ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN SISTEMA DE AUTENTICACIÓN FEDERADA, SINGLE SING ON, PARA UNA EMPRESA DE MEDICINA PREPAGADA"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

EDISON RIGOBERTO HERRERA ÁLVAREZ

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Al culminar otra etapa de mí mis estudios profesionales me permito agradecer infinitamente a mis padres que me han apoyado siempre. A mi esposa por su cariño incondicional y a todos los docentes de la mejor universidad del Ecuador ESPOL.

DEDICATORIA

Dedico éste trabajo a mi hijo Juan José quien con su inocencia me ha inspirado para ser mejor cada día, a mi esposa Gaby por ser mi apoyo incondicional y a mis hermanas por ser mi ejemplo de superación.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

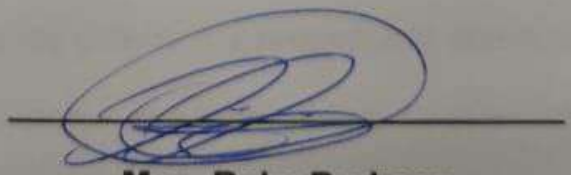
DIRECTOR MSIA

por: MSc. Ana María Falcones

Mgs. Gonzalo Luzardo

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC



Mgs. Roky Barbosa

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

RESUMEN

En líneas generales, el presente trabajo contiene:

- El resumen de la situación actual, incluidas las incidencias contextuales o de negocio.
- Las necesidades y expectativas de la empresa.
- La tecnología propuesta para respaldar los procesos de negocio.
- Los pasos para la implementación de la tecnología seleccionada.
- El soporte post implementación.

Este documento es el punto de partida de la solución y el desarrollo de la misma y supone un esfuerzo conjunto entre todos los participantes tecnológicos y de la empresa. La finalidad del presente trabajo es exponer las necesidades de negocio respecto al proceso de administración centralizada de usuarios externos y presentarlo como caso de negocio para que el lector pueda tomarlo como referencia en posteriores implementaciones y pueda aplicarlo en cualquier vertical de la industria.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

.NET	Framework de desarrollo de Microsoft
AD	Active Directory
ADFS	Active Federation Services
BEA	Company specialized in enterprice infrastructure
CA	Certification Authority
CPU	Central Processing Unit
DMZ	Demilitarized zone
DNS	Domain Name System
IBM	International Business Machines
IIS	Internet Information Services
PKI	Public Key Infrastructure
RSA	The Security Division of EMC
SCOM	System Center Operations
SSL	Secure Sockets Layer
SSO	Single Sing On
URL	Uniform Resource Locator
WAP	Web Application Proxy

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad de la información comprende todos los mecanismos preventivos y reactivos que permiten proteger el activo principal de toda organización, su información con el fin de mantener la confidencialidad, la integridad y la disponibilidad de la misma.

La confidencialidad impide que la información sea divulgada a personas o sistemas no autorizados. Tomando en cuenta los recientes incidentes de seguridad presentados en la empresa de Medicina Prepagada estadounidense Anthem, en donde la información privada de pacientes como los datos de contacto y procedimientos médicos realizados fueron interceptados y vendidos a un alto precio. Se ve la necesidad de contar con un mecanismo de autenticación que permita optimizar el proceso de gestión de usuarios externos, que represente un ahorro de tiempo y recursos pero que a la vez cumpla con los estándares de seguridad modernos.

Este documento contiene las especificaciones técnicas para implementar un sistema de autenticación federada en donde se describe el análisis, diseño e implementación en una empresa de Medicina Prepagada.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

Las Empresas de Medicina Prepagada en el Ecuador trabajan con una red de servicios conformada por organizaciones, sistemas, aplicaciones y procesos de negocio. Varios componentes forman parte de esta red incluyendo clientes, empleados, socios estratégicos, proveedores y prestadores. No existe un estándar que administre o controle la información de estas entidades de forma centralizada. Incluso dentro de una misma organización pueden existir varios repositorios autorizados de datos de identidad que son gestionados de forma autónoma.

Actualmente la mayoría de empresas de seguros cuentan con una administración de usuarios descentralizada lo que implica una serie de actividades enfocadas en la integración entre sistemas, lo que resulta en altos costos en la gestión de identidad así como también poca eficiencia en los procesos. Con este enfoque la administración del ciclo de vida de identidad de un usuario es muy alta. La mayoría de empresas tienen que gestionar empleados, socios estratégicos y clientes. Además, las relaciones entre la empresa y estas entidades cambian constantemente, cada cambio requiere de una acción administrativa.

Estas empresas requieren aprovechar las capacidades de las entidades federadas para permitir interacciones con negocios nuevos. Sin embargo la implementación de sistemas de confianza para permitir transaccionalidad entre entidades federadas transversal a varios negocios es difícil. Por otra parte, las empresas que gestionan identidades federadas sufren un alto riesgo de sufrir daños a la reputación o responsabilidades legales si sus acciones de administración de identidad liberan o utilizan la información de forma que entren en conflicto con las políticas de privacidad. Esto aumenta enormemente el riesgo de la gestión de identidad.

La administración de identidades federadas brinda flexibilidad en la creación de nuevos negocios entre empresas al mismo tiempo permite simplificar los costos de la gestión de identidad. Esto permite a las empresas cubrir los objetivos de integración que mejor se adapte al modelo de negocio, las políticas de TI, los objetivos de seguridad y de gobernanza.

