Diseño e implementación de una solución de integración de autenticación entre plataformas Windows y Linux, utilizando el directorio activo de Windows como controlador de dominio

Jazmín Del Rocío Avilés Carpio [1]
Mildred Yanina Peralta Orrala [2]
Facultad de Ingeniería en Electricidad y Computación [1]
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
jdaviles@espol.edu.ec [1]
myperalt@espol.edu.ec [2]
Director de tesis Ing. José Roberto Patiño Sánchez, mail: jpatino@espol.edu.ec [3]

Resumen

El presente proyecto solventa la problemática en el servicio de autenticación de los usuarios, por la presencia de ambientes híbridos en las empresas, se planteó dos alternativas que permiten la integración del servicio de autenticación entre las plataformas Linux y Windows, utilizando el sistema operativo Windows como controlador de dominio, por lo que se emplearon servidores y estaciones de trabajo virtuales de ambas plataformas para la ejecución de las pruebas, siendo utilizado en el ambiente Windows la estación de trabajo Windows 8 y como servidor Windows Server 2012 R2 y en el ambiente Linux la estación de trabajo Ubuntu 14.04 y como servidor CentOS 7.0.
Los métodos de integración que se utilizaron en este proyecto fueron System Security Services Daemon (SSSD) y Winbind, los cuales involucran a los protocolos Lightweight Directory Access Protocol (LDAP) y Kerberos. Ambos métodos permiten que los clientes Linux se autentiquen con el controlador de dominio Windows, obteniendo la administración centralizada de los usuarios.
Cabe mencionar que SSSD es escogida como alternativa ideal por ser relativamente nueva y de menor complejidad pero de igual adaptabilidad que Winbind limitada únicamente por el uso del protocolo LDAP, que a diferencia de Winbind no posee compatibilidad con protocolos anteriores de acceso a directorios.

Palabras Claves: *Autenticación, Controlador de dominio, Cuenta de usuario, Directorio Activo, Kerberos, LDAP, SSSD, Winbind.*

Abstract

This project solve the problem in the authentication service users, by the presence of hybrid environments in companies, allowing two alternative authentication service integration between the Linux and Windows platforms are raised, using the Windows operating system domain controller, so servants were employed and virtual workstations on both platforms for running the tests, being used in the Windows environment Windows 8 work station and server Windows Server 2012 R2 and the Linux environment work station Ubuntu 14.04 and as CentOS 7.0 server.
Integration methods that were used in this project were System Security Services Daemon (SSSD) and Winbind, which involve protocols Lightweight Directory Access Protocol (LDAP) and Kerberos. Both methods allow Linux clients to authenticate with the Windows domain controller, obtaining centralized management of users.
It should be mentioned that SSSD is chosen as the ideal alternative for being relatively new and less complex but equally adaptability Winbind limited only by using the LDAP protocol, which unlike Winbind does not have backward compatibility directory access protocol.

Keywords*: Authentication, Domain Controller, User Account, Active Directory, Kerberos, LDAP, SSSD, Winbind.*

1. Introducción

El sistema operativo es un conjunto de procesos que se ejecutan en el computador permitiendo el funcionamiento de programas, el cual con el pasar de los años ha tenido avances y mejoras significativas, que han permitido que la información en empresas o usuarios finales se maneje de manera didáctica, segura y pueda ser almacenada en uno o varios puntos con el objetivo de compartir información.

Cabe mencionar que el sistema operativo de mayor acogida en el mercado para clientes y usuario finales es Windows, sin embargo posee un fuerte

contrincante los sistemas operativos Linux, ambos sistemas pueden estar presentes en una empresa por múltiples razones dando lugar a un ambiente híbrido, lo que sin duda soluciona problemas individuales pero provoca una compleja administración como por ejemplo el servicio de autenticación de los usuarios en la red.

Cada familia Linux y Windows administra sus sistemas de manera independiente, en otras palabras no existe una mezcla directa de sistemas Linux y Windows aunque teóricamente manejan los mismos protocolos, por lo cual en el presente proyecto se explica al lector en detalle los programas adicionales a utilizar para integrar el servicio de autenticación de ambos sistemas logrando centralizar la administración de los usuarios.

2. Descripción

En la actualidad, es frecuente la existencia de plataformas híbridas en las organizaciones, ya sea por motivos económicos, requerimientos específicos o inclusive preferencia por un determinado sistema.

