

INSTITUTO UNIVERSITARIO AERONÁUTICO



TRABAJO FINAL DE POSGRADO

CARRERA:
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

***HARDENING DE SEGURIDAD DE GESTOR
DOCUMENTAL ALFRESCO***



ALUMNO:
CARLOS IGNACIO TAPIA - D.N.I. 28.657.987
TUTOR: M.Cs. ING. EDUARDO CASANOVAS

DICIEMBRE 2014



HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción	Autor
04/10/2013	1.0	Documento inicial del Trabajo Final de Posgrado	Carlos Tapia
14/10/2013	1.1	Agregado de bibliografías de consulta	Carlos Tapia
15/10/2013	1.2	Agregado de marco teórico para el proyecto	Carlos Tapia
30/10/2013	2.0	Agregado de narrativas y gráficos de los procesos relevados	Carlos Tapia
10/11/2013	3.0	Armado de línea de tiempo del proceso de tesis genérico	Carlos Tapia
17/11/2013	4.0	Control general de redacción, paginación, índice	Carlos Tapia
23/02/2014	5.0	Comparación de gestores documentales	Carlos Tapia
01/03/2014	6.0	Diseño de flujo de trabajo en Alfresco	Carlos Tapia
10/05/2014	7.0	Descripción del hardware a utilizar	Carlos Tapia
01/09/2014	8.0	Armado de glosario	Carlos Tapia
10/09/2014	9.0	Ajustes en referencias bibliográficas	Carlos Tapia
20/09/2014	10.0	Sección de demostración de uso	Carlos Tapia
21/09/2014	11.0	Sección implementación de la solución	Carlos Tapia
21/09/2014	12.0	Apartado de mejoras a futuro	Carlos Tapia
07/10/2014	13.0	Incorporación de anexo de instalación de Alfresco y workflows	Carlos Tapia
10/10/2014	14.0	Ajustes finales en referencias y bibliografía	Carlos Tapia
14/11/2014	15.0	Incorporación de anexo de configuración de virtual machines	Carlos Tapia
12/11/2014	16.0	Mejoras en las conclusiones y trabajos futuros	Carlos Tapia
02/12/2014	17.0	Correcciones en indización, anexos	Carlos Tapia
05/12/2014	18.0	Modificaciones en referencias bibliográficas y títulos de tablas y figuras. Cambios en redacciones en general.	Carlos Tapia



ÍNDICE TEMÁTICO

01. Introducción	3
02. Objetivos y alcance del trabajo	6
02.01. Situación Problemática	6
02.02. Objeto de Estudio	6
02.03. Objetivos	6
02.03.1. Objetivo general	7
02.03.2. Objetivos específicos	7
02.04. Delimitación del proyecto	7
03. Marco Teórico	8
03.01. Propiedades de Seguridad que se buscan	14
04. Alternativas a Sistemas de Gestión Documental	15
04.01. Alfresco	15
04.02. Nuxeo	15
04.03. Comparativa de Gestores Documentales Open-Source	17
05. Detalles del software a utilizar	18
06. Hardware a utilizar	22
07. Descripción del proceso a abordar con el Gestor Documental	23
08. Implementación de la solución	27
09. Demostración de uso	29
10. Conclusión	39
11. Trabajos Futuros	40
12. Referencias bibliográficas	41
13. Glosario	42
Anexos	44
Anexo I: Detalles de instalación y configuración de Alfresco	44
Anexo II: Diseño de workflows en Alfresco	53





ÍNDICE DE FIGURAS

Figura N° 01 - Arquitectura inicial de componentes de Alfresco	10
Figura N° 02 - Arquitectura simplificada de implementación Alfresco	18
Figura N° 03 – Medidas de hardening de Alfresco	19
Figura N° 04 - Proceso a abordar - parte 1	23
Figura N° 05 - Proceso a abordar - parte 2	24
Figura N° 06 - Proceso a abordar - parte 3	25
Figura N° 07 - Flujo de información de anteproyecto de tesis	26
Figura N° 08 – Despliegue de máquinas virtuales a utilizar	27
Figura N° 09 - Acceso de tutor a interfaz web de Alfresco	29
Figura N° 10 - Flujo de aprobación en Alfresco	30
Figura N° 11 - Inicio del flujo de aprobación en Alfresco	31
Figura N° 12 - Prueba de datos en el flujo de aprobación en Alfresco	31
Figura N° 13 - Firma Digital dentro del flujo de aprobación en Alfresco	32
Figura N° 14 - Documento firmado en Alfresco	32
Figura N° 15 - Acceso de Secretaría de Alumnos en Alfresco	33
Figura N° 16 - Acceso de Secretaría de Alumnos en Alfresco	33
Figura N° 17 - Tareas activas en el flujo de trabajo en Alfresco	34
Figura N° 18 - Tareas completadas en el flujo de trabajo en Alfresco	34
Figura N° 19 - Pantalla de resumen del flujo de trabajo en Alfresco	35
Figura N° 20 - Listado de documentos firmados en el flujo de Alfresco	36
Figura N° 21 - Recibo de firma auto-generado en Alfresco al firmar	37
Figura N° 22 - Corroboración de la Firma Digital en el documento	38
Figura N° 23 – Pantalla inicial de intalación de CentOS 6	44
Figura N° 24 – Selección de idioma en la instalación de CentOS 6	45
Figura N° 25 – Elección del hostname para la máquina	46
Figura N° 26 – Elección del huso horario	46
Figura N° 27 – Selección del tipo de instalación	47
Figura N° 28 – Comando de instalación de Alfresco	47
Figura N° 29 – Lenguaje de instalación de Alfresco	47
Figura N° 30 – Pantalla de bienvenida de instalación de Alfresco	47
Figura N° 31 – Elección del tipo de instalación de Alfresco	48
Figura N° 32 – Selección de componentes a instalar en Alfresco	48
Figura N° 33 – Elección del directorio de instalación para Alfresco	49
Figura N° 34 – Configuración de Tomcat	49



<i>Figura N° 35 – Confirmación de la instalación finalizada</i>	49
<i>Figura N° 36 – Diagrama de flujo en Eclipse</i>	54

ÍNDICE DE TABLAS

<i>Tabla N° 01 - Comparación de gestores documentales</i>	17
---	----



01. INTRODUCCIÓN

El presente trabajo se concibió como parte complementaria del Trabajo Final de la Especialización del Ing. Fernando Boiero ("**Aplicación de Firma Electrónica a Procesos del IUA**"), de modo tal que este trabajo cubra la implementación de un Gestor Documental con seguridad reforzada, mientras que el trabajo del Ing. Boiero abarque la implementación de una infraestructura PKI con la cual llevar adelante la gestión de certificados digitales, confluyendo ambos trabajos en la implementación de un flujo de información referido a firma digital sobre el Gestor Documental Alfresco en su versión Community.

El mencionado Gestor está desarrollado en JSP y se implementa en un servidor de Aplicaciones Apache Tomcat. El mismo implementa las especificaciones de los servlets y de JavaServer Pages (JSP) de Sun Microsystems y se busca aprovechar el hecho de que Tomcat es un servidor web con soporte de servlets y JSPs.

Apache Tomcat cuenta con un impresionante historial en lo que respecta a la seguridad. De acuerdo con los Apache Tomcat Wiki páginas oficiales, nunca ha habido un caso reportado de un perjuicio real, o pérdida de datos importantes debido a un ataque malintencionado en cualquier instancia de Apache Tomcat. Las vulnerabilidades, tanto mayores como menores, son descubiertas por la comunidad Tomcat misma o los investigadores de seguridad, de manera colaborativa, y posteriormente se lanzan los parches necesarios rápidamente para subsanar las potenciales brechas de seguridad. Por lo tanto, la instalación por defecto de Tomcat puede decirse que es "bastante segura".

