015].

[8] «NIST SP 800-44 Version 2, Guidelines on Securing Public Web Servers - SP800-44v2.pdf». .

[9] «NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy - sp800-41-rev1.pdf». .

[10] «Fear the golden ticket attack! | InfoWorld». [En línea]. Disponible en: http://www.infoworld.com/article/2608877/security/fear-the-golden-ticket-attack-.html. [Accedido: 14-may-2015].

[11] «CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf». .

[12] «Securing Critical and Service Accounts». [En línea]. Disponible en: https://msdn.microsoft.com/en-us/library/cc875826.aspx. [Accedido: 13-dic-2015].

[13] «Running Apache for Windows as a Service». [En línea]. Disponible en: http://kypros.org/manual/win_service.html. [Accedido: 13-dic-2015].

[14] «NIST SP 800-113, Guide to SSL VPNs - SP800-113.pdf». .

[15] D. Stebila y K. Igoe, «X.509v3 Certificates for Secure Shell Authentication». [En línea]. Disponible en: https://tools.ietf.org/html/rfc6187. [Accedido: 02-dic-2015].

[16] «PKI». [En línea]. Disponible en: http://www.oasis-pki.org/resources/techstandards/. [Accedido: 02-dic-2015].

[17] «What is multifactor authentication (MFA)? - Definition from WhatIs.com». [En línea]. Disponible en: http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA. [Accedido: 20-may-2015].

[18] «ISO/IEC 17789:2014 - Information technology -- Cloud computing -- Reference architecture». [En línea]. Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=60545. [Accedido: 24-jul-2015].

[19] «Two-Factor Authentication for Drupal CMS», *Duo Security*. [En línea]. Disponible en: https://www.duosecurity.com/docs/drupal. [Accedido: 08-jul-2015].

[20] «CA Strong Authentication - CA Technologies». [En línea]. Disponible en: http://www.ca.com/ar/securecenter/ca-strong-authentication.aspx. [Accedido: 24-jul-2015].

[21] E. Garibay, «Administracion de Bases de Datos: Espejeo en Bases de Datos», *Administracion de Bases de Datos*, 29-abr-2013. .

[22] Andres Jadan, «Federación de Identidad aplicada a la autenticación de aplicaciones entre organizaciones». 15-dic-2014.

[23] «Two-Factor Authentication for Microsoft AD FS 2.0 and 2.1 - Duo Security». [En línea]. Disponible en: https://www.duosecurity.com/docs/adfs. [Accedido: 08-jul-2015].

[24] «VPN Protocols». [En línea]. Disponible en: http://www.vpnc.org/vpn-standards.html. [Accedido: 24-jul-2015].