1.2 SOLUCIÓN PROPUESTA

La autenticación federada fue diseñada con la intención de permitir a un usuario autenticarse sin problemas en diferentes sitios dentro de una red de prestadores. La presente propuesta se basa en la gestión de identidad federada, a través de la implementación de Active Directory Federation Services (ADFS) [1].

ADFS es un componente de software creado por Microsoft que puede ser instalado en un sistema operativo Windows Server y que implementa el protocolo *WS-Federation*. Utiliza un modelo de autenticación basada en notificaciones [2].

Debido a las relaciones de confianza establecidas entre los participantes de la federación, un miembro es capaz de autenticar a un usuario y luego actuar como emisor del usuario y los otros miembros de la federación actúan como partes que confían. Es decir, se basan en la información que comparte el emisor sin la participación del usuario.

Los resultados esperados son la implementación de SSO para los usuarios del sistema de Medicina Prepagada y la aplicación Médico en Línea, en fases posteriores se realizara la migración del resto de aplicaciones de la empresa.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS Y DISEÑO

En esta sección se describe la documentación de la fase de análisis y relevamiento de información para la "**Implementación de un sistema de autenticación federada, Single Sing On, para una Empresa de Medicina Prepagada**".

La etapa de relevamiento de información es una oportunidad para que el negocio y el equipo implementador discutan, acuerden y compartan la misma visión y alcance del proyecto. Al finalizar ésta etapa se definirá la

situación actual y objetivos de diseño. El enfoque en ésta etapa inicial, es la de entender y priorizar las necesidades del negocio, así como especificar las modificaciones a la arquitectura de infraestructura de la empresa.

2.1.1 ESTADO ACTUAL

Las empresas de seguros de Medicina Prepagada tienen como objetivo cuidar de la salud de sus clientes a través de la oferta de planes y productos orientados a tres segmentos principales de mercado los planes familiares, pymes y corporativos. En el Ecuador existen varias empresas que ofrecen este servicio, cada empresa se diferencia de la competencia al ofrecer una serie de beneficios expresados en máximos de cobertura para cada procedimiento médico.

La tecnología actual habilita a las empresas a ofrecer medios de consulta y transacciones a sus clientes debido al crecimiento acelerado de Internet. Gracias a este crecimiento cada servicio

debe ser soportado por una plataforma de software que exponga estos requerimientos sobre Internet por otra parte la ejecución de proyectos de software es compleja debido a que hay limitaciones respecto al tiempo sobre la cantidad de requerimientos funcionales a implementar por consiguiente los requerimientos no funcionales como por ejemplo la autenticación y el control de acceso son abordados de la manera más simple posible teniendo varios repositorios en donde se almacenan usuarios externos.

Los clientes poseen varias identidades para cada servicio publicado en Internet esto implica riesgos de seguridad al no contar con un estándar de autenticación y mucho trabajo de administración para mantener el acceso a cada usuario externo por cada aplicación desplegada en Internet. Por consiguiente el trabajo administrativo implica costos de mantenimiento, la duplicación de horas de trabajo al tener que mantener varios repositorios de usuario y el riesgo de afectar a la confidencialidad de la información.

A continuación se muestra el estado actual de las aplicaciones desplegadas en Internet:

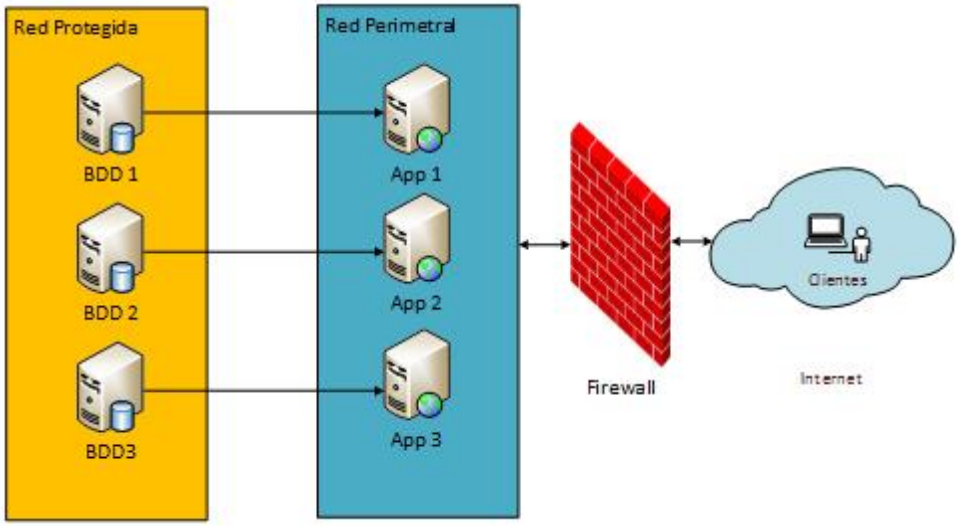


Figura 2.1 Situación actual

2.1.2 DISEÑO DE LA SOLUCIÓN

Con el objetivo de reducir los costos relacionados al mantenimiento de usuarios externos y proteger la confidencialidad de la información se ha definido que los clientes tendrán una sola identidad para tener acceso a los servicios de Medicina Prepagada. Puesto que se ve la

necesidad de ingresar a los servicios desde cualquier sitio y la autenticación de los usuarios internos actualmente se administra con Microsoft Active Directory (AD), se define desplegar servicios de ADFS en dos redes privada y perimetral, cada red va acompañada de un rol de ADFS.