Partiendo de esta base, también es importante recalcar que existen medidas adicionales que se pueden tomar para hacer Tomcat lo más seguro posible para hacer frente a potenciales ataques. Como suele suceder con los análisis de seguridad, el nivel de exigencia que se le aplique a Tomcat es una cuestión de equilibrio de facilidad de uso y restricciones de acceso. Por ejemplo, si bien la instalación automatizada es sencilla, rápida y permite al administrador realizar otras tareas mientras se completa, desde el punto de vista de seguridad es más conveniente efectuar una instalación paso a paso, documentando cada parámetro de



seguridad y estableciendo las opciones o valores más exigentes para obtener como output un Gestor Documental recién instalado y con seguridad reforzada.

De esta manera, lograremos tener un Gestor Documental “seguro” y se podrá complementar con la implementación de una Infraestructura de Clave Pública o Public Key Infrastructure (PKI) que proporcione el software, hardware, políticas y mecanismos de seguridad necesarios que permiten garantizar la ejecución de operaciones criptográficas como el cifrado, la Firma Digital o el no repudio de operaciones electrónicas.

La conjunción de los trabajos finales (el presente más el llevado adelante por el Ing. Boiero) brindará confianza a la comunicación de procesos de negocio del Instituto Universitario Aeronáutico (IUA), como así también servirá para ganar en seguridad y trazabilidad en los procesos de negocio.

A continuación, se reseña brevemente el contenido de los capítulos que integran el trabajo:

- Capítulo 02 - Objetivos y alcance del trabajo: se describen los objetivos generales y específicos, como así también la delimitación del trabajo.
- Capítulo 03 - Marco Teórico: se brindan detalles de las funciones de un Gestor Documental y de su hardening de seguridad.
- Capítulo 04 - Alternativas a Sistemas de Gestión Documental: se plantea la investigación de distintas soluciones de Gestión Documental.
- Capítulo 05 - Detalles del software a utilizar: se determina la combinación de software a utilizar para brindar una solución Gestión Documental segura.
- Capítulo 06 - Hardware a utilizar: se menciona el equipamiento y recursos a utilizar para implementar la solución.
- Capítulo 07 - Descripción del proceso a abordar con el Gestor Documental: se explica el proceso de negocio a abordar para aplicar la solución propuesta.
- Capítulo 08 - Implementación de la solución: se detallan los procedimientos de implementación de la solución.
- Capítulo 09 - Demostración de uso: se muestra la solución aplicada a un caso de uso.
- Capítulo 10 - Conclusión: se entregan las conclusiones del trabajo.



- Capítulo 11 - Trabajos Futuros: se plantean futuras líneas de investigación para continuar este trabajo.
- Capítulo 12 - Referencias bibliográficas: se vincula este trabajo con las fuentes de información utilizadas para consulta.
- Capítulo 13 - Glosario: se definen conceptos para facilitar la lectura del documento.



02. OBJETIVOS Y ALCANCE DEL TRABAJO

02.01. SITUACIÓN PROBLEMÁTICA

En la actualidad, no son pocas las organizaciones que eligen gestores documentales para almacenar y gestionar los documentos que sustentan sus procesos de negocios. Este trabajo plantea la posibilidad de implementar dentro de la red el IUA un gestor documental que permita la correcta y formal documentación de los procesos a partir de un gestor documental que no sólo almacene los archivos si no también que permita armar flujos de trabajo y que además brinde seguridad adecuado para la documentación almacenada.

02.02. OBJETO DE ESTUDIO

En el presente Trabajo Final se analizará el concepto, aplicación práctica y beneficios de la instalación de un Gestor Documental con seguridad reforzada, cómo éste puede ayudar a la trazabilidad de los procesos y su formalización, agregando a la vez, propiedades de Seguridad Informática en las comunicaciones internas.

De esta manera, se mostrará la posibilidad de sistematizar los procesos internos del IUA, es decir, canalizar las comunicaciones entre las distintas áreas del IUA de manera formal y permitiendo trazabilidad y la obtención de métricas para la mejora continua de la gestión.

02.03. OBJETIVOS

A continuación se detallan los objetivos del proyecto, describiendo brevemente los resultados esperados a su conclusión.



02.03.1. OBJETIVO GENERAL

Implementar un gestor documental de código abierto con seguridad reforzada y mostrar los beneficios de seguridad y trazabilidad en la gestión de los procesos internos del IUA.

02.03.2. OBJETIVOS ESPECÍFICOS

- Instalar un gestor documental para formalizar flujos de información.
- Mostrar las ganancias de seguridad y trazabilidad de la solución a implementar.
- Lograr tener el Gestor Documental con propiedades de estabilidad y escalabilidad.
- Utilizar en todos los casos herramientas open-source para asegurar su mantenimiento a futuro.

02.04. DELIMITACIÓN DEL PROYECTO

El presente trabajo se circunscribe al proceso de gestión de ante-proyectos de trabajos finales aplicable tanto a los títulos de Grado como de Pre-Grado.

Como se define en el Apartado 11, se buscará a futuro implementar mejoras y aplicar el objeto de este trabajo a otros procesos internos del Instituto.

Asimismo, para delimitar este trabajo se definirá la arquitectura tomando las notas de instalación de Alfresco y sus recomendaciones de despliegue, por lo cual se tomará como base un Sistema Operativo GNU/Linux de 64bits y como Base de Datos PostgreSQL 9.0.4, Servidor de Aplicaciones Tomcat 7.0.30 y en relación al kit de desarrollo, se utilizará Java 1.7.0 u7. Estos componentes vienen incluidos en el paquete de instalación Community en su release actual 4.2.



03. MARCO TEÓRICO

Para comenzar a explicar el marco teórico, se define a continuación qué se entiende por Gestión Documental, Sistema de Gestión Documental y posteriormente se brinda un concepto de hardening de seguridad para aunar estas definiciones y considerar sus implicancias en conjunto.

De acuerdo a Wikipedia, por "Gestión Documental" se entiende el "conjunto de normas técnicas y prácticas usadas para administrar el flujo de documentos de todo tipo en una organización, permitir la recuperación de información desde ellos, determinar el tiempo que los documentos deben guardarse, eliminar los que ya no sirven y asegurar la conservación indefinida de los documentos más valiosos, aplicando principios de racionalización y economía". La definición entregada no tiene en sí implicancias de Tecnología de Información, es por ello que, paso seguido, se analizará el concepto de "Software de Gestión Documental".

También tomando como definición universal aquella proporcionada por Wikipedia, un Sistema de Gestión Documental (en inglés, Document Management System) "son todos aquellos programas de ordenador creados para la gestión de grandes cantidades de documentos, suele rastrear y almacenar documentos electrónicos o imágenes de documentos en papel. Estos documentos no tienen una organización clara de sus contenidos, al contrario de lo que suele suceder con la información almacenada en una base de datos. La combinación de este tipo de bibliotecas de documentos con índices almacenados en una base de datos permite el acceso rápido mediante diversos métodos a la información contenida en los documentos. Estos generalmente se encuentran comprimidos y además de texto pueden contener cualquier otro tipo de documentos multimedia como imágenes o vídeos. Los sistemas de gestión de documentos comúnmente proporcionan medios de almacenamiento, seguridad, así como capacidades de recuperación e indexación". En este último concepto, si bien aparecen fuertemente las implicancias de Tecnología de Información, es apenas insipiente la preocupación por Seguridad Informática. Para incorporar este último concepto, nuevamente nos valemos de Wikipedia, en esta oportunidad mediante la definición de "Hardening (Computing)", que traducida al español indica: "En computación, hardening se denomina usualmente al proceso de reforzar la seguridad de un sistema mediante la reducción de su superficie de vulnerabilidad". Esta definición nos indica que la



reducción de la superficie de vulnerabilidad o superficie de ataque, ayudará a que el sistema en cuestión sea más seguro y se disminuyan las chances de que potenciales atacantes tengan éxito en sus intentos de intrusión.