Debido a ello, el proyecto se lleva a cabo con las plataformas más utilizadas en el mercado empresarial, Linux y Windows, porque Windows al poseer una interfaz intuitiva para el usuario se convierte en un sistema de configuración elemental y de mayor uso en el mercado, con lo cual se le atribuye un número considerable de aplicaciones compatibles, a su vez Linux es reconocido por su confiabilidad y robustez, además que es un sistema de código abierto, con lo cual la empresa no invierte en licenciamiento.

Pero independientemente de la infraestructura tecnológica a manejar dentro de una red corporativa, sea ésta Linux o Windows, el personal de tecnología de información (TI) tiene como prioridad asegurar un servicio de alta disponibilidad, calidad y productividad para la compañía.

3. Antecedentes

Siempre han existido inconvenientes relacionados en la administración de las cuentas de los usuarios, como por ejemplo: la información de la cuenta de un usuario está almacenada en la base de datos del sistema operativo donde fue creado, en este caso un servidor Windows, el usuario puede acceder al sistema libremente y sin inconvenientes, no obstante al necesitar acceso a los servidores o estaciones de trabajo Linux, este requerimiento no podrá llevarse cabo ya que el servidor Linux no posee información sobre la cuenta del usuario, es por ello que el administrador de la red se verá obligado a crear una nueva cuenta de usuario, usada únicamente para realizar esta función, cabe recalcar que esta tarea puede llevarse a cabo con múltiples usuarios, lo que involucra un considerable esfuerzo administrativo.

4. Objetivos

Objetivo General

Analizar, diseñar e implementar una solución de autenticación para la integración de plataformas Linux y Windows con la finalidad de centralizar la gestión de los usuarios en un ambiente empresarial, integrado por el Directorio Activo de Windows.

Objetivos Específicos

• Analizar el servicio de autenticación de los sistemas operativos Linux y Windows.
• Analizar el presupuesto de la solución.
• Diseñar e implementar una solución de autenticación para la unificación de plataformas híbridas.
• Ofrecer una solución asequible y de corto tiempo para facilitar a las empresas una adecuada administración de sus usuarios.

5. Metodología

En el proyecto se utilizó la metodología cascada, ésta técnica es un proceso secuencial de actividades, las cuales fueron desarrolladas de la siguiente manera:
1. Investigar la solución de la problemática: En este pasó se realizó una investigación sobre los métodos de autenticación de los usuarios dentro de un ambiente de dominio entre las plataformas Linux y Windows, así también como los protocolos involucrados.
2. Analizar los requerimientos de la implementación: Se selecciona el software virtualizador y los sistemas operativos Linux y Windows a utilizar.
3. Crear el diseño de la implementación: Se lleva cabo el diseño lógico de la solución propuesta y la investigación de las configuraciones pertinentes.
4. Implementar la solución: Se ejecutan las alternativas de solución de acuerdo a las configuraciones específicas para las distintas plataformas.
5. Realizar pruebas: En este último paso se elaboran diversas pruebas para evaluar la implementación realizada, así también se establecen las ventajas, desventajas y limitaciones de acuerdo a los resultado obtenidos para la elaboración de las conclusiones.
En la Figura 1 se puede visualizar de manera gráfica la metodología utilizada en el proyecto.

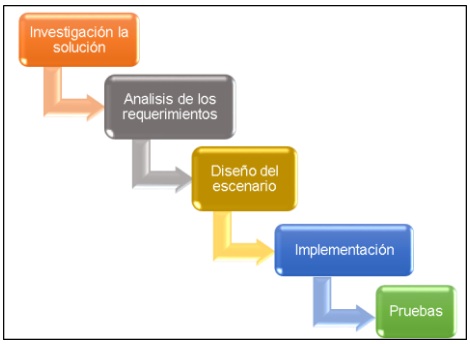

Figura 1. Metodología Cascada

6. Integración de plataformas en el Ecuador

En el Ecuador, las organizaciones con plataformas heterogéneas han ido en aumento por la emisión del decreto 1014, que establece en las empresas de Administración Pública la utilización de software libre en sus sistemas y equipamientos informáticos [1], por ello las compañías han llevado a cabo la incorporación y migración a software no licenciado, sin embargo el arraigado conocimiento de los sistemas Windows y la poca noción de la plataforma Linux, ha producido conflictos sobre la autenticación para los administradores o jefes del departamento de informática e inclusive a los propios trabajadores de la empresa.