La primera red es la red perimetral o DMZ definida para brindar el acceso desde Internet además aquí se encuentra el servidor WEB Application Proxy destinado para permitir la comunicación entre Internet y el servidor federación. La segunda red contiene el servicio de Active Directory y se encuentra protegida en consecuencia los usuarios externos no pueden tener acceso desde Internet también cuenta con el servicio Active Directory Federation Services el cual facilita el proceso seguro de distribución de identidad de usuario por medio de relaciones validas de federación.

El diseño conceptual propuesto se muestra en la siguiente figura:

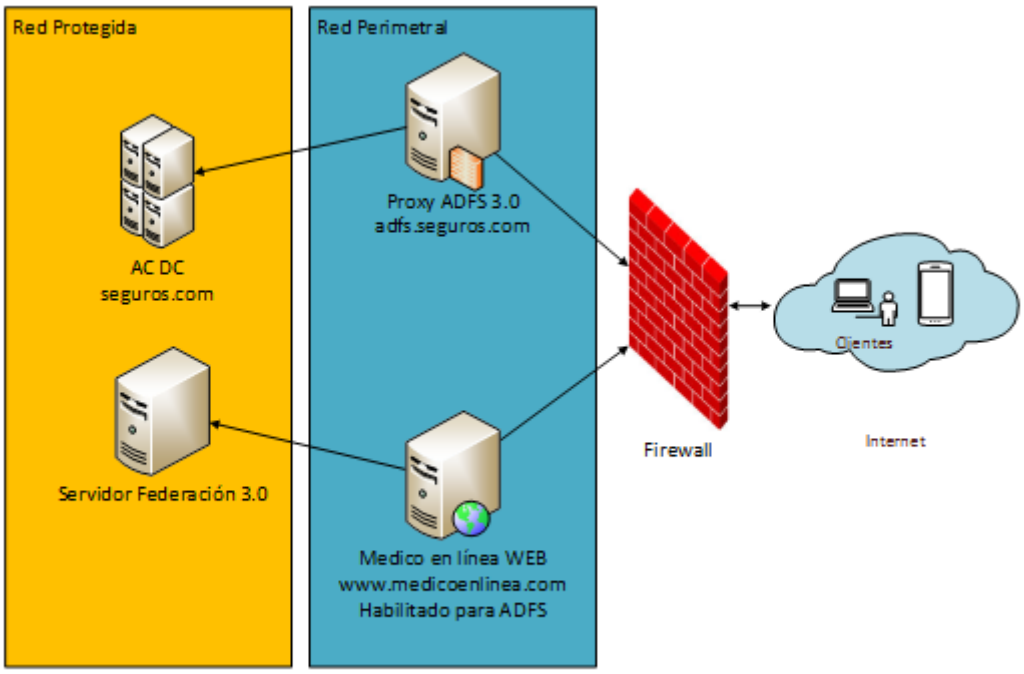


Figura 2.2 Diseño de solución

Se da por hecho que la empresa de Medicina Prepagada ya cuenta con la configuración de AD, DNS y tiene segmentada la red en red privada y red perimetral.

2.1.3 COMPONENTES DE LA SOLUCIÓN

Se ha seleccionado la versión de ADFS 3.0 para configuración de la identidad federada la cual se debe instalar sobre el sistema operativo Windows Server 2012 R2 Update 1.

2.1.4 ROLES ADFS

ADFS se debe instalar en dos roles:

- Active Directory Federation Services
- Web Application Proxy

Los cuales deben ser instalados en dos servidores diferentes. Para esta configuración únicamente se desplegaran dos servidores uno para cada rol, no se ha considerado servidores de contingencia por una limitación de presupuesto.

2.1.5 CERTIFICADOS

Es necesario contar con un certificado SSL previo a la configuración tenemos tres opciones de certificado:

- Certificado auto firmado.
- Certificado emitido por la PKI interna.
- Certificado por una entidad CA.

Para esta instalación se seleccionó el certificado emitido por una CA y el certificado fue creado para el dominio win-msg476nnbar.seguros.ec.

2.2 CREACIÓN E IMPLEMENTACIÓN

Como pudimos visualizar en la sección anterior el servicio ADFS se procederá a instalar en dos roles Active Directory Federation Services y Web Application Proxy.

INSTALACIÓN DE ACTIVE DIRECTORY FEDERATION SERVICES

Para implementar ADFS es necesario seguir los siguientes pasos:

1. Ingrese al servidor Windows Server 2012 R2 dentro del administrador del sistema agregue el rol Active Directory Federation Services.