Habiendo definido estos conceptos, se comprende más claramente el fin buscado y habilita la posibilidad de descripción del hardening de Seguridad de un Gestor Documental (específicamente aplicado al Gestor Documental Alfresco, que es el que se utilizará para el presente proyecto).

Para estructurar el sistema y lograr una arquitectura segura que mitigue las amenazas más comunes, como primera medida es necesario basarse en estadísticas actuales y objetivas respecto de ataques a recursos informáticos relacionados con el objeto de estudio. Para ello, se utilizará el Top 10 de los riesgos más críticos de seguridad en aplicaciones web elaborado por OWASP [\[01\]](#) (Open Web Application Security Project, en inglés "Proyecto abierto de seguridad de aplicaciones web", el cual es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro). De esta investigación de OWASP podemos enumerar los ataques más comunes de la siguiente forma:

- A1. Injection.
- A2. Broken Authentication and Session Management.
- A3. Cross Site Scripting (XSS).
- A4. Insecure Direct Object References.
- A5. Security Misconfiguration.
- A6. Sensitive Data Exposure.
- A7. Missing Function Level Access Control.
- A8. Cross Site Request Forgery (CSRF).
- A9. Using Known Vulnerable Components.
- A10. Unvalidated Redirects and Forwards.

Tomando como referencia estos diez puntos vamos a plantear las posibles soluciones sobre la línea base definida para este trabajo.

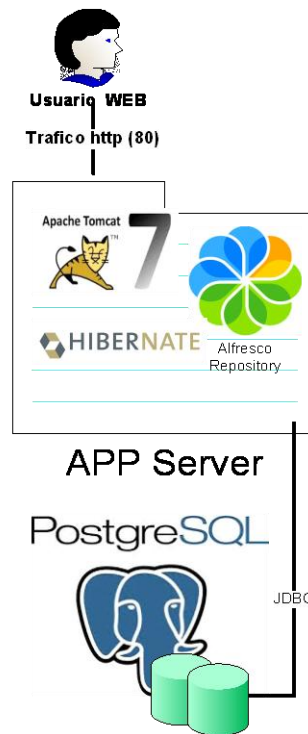


Figura N° 01 - Arquitectura inicial de componentes de Alfresco

Este esquema simplificado describe el entorno de nuestro servidor de aplicaciones. Vamos a delimitar cuales son los impactos que pueden tener los 10 posibles problemas anteriores sobre esta arquitectura simplificada. De esta forma vamos a intentar modificarla para llegar a una arquitectura robusta que minimice cada uno de estos puntos.

A1) Inyección:

Este ataque intenta engañar a una aplicación incluyendo comandos no deseados en los datos enviados a un intérprete.

De acuerdo al intérprete, se agrupan en diferentes tipos como por ej.: SQL, OS Shell, LDAP, XPath, Hibernate, etc.

Si bien es simple mitigarlo porque sólo habría que validar que en los diferentes input de nuestro sistema no se filtren este tipo de mensajes. Por su evolución dinámica, se aprovecha de diferentes recursos como por ejemplo los encoding de los mensajes, validarlo en cada entrada de una aplicación implica un trabajo importante. Además si tenemos en cuenta el caso sobre el que vamos a trabajar que es un sistema ya desarrollado por un tercero, por más que tengamos los fuentes del mismo, realizar este tipo de validaciones de forma dinámica y evolutiva sería muy complicado.



A2) Broken Authentication and Session Management

(anteriormente 2010-A3): corresponde al mal manejo de las sesiones en aquellas aplicaciones que utilizan autenticación.

A menudo, a la hora de implementar aplicaciones web, los desarrolladores suelen no darle la importancia y la revisión necesaria a la sesión del usuario. Los mismos, muchas veces, crean esquemas propios de autenticación o gestión de sesiones exponiendo vulnerabilidades que pueden poner en riesgo información sensible del usuario.

Estos métodos propios de autenticación o de gestión de sesiones de usuario creados por los desarrolladores son pocas veces exhaustivamente probados y son utilizados con un gran número de defectos que pueden traer consecuencias severas.

Es por esta razón que estos esquemas o métodos contienen vulnerabilidades en las secciones de cierre de sesión, gestión de contraseñas, tiempo de desconexión, función para recordar contraseña, pregunta secreta y actualización de cuenta entre otros, y podrían permitir que algunas o todas las cuentas sean atacadas. Una vez que el ataque resulte exitoso, el atacante podría realizar cualquier acción que la víctima pudiese realizar. Las cuentas privilegiadas son los objetivos prioritarios para los atacantes.

A3) Cross-Site Scripting (XSS)

(anteriormente 2010-A2): ocurre cuando existe validación pobre de la información ingresada por el atacante.

Es un ataque típico de las aplicaciones Web, que permite a una tercera parte inyectar en páginas web vistas por el usuario código JavaScript o en otro lenguaje script similar (ej: VBScript), evitando medidas de control como la Política del mismo origen. Este tipo de vulnerabilidad se conoce en español con el nombre de Secuencias de comandos en sitios cruzados.

Es posible encontrar una vulnerabilidad XSS en aplicaciones que tengan entre sus funciones presentar la información en un navegador web u otro contenedor de páginas web. Sin embargo, no se limita a sitios web disponibles en Internet, ya que puede haber aplicaciones locales vulnerables a XSS, o incluso el navegador en sí.

XSS es un vector de ataque que puede ser utilizado para robar información delicada, secuestrar sesiones de usuario, y comprometer el navegador, subyugando la integridad del sistema. Las vulnerabilidades XSS han existido desde los primeros días de la Web.



A4) Insecure Direct Object References

Puede derivar en un acceso no autorizado a información crítica debido a errores en el diseño o desarrollo. Una referencia directa insegura a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.

Por ejemplo, en las aplicaciones "Home Banking", es común usar el número de cuenta como clave primaria. Por lo tanto, es tentador usar el número de cuenta directamente en la interfaz web. Incluso si los desarrolladores tomaron las medidas necesarias para prevenir ataques de SQL Injection, si no hay validaciones extra que verifiquen que el usuario es el dueño de la cuenta y que está autorizado para verla, un atacante puede forzar el parámetro número de cuenta y lograr ver o cambiar todas las cuentas.

A5) Security Misconfiguration

Un buen nivel de seguridad requiere lograr configuraciones seguras definidas e implementadas tanto en la aplicación, marco de trabajo, servidor de aplicaciones, servidor web, servidor de bases de datos, como así también en la plataforma. Las configuraciones seguras deben ser definidas, implementadas y mantenidas, teniendo en cuenta que los parámetros por defecto suelen ser inseguros. Adicionalmente, el software debe mantenerse actualizado.

A6) Sensitive Data Exposure

(2010-A7 Insecure Cryptographic Storage y 2010-A9 Insufficient Transport Layer Protection formaron 2013-A6): se refiere a la protección incorrecta de datos críticos tales como, por ejemplo, números de tarjetas de crédito, contraseñas, entre otros. Exposición de datos Sensibles

A7) Missing Function Level Access Control

Corresponde a la falta de controles desde el servidor, permitiendo a un posible atacante acceder a funciones a las que no debería.

A8) Cross-Site Request Forgery (CSRF)

(anteriormente 2010-A5): Permite a un atacante generar peticiones sobre una aplicación vulnerable a partir de la sesión de la víctima.