7. Servicio de autenticación

La autenticación es un proceso en el cual se identifica a un usuario o servicio de acuerdo a ciertos criterios [2], por lo que un mecanismo de autenticación es un servicio del sistema que facilita la identificación de algo o alguien, mediante el conocimiento de cierta información o posesión de un objeto que permita verificar su identidad. Al igual que los servicios de directorios los servicios de autenticación manejan sus propios protocolos, como es el caso del protocolo Kerberos que será utilizado en la implementación del proyecto por ser compatible con ambas plataformas.

Kerberos es un protocolo de elección para entornos de red multi-plataforma, utiliza criptografía de claves simétricas brindando seguridad al momento de validar los usuarios con los servicios de la red esto se lo realiza con el fin de evitar enviar las contraseñas a través de la red. [3]

Para la autenticación del servidor principal en Windows server con los clientes Windows se utiliza la autenticación kerberos versión 5, el cual emite tickets para tener acceso a la red, estos tickets contienen información cifrada para confirmar la identidad del usuario.

8. Tipos de Integración

Se entiende a la integración en informática como un proceso cuyo objetivo es unir los datos contenidos en diferentes subsistemas para convertirlo en uno sistema más extenso, permitiendo un método rápido y sencillo para compartir datos cada vez que fuera necesario [4]. No obstante el concepto es enfocado al servicio de autenticación de las plataformas, con lo cual se unifica la autenticación de los usuarios mediante el nombre de usuario y contraseña alojados en un directorio principal.
La integración se puede realizar de dos maneras:

- Directa
- Indirecta

La integración directa como se puede observar en la Figura 2, facilita que los sistemas Linux interactúen directamente con el Directorio Activo de Windows sin ningún tipo de equipo intermediario [5]

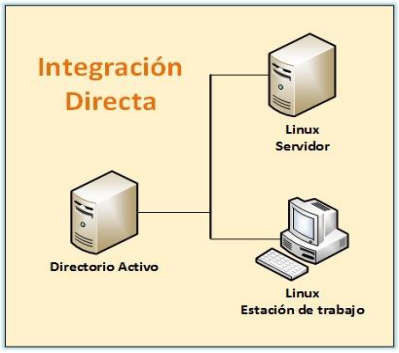

Figura 2. Integración Directa

A su vez, mediante la integración indirecta como se visualiza en la Figura 3, los sistemas Linux deben de interactuar con un equipo intermediario que trabaja de identificador central y éste a su vez se comunica con el Directorio Activo de Windows. [5]

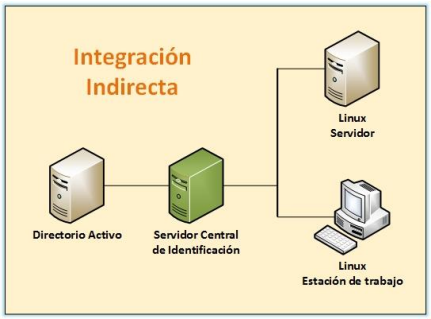

Figura 3. Integración Indirecta

9. Métodos de autenticación de multiplataforma

La unificación de las plataformas en un ambiente empresarial ha ido en crecimiento, ya sea por las restricciones a datos e información privilegiada o por el control de cuentas de usuarios, pero debido a la incompatibilidad de las principales plataformas, se han desarrollado diversas alternativas para cumplir con dicha función, las cuales dependen del tipo de integración a realizar, alcance u otros. Ya que se decidió utilizar la integración directa se escogió dos mecanismos para realizar dicha autenticación, los cuales son: Winbind y SSSD.

9.1 SSSD

System Security Services Daemon es un conjunto de demonios que permiten la administración de directorios y mecanismos de autenticación, proporcionando una interfaz NSS y PAM. [6]. Es un intermediario entre los clientes locales y el servidor principal, que realiza la gestión de controlar el dominio, es decir proporciona el acceso a varios proveedores de identidad y autenticación. [7]

SSSD, es independiente de las aplicaciones, ya que trabaja con un robusto almacenamiento de caché local que pertenece a la identidad de un grupo o de un usuario. La ventaja de esta solución es que almacena las credenciales en el equipo local, en otras palabras permite trabajar desconectado de la red [8] [9], sin embargo no es compatible con el protocolo NTLM. En la Figura 4 se muestra de manera sencilla el esquema de funcionamiento de SSSD y la presencia de los protocolos LDAP y kerberos.