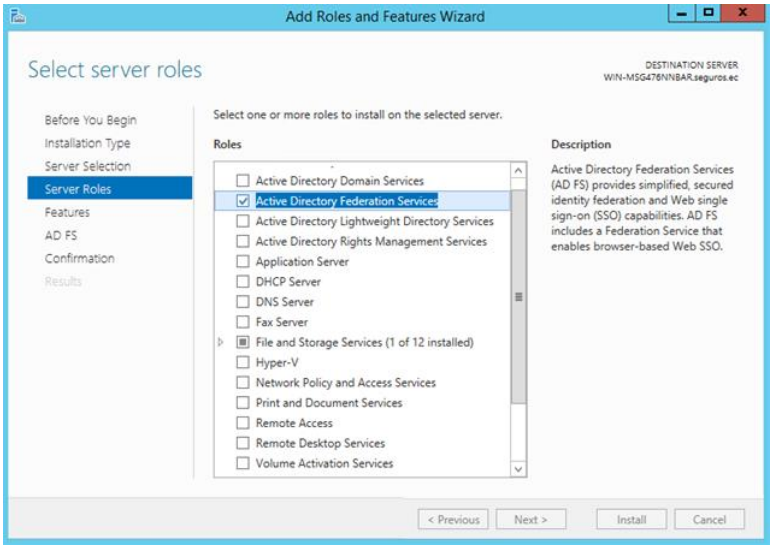


Figura 2.3 Seleccionar rol del servidor

2. Continúe con el instalador hasta el final y luego en la consola de administración haga click en Configure el servicio de federación.

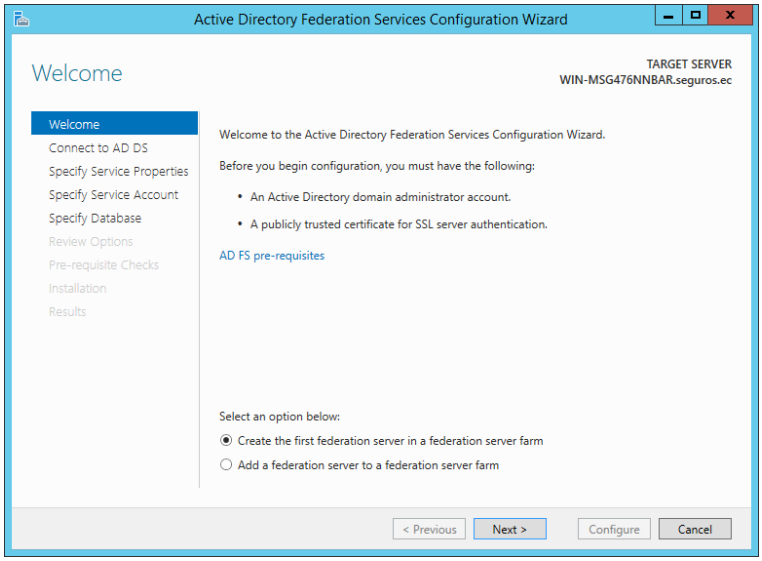


Figura 2.4 Instalación ADFS

3. Continuar los pasos de instalación hasta el punto Especificar propiedades del servicio, seleccione el certificado win-msg476nnbar.seguros.ec y luego introduzca el nombre del servicio.

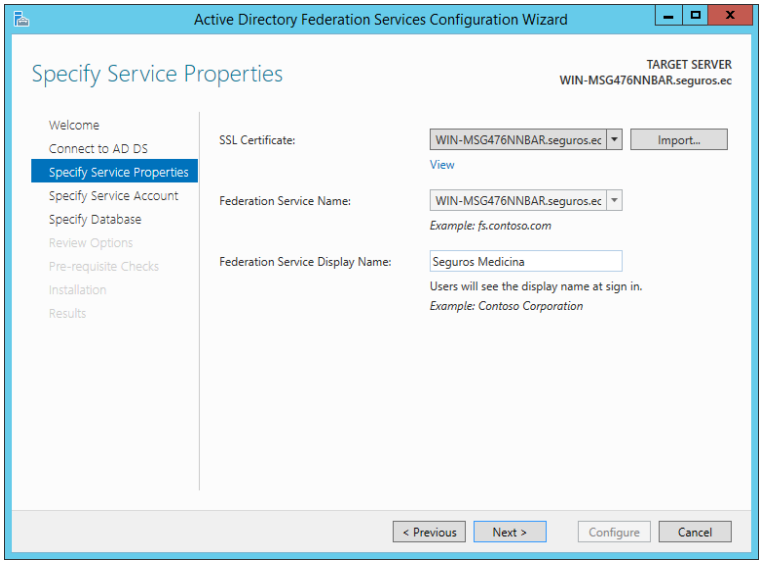


Figura 2.5 Certificado SSL

4. Continuar con el asistente hasta el final, al terminar cierre el asistente.

PROBAR LA INSTALACIÓN DE ACTIVE DIRECTORY FEDERATION SERVICES

Para verificar que la instalación esté correcta haga lo siguiente:

1. Dentro del servidor ADFS abra el explorar de internet predeterminado.

   Digite la URL

https:// win-msg476nnbar.seguros.ec /adfs/ls/idpinitiatedsignon.htm

2. Es necesario comprobar que no existe ninguna advertencia en el certificado SSL.
3. Debe aparecer una página similar a la siguiente imagen.