A9) Using Known Vulnerable Components

(anteriormente formaba parte de 2010-A6): corresponde a la explotación de librerías, frameworks y otros componentes



vulnerables por parte de un atacante con el fin de obtener acceso o combinar con otros ataques.

A10) Unvalidated Redirects and Forwards

Los atacantes aprovechan el uso de redirecciones de sitios web a otros sitios utilizando información no confiable (untrusted) para redirigir a las víctimas a sitios de phishing o que contienen malwares.



03.01. PROPIEDADES DE SEGURIDAD QUE SE BUSCAN

Las características de Seguridad de la Información que pueden obtenerse al aplicar hardening a Alfresco son las que se enuncian a continuación:

- **Confidencialidad**: Se refiere a la capacidad de proteger a una comunicación entre dos interlocutores para no ser interceptada ni interferida por una tercera persona que no forme parte de la comunicación. Para ello, la PKI utiliza mecanismos de cifrado que evitarían que individuos no autorizados se hagan de los mensajes.
- **Autenticación**: Apunta a que se brinde acceso a una comunicación electrónica sólo a quienes se pueda corroborar su identidad y se pueda constatar su habilitación. En este caso, los certificados digitales y la estructura de confianza intrínseca a la PKI conforman una alternativa de autenticación a la tradicional presentación de credenciales (usuario/contraseña).
- **Integridad**: Se necesario comprobar que la información enviada sea exactamente la misma que la que se reciba. El control apunta a garantizar que los datos no fueron alterados dentro del canal de comunicación. Adicionalmente, el control sirve para corroborar que 1 archivo se mantiene inalterado en el tiempo o en distintos medios de almacenamiento, garantizando que poseen en mismo contenido. A nivel técnico, este control es logrado a través de las funciones de hash que permiten efectuar comparaciones inequívocas de integridad de datos.
- **No-repudio**: Esencialmente implica que los interlocutores no pueden negar haber enviado los mensajes que los muestren como remitentes. Esta propiedad hace que, ante algún problema entre las partes al haber intercambiado mensajes electrónicos, sea innegable evidencia presente dentro del sistema de comunicación que pueda ser utilizada para probar con suficiente certeza lo que realmente sucedió. Esto cobra especial importancia en operaciones financieras o trámites de índole legal cuyas consecuencias pueden ser de relevancia. Esta característica de Seguridad habitualmente está más relacionada a la implementación de infraestructura PKI.



04. ALTERNATIVAS A SISTEMAS DE GESTIÓN DOCUMENTAL

04.01. ALFRESCO

Alfresco [02] es una plataforma open-source que tiene como objetivo la colaboración y la gestión documental para aquella información crítica para la organización. Interviene en la automatización de los procesos organizacionales que utilizan intensivamente documentos, permitiendo la colaboración a gran escala. De esta manera, se mejora la prestación a los clientes internos de la organización (y externos, si aplicare).

Es una solución versátil compatible con software tanto de la vertiente Microsoft, como de la rama Linux. Posibilita la creación y gestión de contenidos empresariales desde una gran cantidad de CMSs (Content Management Systems), blogs y paquetes ofimáticos (Office y OpenOffice)

La gestión documental de Alfresco ofrece las siguientes características:

- Control de versiones.
- Visualizaciones previas en línea.
- Flujo de trabajo eficaz.
- Integración con MS Office y GoogleDocs.
- Grupos y tipos de propiedades.
- Búsqueda exhaustiva.

04.02. NUXEO

Nuxeo [03] aporta soluciones a las necesidades primarias de gestión documental de las empresas, permitiendo gestionar cómodamente documentos mediante control de versiones, flujos de trabajo asociados, publicación remota o búsqueda avanzada a texto completo, además de integración con suite ofimáticas habituales como Microsoft Office y Open Office. Además, a través de la aplicación complementaria Nuxeo Digital Asset Management también se ofrece soporte para imágenes y vídeos.



Su implementación es sencilla si lo que se quieren cubrir son necesidades no muy específicas y además al estar desarrollado sobre estándares abiertos, cuenta de entrada con la facilidad de ampliar su funcionalidad mediante desarrollo y resulta interoperable con terceros lo cual pone al alcance de un mayor número de técnicos el conocimiento necesario para trabajar sobre él, ganando así en productividad. El que sea una plataforma significa que contempla el crecimiento futuro (fase beta en positivo) y además lo ventajoso es que su adaptación a propósitos específicos no es tan costosa como en el caso de Sharepoint, Documentum, IBM FileNet, u otras soluciones cerradas. Escoger esta solución te ofrece las siguientes características:

- Colaboración, flujos de trabajo, búsquedas eficientes.
- Flexibilidad, empleando una arquitectura basada en estándares.
- Robustez, utilizando Java para entornos Enterprise (J2EE) entre otras tecnologías.
- Velocidad, gracias a la integración con el rápido motor de búsqueda Lucene.
- Capacidad de evolución en captura inteligente de documentos mediante Athento.
- Seguridad gracias a la implementación de estándares como SSL, Single Sign On (SSO) y facilitando el cumplimiento con normativas como la ISO 27.001 (Seguridad de la Información) o la Ley de Protección de Datos (LOPD).



04.03. COMPARATIVA DE GESTORES DOCUMENTALES OPEN-SOURCE

Como alternativas comparables a los efectos de seleccionar un gestor documental se tomó a Alfresco Community Edition y a Nuxeo, teniendo en cuenta que ambos gozan de gran reputación y un importante número de organizaciones los utilizan para sus procesos de negocios. Si bien existen otras alternativas interesantes para implementar gestión documental corporativa, el análisis del presente trabajo se limita a los 2 paquetes de software mencionados:

<i>Criterio comparativo</i>	<i>Nuxeo</i>	<i>Alfresco</i>
Facilidad de uso	Alta	Alta
Capacidad de modelo de seguridad granular	Alta	Alta
Posibilidad de personalización	Alta	Alta
Capacidad de Gestión de workflows	Alta	Alta
Afinidad del implementador con la solución	Baja	Alta
Escalabilidad	Meda	Alta
Capacidad de integración con otros sistemas	Media	Media
Calidad de la documentación	Media	Media
Acceso a Soporte Técnico	Medio	Medio
Afinidad del implementador con el hardening de la solución	Baja	Alta

Tabla N° 01 - Comparación de gestores documentales



05. DETALLES DEL SOFTWARE A UTILIZAR

Teniendo en cuenta los análisis llevados adelante en los puntos anteriores, se concluye que la mejor alternativa para la gestión documental es Alfresco.

El diagrama de red básico sobre el cual se instalará Alfresco se presenta a continuación, contemplando las funcionalidades de repositorio y además de manejo de workflows:

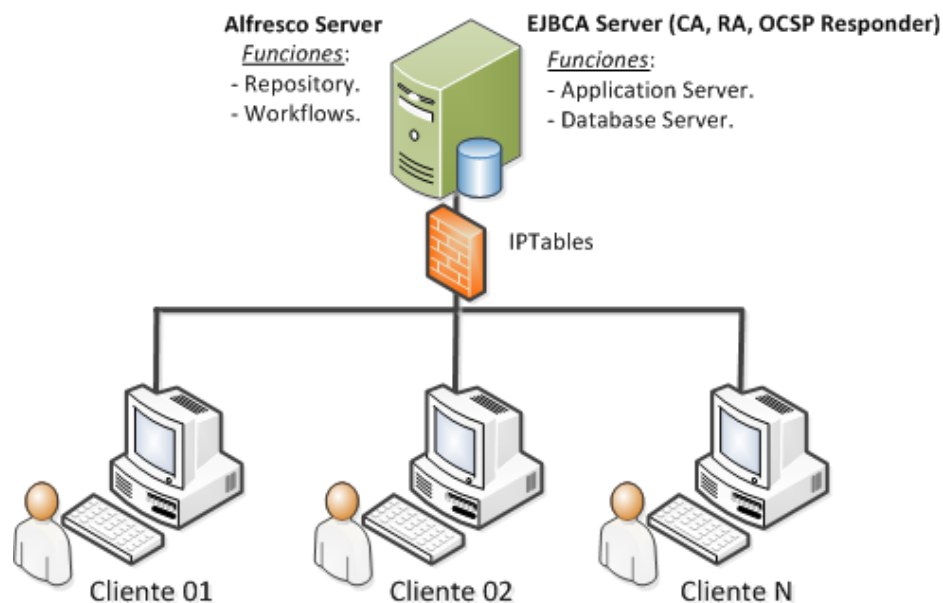


Figura N° 02 - Arquitectura simplificada de implementación Alfresco

Adicionalmente, a los efectos de cumplir con un exhaustivo hardening de Alfresco, se estudian las parametrizaciones y mejoras que se aplicarán.