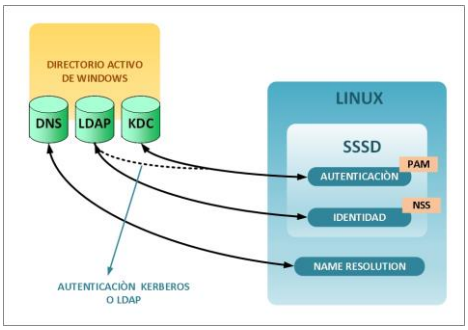

Figura 4. Esquema SSSD

9.2 Winbind

Es un componente de la suite samba que permite inicio sesión unificado, extrayendo información de identidad de un usuario, como el nombre usuario y su respectiva contraseña del Directorio Activo de Windows logrando que actúe como un miembro del dominio [10]. Winbind trabaja con el módulo PAM y el servicio de nombres NSS, lo que le permite realizar tres funciones separadas: autenticar las credenciales de usuarios, nombre de usuario y contraseña a través PAM, facilitar la resolución de identidad mediante NSS, es decir que permite adquirir información del nombre del host o del usuario, y también mantener una base de datos llamada winbind_idmap.tdb, en donde se registran las identificaciones entre ambas plataformas.

Cabe aclarar que Winbind resuelve el problema de sincronizar contraseñas entre distintos sistemas, ya que toda la información relacionada a las contraseñas se guarda en un solo punto, en el controlador de dominio Windows. [11]. En la Figura 5 se observa el funcionamiento del esquema de Winbind trabajando como intermediario y relacionándose con LDAP y kerberos.

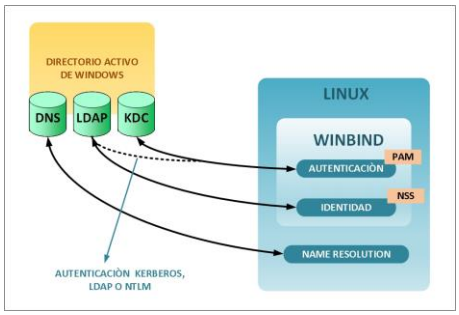

Figura 5. Figura ejemplo

10. Diseño del esquema lógico de la red

En la Figura 6 se muestra el diseño propuesto para la resolución de la problemática, en el cual "Proyecto.com" es el nombre de dominio de la empresa, las estaciones de trabajo Windows y los servidores y estaciones de trabajo Linux se autentican con el Directorio Activo de Windows, el cual es el contenedor de las cuentas de los usuarios de la organización.

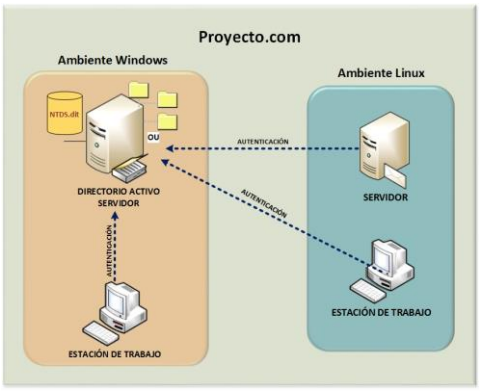

Figura 6. Esquema lógico de la red

11. Configuración

Se ejecuta la instalación de los paquetes de samba o sssd adecuados, e inmediatamente se edita el archivo de configuración principal en ambos escenarios, smb.conf en el caso de utilizar Winbind y sssd.conf en caso de implementar SSSD, cabe mencionar que dependiendo del escenario varían el nombre y cantidad de archivos. Ambas configuraciones deben indica el nombre del dominio, nombre de la máquina que alberga al Directorio Activo, nombre del grupo de trabajo e inclusive los usuarios o grupos que pueden tener acceso al sistema, no olvidar reiniciar el servicio.