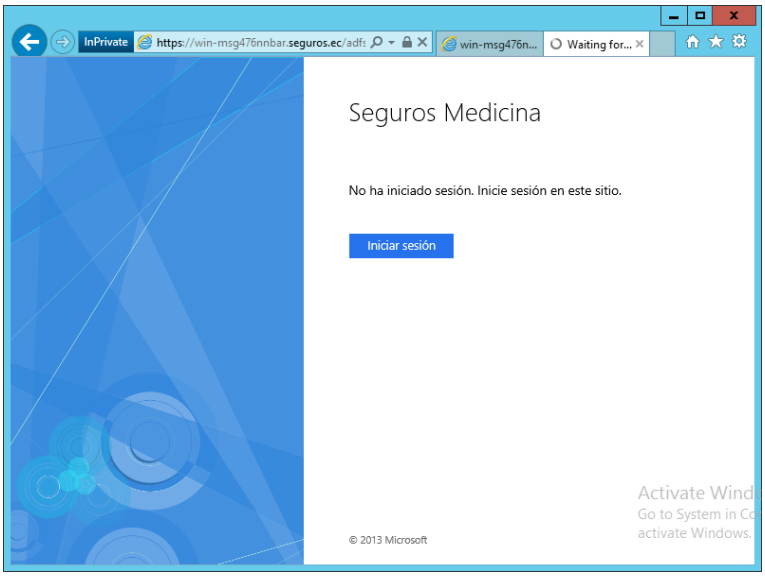


Figura 2.6 Prueba de instalación exitosa

INSTALACIÓN DE WEB APPLICATION PROXY WAP

1. Ingrese al servidor Windows Server 2012 R2 dentro del administrador del sistema agregue el rol Remote Access.
2. En la sección rol de servicio seleccione Web Application Proxy. A continuación se desplegara el asistente para la configuración.

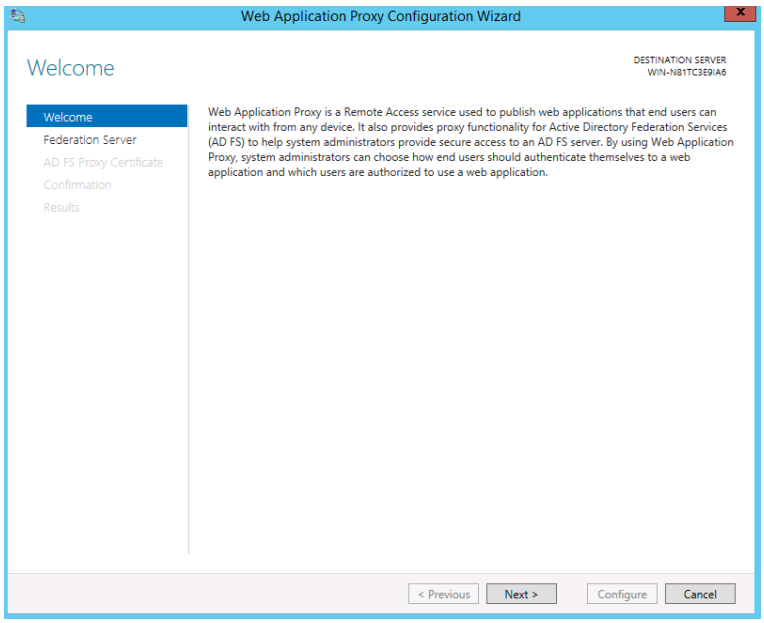


Figura 2.7 Instalación WAP

3. En este punto debemos importar el certificado de seguridad y asegurarnos que se instaló dentro de Trusted Root Certification Authorities.

4. En la opción Servidor de Federación, ingresar el nombre del servicio de federación configurado en el rol anterior.

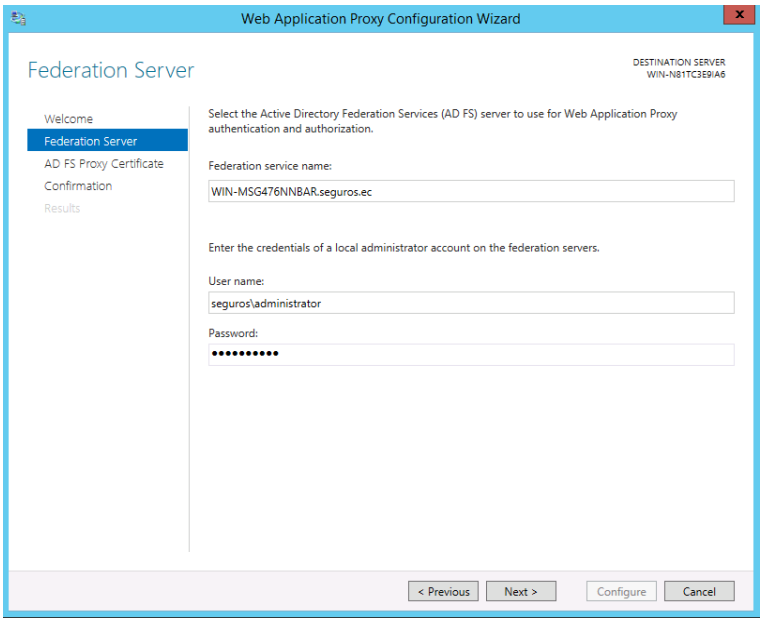


Figura 2.8 Selección servicio de federación

5. Selecciónar el certificado SSL previamente importado.

6. Finalizar la instalación y comprobar que esté funcionando los servicios de federación.

PROBAR LA INSTALACIÓN DE WAP

Para verificar que la configuración esté correcta haga lo siguiente:

1. Dentro del servidor WAP abra el explorar de internet predeterminado. Digite la URL

   https:// win-msg476nnbar.seguros.ec /adfs/ls/idpinitiatedsignon.htm

2. Es necesario comprobar que no existe ninguna advertencia en el certificado SSL.
3. Debe aparecer una página similar a la siguiente imagen.