Analizando los posibles ataques y relevando la arquitectura de una implementación Alfresco tomando en cuenta las características necesarias para un servidor de producción con niveles de servicio adecuados encontramos que es fundamental agregar al modelo anterior algunos elementos que nos faciliten un marco seguro sin cambiar el desarrollo de la solución. De esta forma, para poder mitigar los ataques del tipo A1, A3, A4, A7, A8 y A10 sin modificar el sistema la solución más recomendada por diferentes autores es colocar un firewall activo de aplicaciones web. Siguiendo la filosofía GPL del producto una alternativa recomendable sería montar un servidor



Apache como proxy AJP y habilitar ModSecurity [04], este módulo de Apache, que mediante del filtrado de los distintos métodos HTTP (GET, POST, etc.) adquiere un comportamiento de Firewall Web, filtrando ataques potenciales a nuestros sitios web.

ModSecurity trabaja con sets de reglas especializadas y personalizables, que podemos cargar o excluir según virtualhost o directorio. Estas reglas trabajan filtrando ataques por Cross Scripting o XSS, inyecciones SQL, anomalías en protocolos, Robots maliciosos, Troyanos, inclusión de archivos (LFI), etc. y recientemente se incorpora un set de reglas específicas (slr_rules) para diferentes ECM.

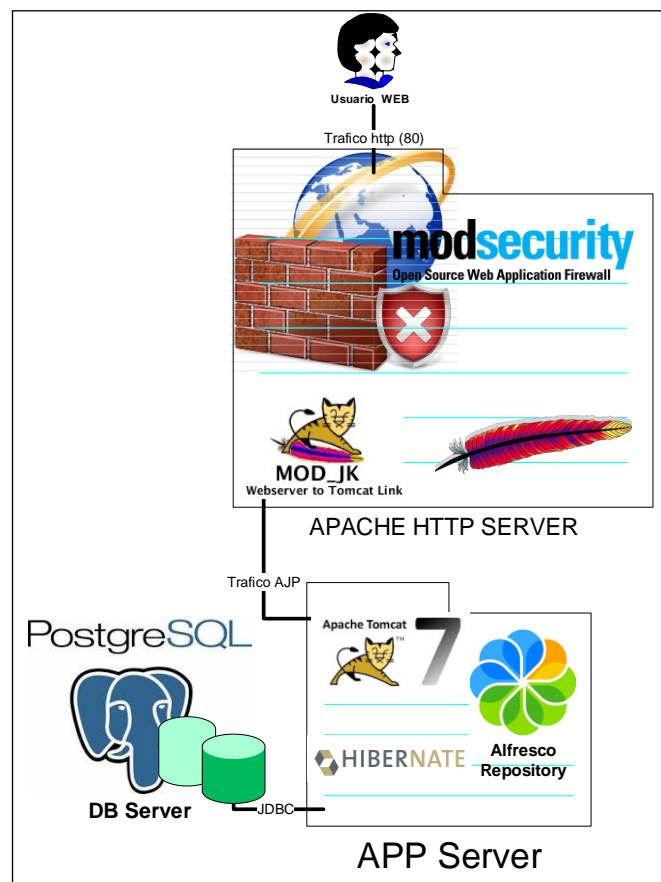


Figura N° 03 – Medidas de hardening de Alfresco

La potencialidad de dicha herramienta es incuestionable, ya que no sólo permite proteger los sitios web desplegados en Apache sino los sitios que puedan estar redirigidos a través de ModProxy, por lo que podemos proteger múltiples aplicaciones web desplegadas en diversos servidores tras un Apache equipado con ModProxy y ModSecurity.



De esta forma podemos mitigar los ataques antes mencionados sin modificar el sistema.

La segunda etapa sería asegurar el AppServer, a nivel del servidor web Tomcat, en su entorno y Sistema Operativo.

Como primera medida ya definida nuestra estructura segura es la configuración inicial de los sistemas operativos de cada componente. En este caso excluiríamos de nuestro alcance a la configuración del servidor de Base de Datos. Nos centraremos en el Apache HTTP Server que agregamos como primera frontera de seguridad y el Apache Tomcat que da soporte a nuestro AppServer.

La primera definición es que estos dos servidores van a estar montados sobre un Sistema Operativo GNU/Linux usando como distribución Ubuntu Server 12.04 LTS. Esta selección fue debido a que Alfresco tiene soporte oficial para distintos Sistemas Operativos, pero el único libre recomendado es GNU/Linux Ubuntu y la última distribución estable de Alfresco Community (4.02C) recomienda como implementación a la versión LTS 12.04 de Ubuntu.

El hardening a nivel sistema operativo de los servidores Apache http y Apache Tomcat se hará ajustando configuraciones del servidor Ubuntu 12.04 LTS agregando y parametrizando las siguientes características:

1. Instalación y configuración de firewall – ufw, habilitando sólo los puertos y protocolos necesarios por server y limitando los diferentes accesos según a qué zona pertenezcan.
2. Habilitar el modo seguro en la memoria compartida – fstab -Por defecto, /dev/shm está montado en modo lectura/escritura, con permisos para ejecutar programas. En los últimos años, muchas listas de correo han notado algunos exploits cuando /dev/shm era usado para atacar otro servicio en funcionamiento, como httpd. La mayoría de estos exploits, sin embargo, se deben a confiar en una aplicación web insegura en lugar de ser una vulnerabilidad en Apache o Ubuntu. Hay unas cuantas razones para montarlo en modo lectura/escritura en configuraciones específicas, tales como una configuración de tiempo real de un touchpad Synaptic para ordenadores portátiles, pero para servidores e instalaciones de escritorio no hay ningún beneficio al montar /dev/shm en modo lectura/escritura. Para cambiar esta opción, es necesario editar el archivo /etc/fstab e incluir la siguiente línea:
tmpfs /dev/shm tmpfs defaults,ro 0 0
3. Deshabilitar el acceso de root del SSH y cambiarle el puerto por defecto.



4. Habilitar el acceso al comando SU sólo al grupo ADMIN.
5. Implementar la configuración segura de red mediante la configuración de sysctl.
6. Deshabilitar recursión DNS, no mostrar versión - Bind9 DNS.
7. Prevenir el IP Spoofing marcando en "on" el nospof.
8. Configurar de forma segura el servidor Apache (en un caso apache HTTP y en el otro Apache Tomcat)
9. Instalar y habilitar en el servidor HTTP el firewall Web antes mencionado - ModSecurity
10. Habilitar la protección de los ataques DDOS (Denial of Service) habilitando ModEvasive
11. Escanear los logs y prevenir los host sospechosos a través de DenyHosts y Fail2Ban.
12. Habilita la prevención y detección de intrusos mediante PSAD.
13. Instalación Segura de PostgreSQL 9.0.4 [\[05\]](#) [\[07\]](#) usando como guía "Security Hardening PostgreSQL" de Scott Mead.
14. Instalación Segura de Apache Tomcat [\[06\]](#): vamos a seguir las guías de consideraciones de seguridad publicadas por el fabricante para la versión 7.042 (última versión estable a la fecha).