Se edita el archivo nsswitch.conf, que determina el orden de búsqueda de las bases de datos del sistema en el cual se debe indicar la utilización de los archivos de Winbind o SSSD dependiendo de la implementación. Se solicita un boleto al servidor Kerberos mediante el comando kinit, y en el caso de Winbind se finaliza con la unión del equipo al dominio Windows.

11.1 SSSD

Configuración SSSD en el servidor CentOS y en la estación de trabajo de Ubuntu:

1. Instalación de paquetes SSSD pertinentes:

Centos: yum -y install realmd sssd oddjob-mkhomedir samba-common adcli

Ubuntu: sudo apt-get install realmd sssd sssd-tools samba-common samba-libs adcli

2. Descubrir el dominio del Directorio Activo mediante realm, el configurará al equipo como cliente SSSD de manera automática.

realm discover serverad.proyecto.com

3. Solicitar el boleto al servidor kerberos:

#kinit Administrator@proyecto.com

4. Unirse al dominio del Directorio Activo

realm join proyecto.com

5. Editar archivo de configuración sssd.conf, para que permita el ingreso por el nombre de usuario, este paso es opcional:

use_fully_qualified_names = False

6. Reiniciar el servicio sssd.

CentOS: systemctl restart sssd

Ubuntu: sudo service sssd restart

7. Comprobar el funcionamiento

id mperalta #usuario del dominio

11.2 Winbind

Configuración Winbind en el servidor CentOS y estación de trabajo Ubuntu:

1. Como primer paso, instalar todos los paquetes relacionados con Winbind:

Centos: yum -y samba-common samba-winbind samba-winbind-clients

Ubuntu: sudo apt-get install winbind samba libpam-winbind libnss-winbind

2. Editar el archivo de configuración smb.conf en la ruta /etc/samba, en este archivo se indican el grupo de trabajo que en este caso es el nombre del dominio, así también como el nombre de la máquina que contiene el Directorio Activo e indicar el tipo de seguridad a usar, que debe ser ads que es la seguridad del Directorio Activo, quedando de la siguiente manera:

```
[global]
  workgroup = PROYECTO
  password server = serverad.proyecto.com
  realm = PROYECTO.COM
  security = ads
  template shell = /bin/bash
  winbind use default domain = false
  winbind offline login = false
```

3. Se Inicia los servicios de samba y winbind, ejecutando:

```
# smbd restart
# nmbd restart
# winbindd restart
```

4. Agregar y modificar archivo de configuración /etc/nsswitch.conf, quedando de la siguiente manera:

```
#nano /etc/nsswitch.conf
passwd: files winbind
shadow: files winbind
group: files winbind
```

5. Se debe solicitar boleto al servidor Kerberos, proporcionando las credenciales de usuario administrador del controlador de dominio:

#kinit Administrator@proyecto.com

6. Para confirmar que la obtención del ticket es exitoso se escribe:

#klist

7. Se agrega la máquina al dominio ejecutando los comandos:

```
#net ads join proyecto.com -U administrator
Enter administrator's password:
Using short domain name -- PROYECTO
Joined 'Centos-Winbind' to realm 'proyecto.com'
```

12. Prueba de funcionalidad

Para verificar el funcionamiento de la implementación en ambos escenarios, se realizaron cuatro pruebas:

1. Inicio de sesión por primera vez.
2. Inicio de sesión posterior al cambio de contraseña.
3. Inicio de sesión de acuerdo a permisos restringidos.
4. Permisos de administrador

Es decir tanto en el escenario de SSSD así como en el escenario de Winbind, se creó varios usuarios en el Directorio Activo de Windows separados en tres grupos de pruebas distribuidos equitativamente, simulando los departamentos de una empresa, la cantidad de usuarios se obtuvo del cálculo mínimo de observaciones, dichos usuarios se autenticaron en la estación de trabajo Windows 8, en el servidor de CentOS y en la estación de trabajo de Ubuntu de cada escenario.

En ambos escenarios los equipos Linux fueron configurados para que creen de manera automática un directorio de usuario la primera vez que éste se autentica, dicha función viene habilitada de manera predeterminada en la estación de trabajo Windows.

Posterior a la autenticación, en el Directorio Activo de Windows se cambió la contraseña de los usuarios y se procedió a realizar una nueva autenticación en todos los equipos y en ambos escenarios, la cual se efectuó sin ningún inconveniente.