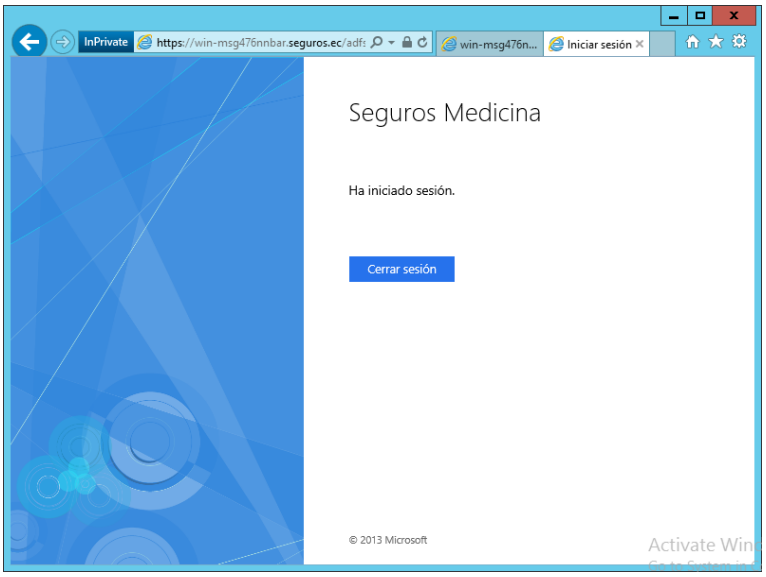


Figura 2.9 Prueba instalación correcta

INTEGRACIÓN CON EL SISTEMA

Los pasos siguientes explicar los pasos necesarios para modificar la aplicación web para utilizar la autenticación mediante ADFS.

1. Registrar el agente web de ADFS, en el archivo web.config del servidor IIS.

```
<webServer>
  - <modules>
        <add
            type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule,
            System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
            PublicKeyToken=31BF3856AD364E35, Custom=null" name="AD FS
            Web Agent"/>
    </modules>
</webServer>
```

Figura 2.10 Registro módulos IIS

2. Modificar el archivo web.config de la aplicación para agregar una sección personalizada que contiene el Handler SSO.

```
<configSections>
  - <sectionGroup name="system.web">
        <section
            type="System.Web.Security.SingleSignOn.WebSsoConfigurationHandler,
            System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
            PublicKeyToken=31BF3856AD364E35, Custom=null"
            name="websso"/>
    </sectionGroup>
</configSections>
```

Figura 2.11 Handler SSO

3. Agregar la referencia del end point del servicio web de ADFS.

```
<websso>
    <fs>https://win-msg476nnbar.seguros.ec/adfs/fs/federationserverservice.asmx</fs>
  - <urls>
        <returnurl>https://webserver/MedicoLinea/Login.aspx</returnurl>
    </urls>
  - <cookies writecookies="true">
        <path>/MedicoLinea</path>
    </cookies>
    <authenticationrequired/>
</websso>
```

Figura 2.12 End point ADFS

4. Agregar las referencias a las dlls SSO del framework .Net.

```
<system.web>
    <authentication mode="None"/>
  - <compilation debug="true" defaultLanguage="c#">
      - <assemblies>
            <add assembly="System.Web.Security.SingleSignOn, Version=1.0.0.0,
                Culture=neutral, PublicKeyToken=31BF3856AD364E35"/>
            <add assembly="System.Web.Security.SingleSignOn.ClaimTransforms,
                Version=1.0.0.0, Culture=neutral,
                PublicKeyToken=31BF3856AD364E35"/>
        </assemblies>
    </compilation>
</system.web>
```

Figura 2.13 Referencia framework .Net

5. En el proyecto web agregar las referencias a los componentes SSO.

```
using System.Web.Security.SingleSignOn;
using System.Web.Security.SingleSignOn.Authorization;
```

Figura 2.14 Uso componente SSO

6. Definir el objeto manejador SSO.

```
private void Page_Load(object sender, System.EventArgs e)
{
    SingleSignOnIdentity SsoId = User.Identity as
SingleSignOnIdentity;
}
```

Figura 2.15 Manejador SSO

7. Validar si esta autenticado el usuario, si es verdadero permitir el acceso, caso contrario enviar a la pagina de inicio de sesión.

```
if (SsoId.IsAuthenticated)
{
    // ...
}
else
{
    // Redirecciona al usuario al AD FS Logon service.
    SsoId.SignIn(Context);
}
```

Figura 2.16 Validación usuario autenticado

8. Publicar la aplicación web y asignar los roles de usuario en la aplicación.

2.3 SUPERVISIÓN Y MANTENIMIENTO

Es necesario monitorear y dar mantenimiento a la plataforma, Microsoft recomienda el uso de la herramienta System Center Operations Manager la cual por medio de ciertos contadores específicos miden el estado o la actividad del sistema, estos contadores pueden ser parte del servidor o puede ser parte de cada aplicación. La empresa de Medicina Prepagada ya cuenta con esta herramienta lo cual nos facilita el trabajo.