Como tercera prueba se realizó un procedimiento en la que el Directorio Activo de Windows restringió el acceso de los usuarios del domino a los equipos Windows a través de grupos acorde a departamentos o funciones, y como prueba final se le otorgó privilegios de Administrador a ciertos grupos, cabe mencionar que en ambas pruebas los equipos Linux fueron configurados de manera diferente e independiente para que realicen la misma función, definiendo un único o varios grupos de usuario que pueden acceder a ciertos equipos y otorgando privilegios a ciertos usuarios para que puedan cambiar la configuración de cada uno de los dispositivos Linux, los resultados de las pruebas se los puede visualizar en la tabla 1.

Tabla 1. Pruebas

Pruebas	Escenarios		
	Windows	SSSD	Winbind
Primer inicio de sesión	Éxito	Éxito	Éxito
Cambio de contraseña	Éxito	Éxito	Éxito
Acceso restringido	Éxito	Éxito	Éxito
Permiso de administrador	Éxito	Éxito	Éxito

13. Análisis de Costos

El costo del proyecto se basa únicamente en el servicio de configuración necesaria para la implementación, el cual es proporcional al número de servidores involucrados en el proyecto, número de usuarios de la empresa y el precio medio utilizado por los competidores directos en el mercado. Para obtener dicho valor se llevó a cabo una serie de cotizaciones a empresas que ofertan servicios similares como se visualiza en la tabla 2.

Tabla 2. Cotización a empresas

Empresa	Valor del servicio
Servicom	**$300.00+iva**
Serconnet	**$900.00+iva**
Pc Ecuador	**$750,00 +iva**
Jsgm Easy – Tec	**$585,00+iva**
64bits	**$500.00+iva**
Sync	**$600.00+iva**
Palosanto	**$750.00+iva**
Dinamoconsulting	**$820.00+iva**
It Soluciones Ecuador	**$400.00+iva**
Its Ecuador	**$600.00+iva**
E-open Solutions Ltda.	**$540.00+iva**
Ecualinux NodoVIP	**$580.00+iva**
Innova services	**$720.00+iva**
Troncal net	**$790.00+iva**

Se cotizó en base a los escenarios de las implementaciones, compuesto por dos servidores principales, un servidor Windows y otro servidor Linux y un aproximado de 75 usuarios, cuyo requerimiento principal es la integración de estas plataformas.Se elabora una tabla de barras visible en la figura 7 cuyo valor promedio se considera como un valor ideal para ofertar en la solución de la problemática, el cual es obtenido realizando la sumatoria de todos los valores que ofrecen las distintas empresas, dividido para el número de empresas que se contactó para el análisis de la cotización, siendo aproximadamente $570+IVA el costo del servicio, incluyendo transporte de los técnicos y otros.

Sin embargo este valor puede varía por la cantidad de servidores o estaciones de trabajo a configurar y el tiempo requerido para dicho proyecto, para lo cual se elabora un plan de trabajo.

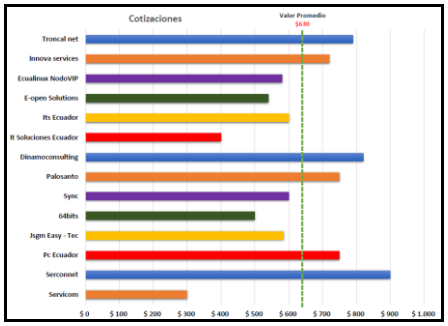

Figura 7. Valor del proyecto por empresa

14. Plan de trabajo

En el plan de trabajo se indican las actividades a realizar en el proyecto, así como el tiempo ideal para su ejecución, lo cual se muestra en la tabla 2 y la Figura 8.