Existen contadores específicos para monitorear ADFS que ayudan para detectar problemas en el servicio y son:

- Solicitudes totales por segundo
- Solicitudes de token totales
- Solicitud de latencia
- Solicitudes rechazadas por segundo
- Total de solicitudes rechazadas
- Todos los contadores de error de inicio de sesión
- % de uso de disco

- % de uso de memoria
- % de uso de CPU

A continuación se muestra una captura de la herramienta de monitoreo:

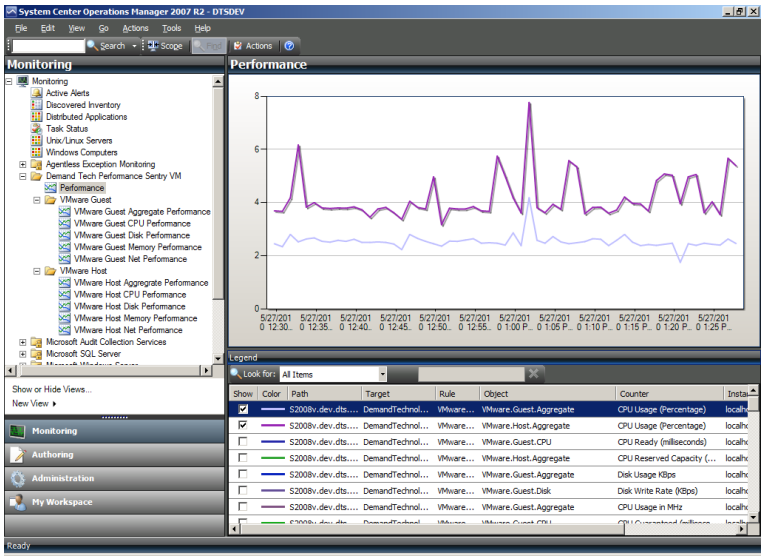


Figura 2.17 Herramienta SCOM

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

Los usuarios experimentan una mejora significativa puesto que se autentican una sola vez en sitio de la empresa y así pueden utilizar los servicios que la empresa de Medicina Prepagada expone.

3.1 REDUCCIÓN DE COSTOS DE MANTENIMIENTO USUARIOS

Para hacer evidente la reducción del esfuerzo en la gestión de usuarios se tomó en cuenta los siguientes indicadores:

Tabla 3.1 Indicadores de medición

Indicador	Formula
Cantidad usuarios externos	= Número de clientes que necesitan acceso a los servicios de la empresa.
Costo por minuto recurso	= Gastos nomina / (Productividad recurso * 60) En este caso vamos a tomar como ejemplo un sueldo de 1.100 mensuales por operador. = 1.100/ 9600 = 0,11 $
Productividad recurso	= Horas-hombre trabajadas es igual a 160 al mes
Tiempo promedio alta usuario sistema	= tiempo en minutos creación usuario.
Costo promedio alta de usuario	= Cantidad usuarios externos x Tiempo promedio alta usuario sistema x Costo por minuto recurso

Antes de la implementación de SSO, cada cliente poseía un usuario y contraseña para el Portal de clientes y otra para Medico en línea. Cada aplicación cuenta con una tabla de usuarios la misma que debía ser llenada por el operador antes de asignar el rol correspondiente dentro de cada plataforma. A continuación se muestra las mediciones realizadas para cada sistema:

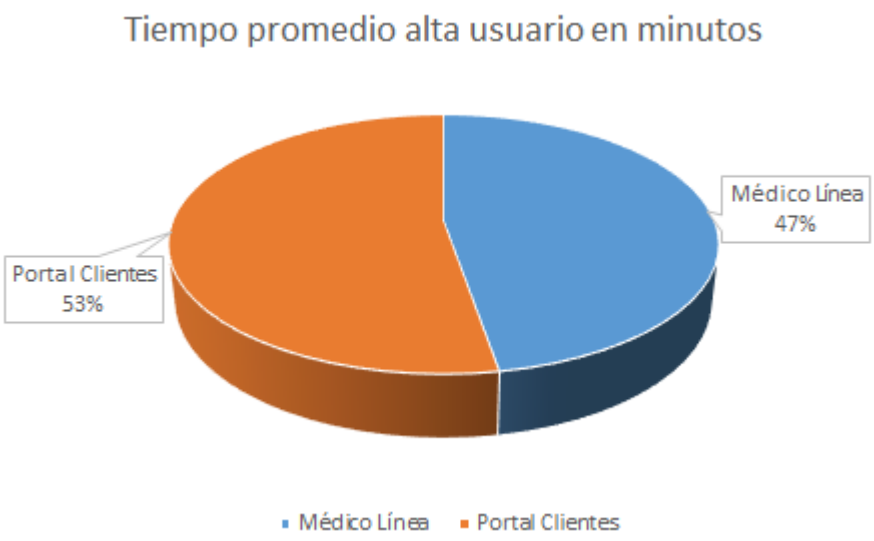


Figura 3.18 Tiempo promedio alta usuario 7,4 minutos

Luego de la implementación de la autenticación SSO el proceso de alta de usuarios externos cambia puesto que ahora son administrados en Active Directory, luego el operador debe asignar el rol en cada sistema web.