Tabla 2. Plan de trabajo

Id	Nombre de la tarea	Duración	Comienzo	Fin
1	**Análisis de la empresa**	**2 días**	**Lun 12/10/15**	**Mar 13/10/15**
2	Análisis de los servicios y estaciones de trabajo	2 días	Lun 12/10/15	Mar 13/10/15
3	**Inicio propuesta de servicio**	**3 días**	**Mie 14/10/15**	**Vie 16/10/15**
4	Reunión con los gerentes y técnicos de la empresa para acordar costos, fechas y métodos para la solución	2 días	Mie 14/10/15	Jue 15/10/15
5	Pago del 70% de cotización para inicio del proyecto	1 día	Vie 16/10/15	Vie 16/10/15
6	**Implementación y Configuración**	**9 días**	**Lun 19/10/15**	**Jue 29/10/15**
7	Implementación de solución en el servidor DC (Controlador de Dominio)	2 días	Lun 19/10/15	Mar 20/10/15
8	Implementación de solución en los servidores Linux	3 días	Mie 21/10/15	Vie 24/10/15
9	Implementación de solución en las estaciones de trabajo Windows	3 días	Lun 26/10/15	Mie 28/10/15
10	Análisis de pruebas de la implementación	1 día	Jue 29/10/15	Jue 29/10/15
11	**Finalización Propuesta de servicio**	**1 día**	**Vie 30/10/15**	**Vie 30/10/15**
12	Pago del 30% restante	1 días	Vie 30/10/15	Vie 30/10/15

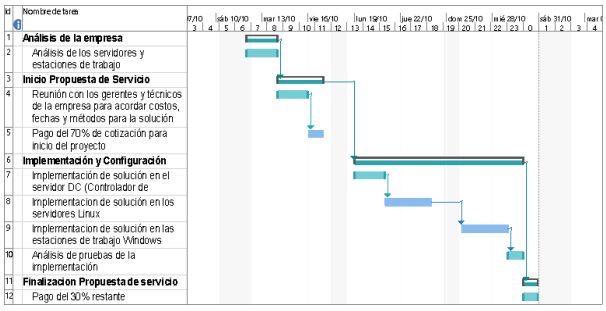

Figura 8. Diagrama de Grantt

Conclusiones

La mayoría de fallas en la seguridad informática a menudo están relacionadas con el acceso de los usuarios al sistema, por lo que la solución propuesta beneficia al control de la autenticación de los clientes. Se logra minimizar la cantidad de errores por medio de la ejecución del demonio realmd, que facilita la configuración de las alternativas SSSD o Winbind. La implementación de la solución SSSD a pesar de ser relativamente nueva permite tener una menor cantidad de archivos de configuración y un menor tiempo de ejecución, además de poseer mayor flexibilidad en comparación con Winbind.

Agradecimientos

Se agradece en primer lugar al Ing. Jorge Magallanes, ya que él fue quien otorgo el tema, un agradecimiento especial al Ing. Fernando Ortiz, porque aporto con información para realizar este proyecto.

Referencias

[1] Correa Delgado Rafael. (2008, Abril) Uso de estándares abiertos y software libre [Online]. Disponible en: http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2014/06/DecretoEjecutivo1014.pdf

[2] Oracle (2011, Mayo) Servicios de autenticación. [Online]. Disponible en: http://docs.oracle.com/cd/E24842_01/html/E23286/secov-5.html

[3] Ghudson (2015, Julio). Kerberos: The Network Authentication Protocol. [Online]. Disponible en: http://web.mit.edu/kerberos/

[4] Pal Dmitri, (2015, Enero). Aspect of Integration, [Online].Disponible en: http://rhelblog.redhat.com/2015/01/28/aspects-of-integration/

[5] Pal Dmitri, (2015, Mayo) Direct, or Indirect, that is the question. [Online]. Disponible en: http://rhelblog.redhat.com/2015/05/27/direct-or-indirect-that-is-the-question/

[6] Linuxman page, (2013, Mayo).SSSD, [Online]. Disponible en: http://linux.die.net/man/8/sssd

[7] Fedoram (2010, Mayo) Features/SSSD [Online]. Disponible en: https://fedoraproject.org/wiki/Features/SSSD

[8] Desde Linux (2013, Agosto). Red SWL (IV): Ubuntu Precise y clearos, Autenticación SSSD contra LDAP nativo, [Online]. Disponible en: http://blog.desdelinux.net/red-swl-iv-ubuntu-precise-y-clearos-autenticacion-sssd-contra-ldap-nativo/

[9] RedHat, Guía de Planificación de Migración - SSSD, edición 6, 2010.

[10] Potter Tim, (2011, Junio). Manual de referencia, capítulo 21. Winbind: Uso de cuentas de Dominio, [Online]. Disponible en: http://www.bdat.net/documentos/samba/html/winbind.html