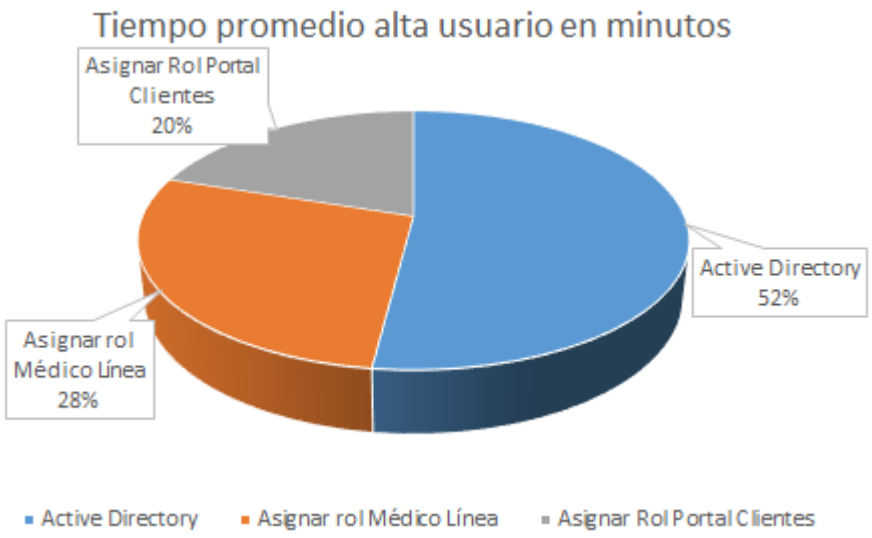


Figura 3.19 Tiempo promedio de alta usuario 5 minutos

Vamos a calcular el costo total de alta de usuarios.

Costo promedio alta de usuario antes SSO= 7,4 * 0,11 = 0,78 $

Costo promedio alta de usuario luego SSO= 5 * 0,11 = 0,57 $

Ahorro por transacción = 0,78 - 0,57 = 0,21 $

Como podemos validar existe un ahorro de 0,21 $ por cada operación de alta de usuario externo este valor representa un ahorro del 27 % de por cada transacción, si tomamos en cuenta que la empresa de Medicina Prepagada incluye en promedio 1000 clientes mensuales entonces el ahorro es más evidente en términos financieros:

Ahorro promedio = 1.000 * 0,21 = 210 $

En tiempo representa = 1.000 * (7,4 - 5) / 60 = 40 horas de esfuerzo

3.2 DETECCIÓN DE PROBLEMAS DE AUTENTICACIÓN

Luego de la puesta en producción de la herramienta fue necesario realizar una campaña de marketing para comunicar a los clientes como ingresar a la plataforma de Médico en Línea. Se pudo observar un incremento del 50% de incidencias totales procesadas por contact center de empresa respecto a problemas con el ingreso a la plataforma, sin embargo luego

de dos semanas el número de incidencias se estabilizo con el 10% de llamadas por problemas con el ingreso.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Mediante la implementación de un sistema centralizado de administración de usuarios es posible la disminución de los costos asociados gracias a la reducción de esfuerzo puesto que no se duplican los registros de identidad.

2. Los administradores de IT optimizan su trabajo debido a que enfocan su esfuerzo en crear una única identidad con las medidas de seguridad apropiadas al contrario de conceder el acceso a varios sistemas sin garantías de privacidad.

3. ADFS implementa el protocolo WS-Federation dado que fue diseñado por Microsoft, IBM, Verisign, BEA y RSA Security la empresa está en condición de colaborar con cualquier socio estratégico a futuro.

4. Cuando un cliente termina su contrato con la empresa de Medicina Prepagada basta con deshabilitar al usuario externo en AD para bloquear el servicio.

RECOMENDACIONES

1. Recomienda continuar con el proyecto para agregar el resto de aplicaciones a esta plataforma y así contar con los beneficios de la administración de usuarios centralizada.

2. ADFS debe ser configurado con un certificado SSL para el dominio de la empresa de Medicina Prepagada, este certificado debe ser renovado anualmente se recomienda contar con un responsable en esta gestión.

3. Es importante tener clara la arquitectura de la administración de usuarios por lo que se recomienda establecer un proceso de capacitación a los operadores de infraestructura y al área de desarrollo de aplicaciones con el objetivo aprovechar al máximo esta plataforma.

4. ADFS permite a la organización contar con una arquitectura escalable por otra parte el negocio de la Medicina Prepagada cambia dinámicamente por lo cual se recomienda tener presente esta implementación cuando se planifique la integración con una red de prestadores.

BIBLIOGRAFÍA

[1] Microsoft Developer Network, Introducción a ADFS, https://msdn.microsoft.com/es-es/library/cc786469(v=ws.10).aspx, fecha de consulta julio 2015.

[2] IBM, Web Services Federation Language (WSFederation), http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf?S_TACT=105AGX04&S_CMP=LP, fecha de consulta julio 2015.

[3] Microsoft Developer Network, Understanding WS-Federation, https://msdn.microsoft.com/en-us/library/bb498017.aspx, fecha de consulta julio 2015.

[4] We Live Security, Robo de registros y datos de salud: más que información médica, http://www.welivesecurity.com/la-es/2015/03/02/robo-de-registros-datos-salud-informacion-medica/, fecha de consulta julio 2015.

[5] Microsoft Developer Network, Escenarios de federación, https://msdn.microsoft.com/es-es/library/cc757344(v=ws.10).aspx fecha de consulta julio 2015.