06. HARDWARE A UTILIZAR

Como prototipo de implementación de la arquitectura antes descrita vamos a utilizar tres máquinas virtuales sobre un servidor VMWare Hipervisor 5.01. El servidor asignado para este fin es un en un servidor IBM x 3300 M4 - Procesador Xeon 4C E5-2407 80W 2,66 GHz/1066 MHz/ 10 MB, HDD: 3x2 TB 7,2K 6Gbps Sata 3,5" Memoria: 32GB de RAM DDR3 1333 MHz.

El detalle de la asignación del hardware virtual entre las máquinas virtuales se tratará en la sección de "Implementación de la Solución".



07. DESCRIPCIÓN DEL PROCESO A ABORDAR CON EL GESTOR DOCUMENTAL

A continuación se muestra la línea de tiempo correspondiente al proceso completo de tesis que cualquier tesista del IUA, ya sea de Trabajo Final de Pregrado, Proyecto de Grado o Trabajo Final de Posgrado, debe transitar desde la inscripción a la correspondiente materia y hasta la defensa de la tesis ante el tribunal designado (se resalta que el presente trabajo de Gestor Documental es complementario con el trabajo final presentado por el Ing. Boiero, teniendo en cuenta las posibilidades brindadas por una infraestructura PKI).

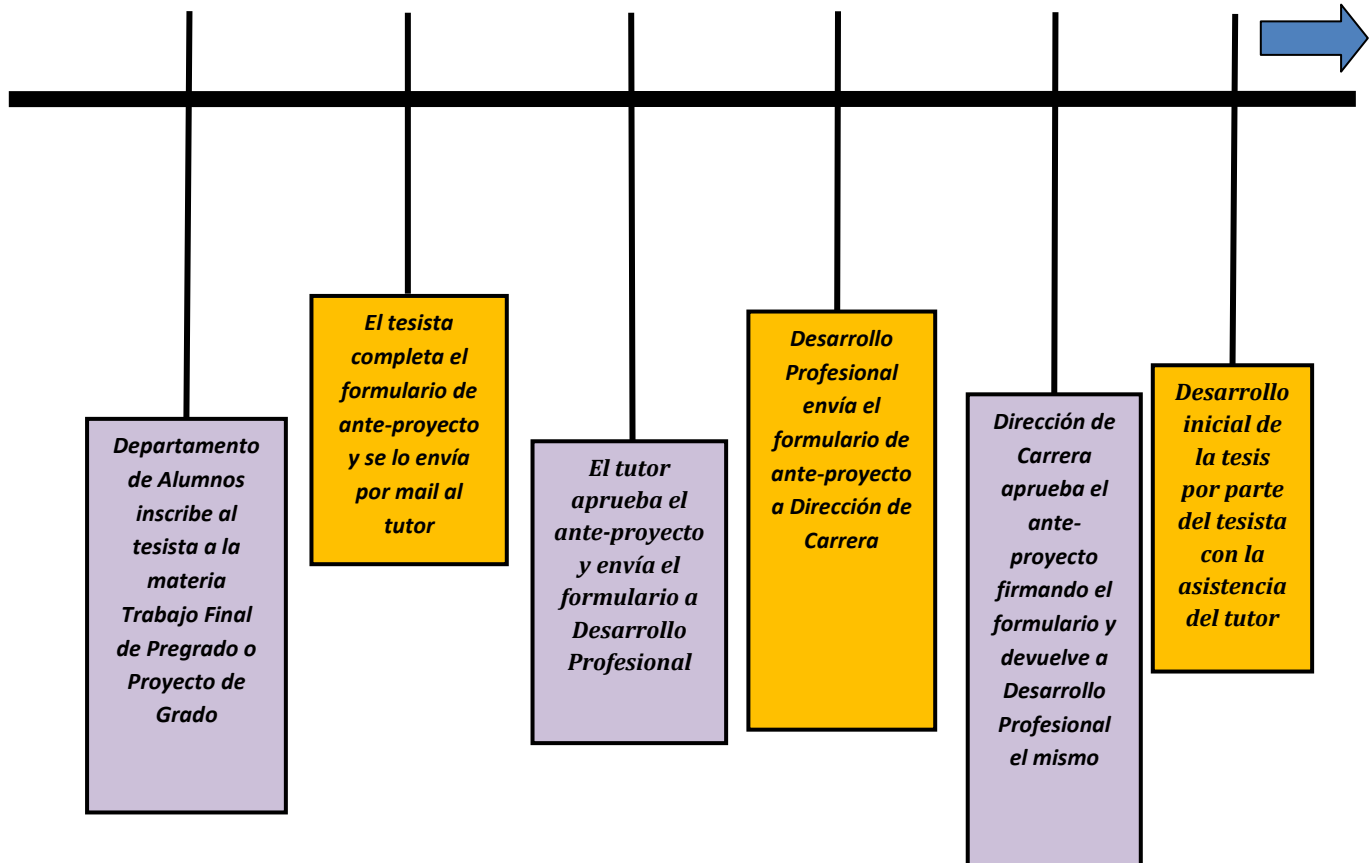


Figura N° 04 - Proceso a abordar - parte 1

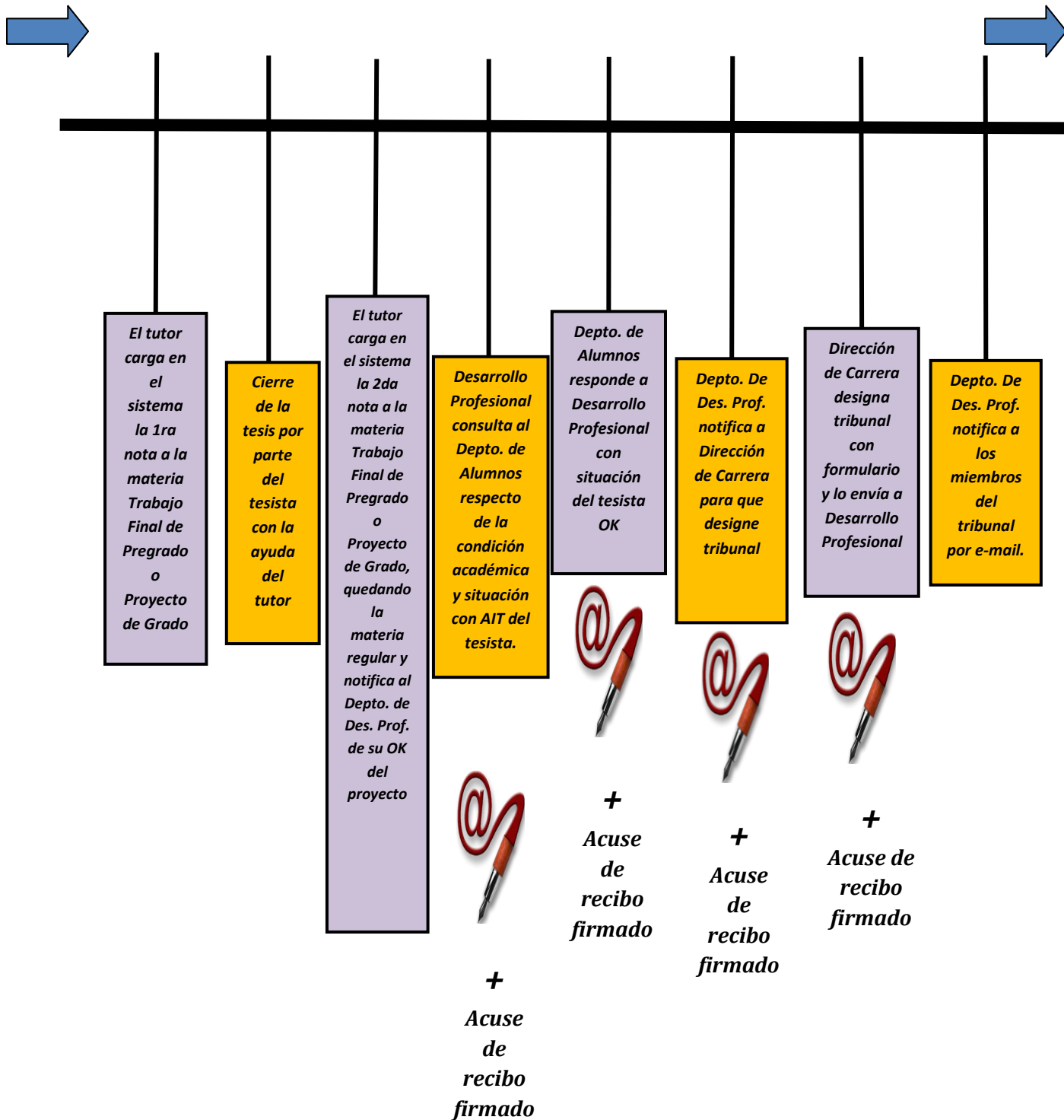


Figura N° 05 - Proceso a abordar - parte 2

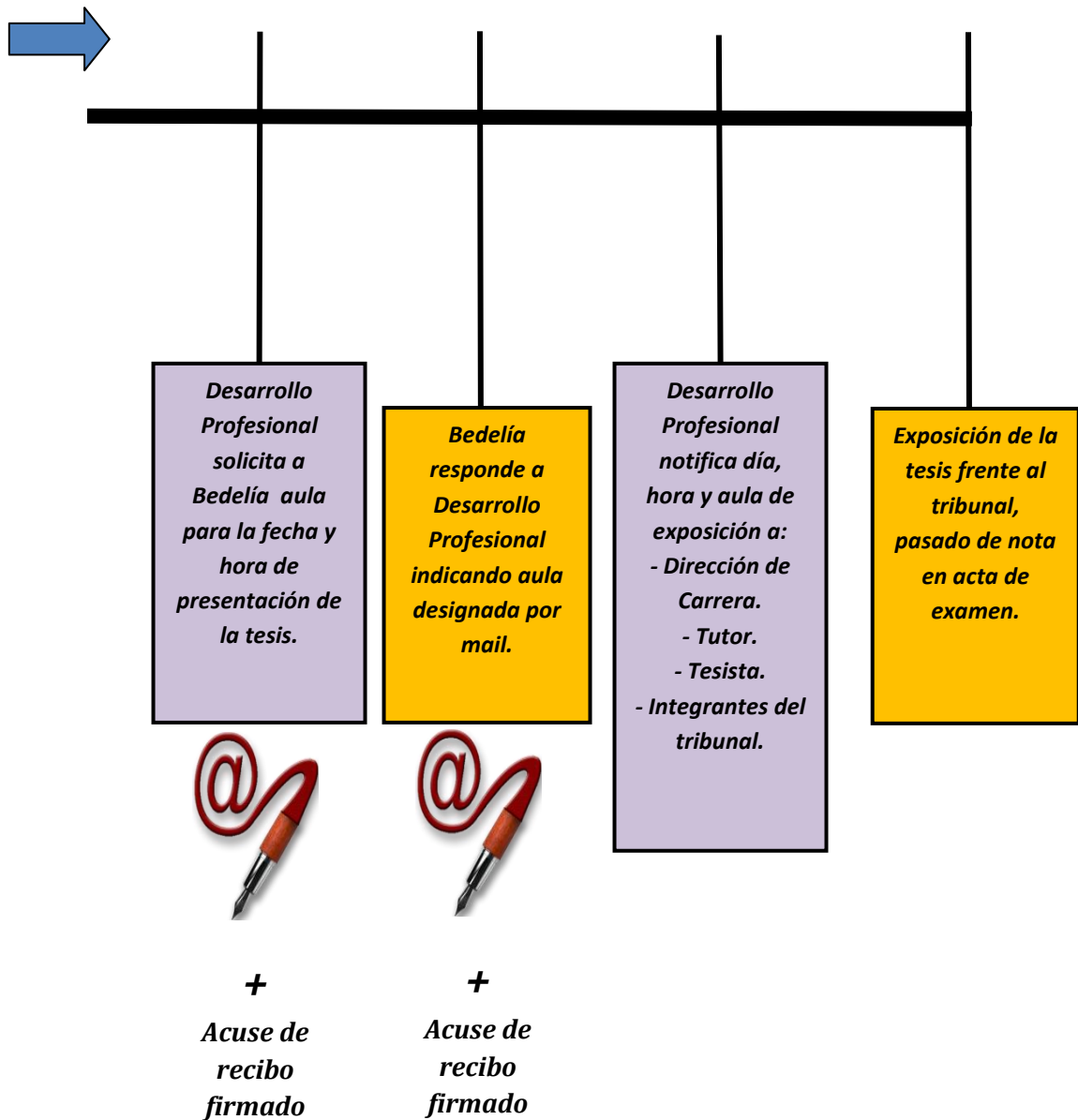


Figura N° 06 - Proceso a abordar - parte 3

A partir del relevamiento realizado con la Dirección de Carrera de Ingeniería de Sistemas y la Coordinación Ejecutiva, se procedió a limitar el alcance del presente proyecto a los siguientes sub-procesos, sirviendo los mismos de ejemplo de aplicación para virtualmente cualquier proceso interno del IUA:



Flujo de Anteproyecto

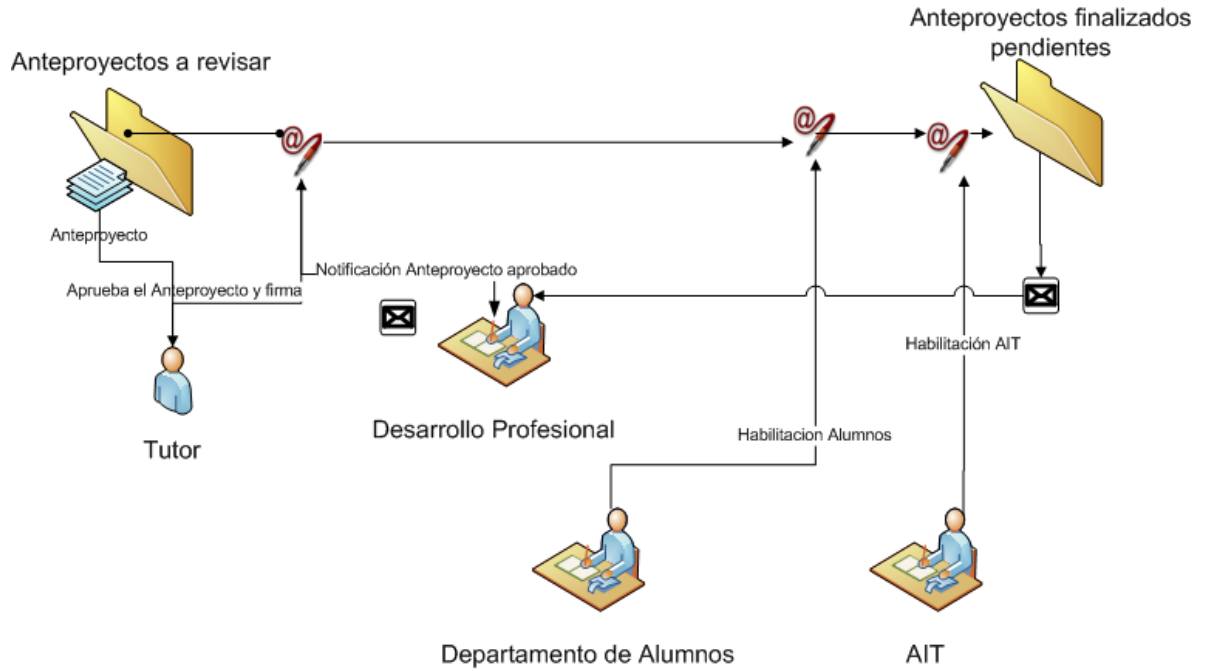


Figura N° 07 - Flujo de información de anteproyecto de tesis



08. IMPLEMENTACIÓN DE LA SOLUCIÓN

Para implementar la solución del Gestor Documental Alfresco y para realizar su posterior hardening de seguridad si efectuó el siguiente despliegue:

Estos recursos de hardware "real" se utilizarán para correr las 3 Máquinas Virtuales, con las siguientes características:

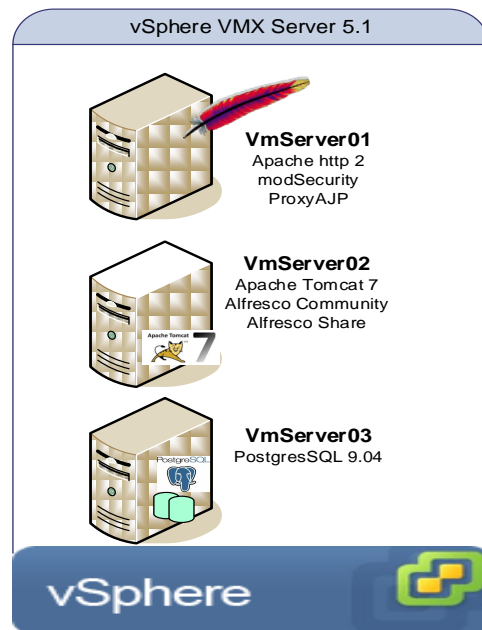


Figura N° 08 – Despliegue de máquinas virtuales a utilizar

a) VMServer01:

Es nuestra máquina virtual de Front-End donde se publica nuestro sistema web al público por intermedio de un proxy AJP, componente diseñado para interconectar Apache HTTP con Apache Tomcat, este componente tiene la capacidad de poner en el Back-End servidores Tomcat redundantes pudiendo priorizarlos y asignarle porcentajes de las transacciones, para poder armar una arquitectura escalable. Como seguridad adicional se habilitó el módulo de firewall web ModSecurity con la configuración anteriormente mencionada.



Como hardware virtual se estableció: 8GB de RAM, 4 núcleos dos interfaces de red una de pública y otra privada y un disco de 100GB.

b) VMServer02:

Esta máquina virtual se encuentra en el Back-End donde se montó el servidor de aplicaciones Apache Tomcat 7 y se desplegó el Sistema Alfresco Community 4.02.

Como mencionamos anteriormente, esta máquina virtual se puede replicar haciendo que la solución sea redundante para mejorar la disponibilidad en el caso de ser necesario.

Como hardware virtual se estableció: 8GB de RAM, 4 núcleos dos interfaces de red una de pública y otra privada y un disco de 1TB.

c) VMServer03

También se encuentra en el Back-End donde se cuenta con el servidor de Base de Datos PostgreSQL 9.04.

En el caso de ser necesario este server se puede configurar de forma redundante en una configuración maestro esclavo.

Como hardware virtual se estableció: 12GB de RAM, 4 núcleos dos interfaces de red una de pública y otra privada y un disco de 100GB.

La instalación de Alfresco se efectuó con las opciones que se presentan por defecto a lo largo de las pantallas, según se muestra en el [Anexo I](#).

Para darle soporte al proceso descrito en el punto anterior se utilizó el motor de workflows Activity que trae incorporado Alfresco. Además se le agregó un AMP (Alfresco Module Package) denominado Alfresco PDF Toolkit permite añadir una serie de funcionalidades extra al gestor documental Alfresco. De esta forma es posible manipular y trabajar con documentos PDF. En este caso la función que más se aprovechará es la de firmar digitalmente documentos desde un workflow (WF). Los detalles técnicos de las funcionalidades de workflow se incorporan en el [Anexo II](#).



09. DEMOSTRACIÓN DE USO

Para el proceso seleccionado los usuarios son tres diferentes:

- A. Usuario Tutor: Se le va a emitir un certificado con perfil Docente.
- B. Usuario Secretaría de Alumnos: Se le va a emitir un certificado con Perfil Empleado
- C. Usuario AIT: Se le va a emitir un certificado con Perfil Empleado

Como precondition para la utilización completa de Alfresco y sus workflow, se contó con la infraestructura PKI provista por el proyecto del Ing. Boiero, permitiendo contar con los certificados digitales necesarios para realizar las tareas de firma electrónica dentro de Alfresco.

De esta manera, habiendo sido generado y descargado el certificado digital en la terminal del usuario, se procede a subirlo a su carpeta personal de Alfresco, en la carpeta certificado dispuesta para tal fin.

A este procedimiento lo debe realizar cada usuario que necesite firmar electrónicamente desde Alfresco. A continuación se describen los pasos del proceso sistematizado:

- a) El tutor accede al sistema ingresando su usuario y password, el sistema despliega las carpetas de trabajo "Proyectos_Finalizados" y "Proyectos_Pendientes_Aprobacion"

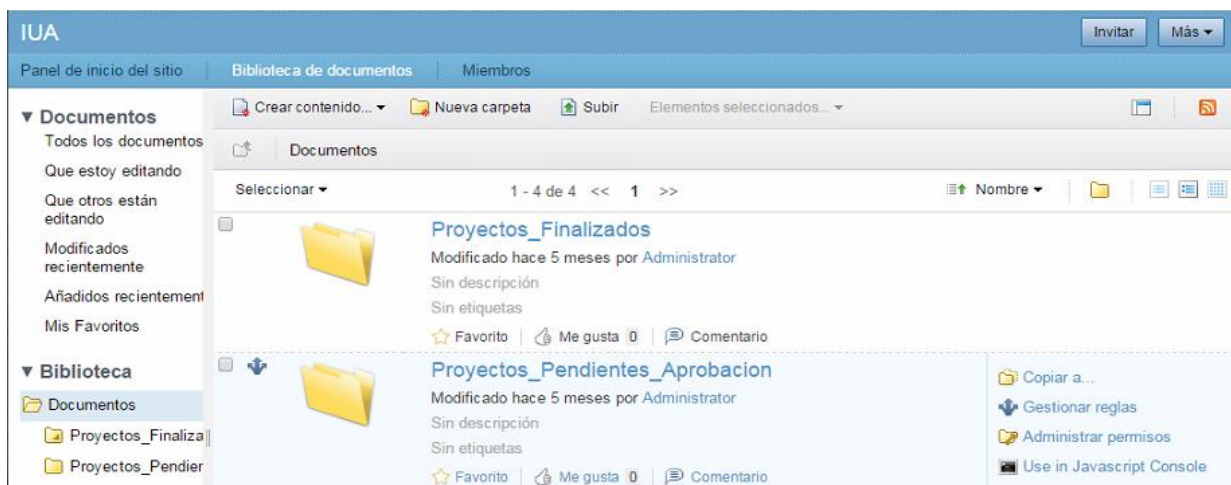


Figura N° 09 - Acceso de tutor a interfaz web de Alfresco



b) El tutor selecciona la carpeta “Proyectos_Pendientes_Aprobacion” e inicia un flujo de aprobación.

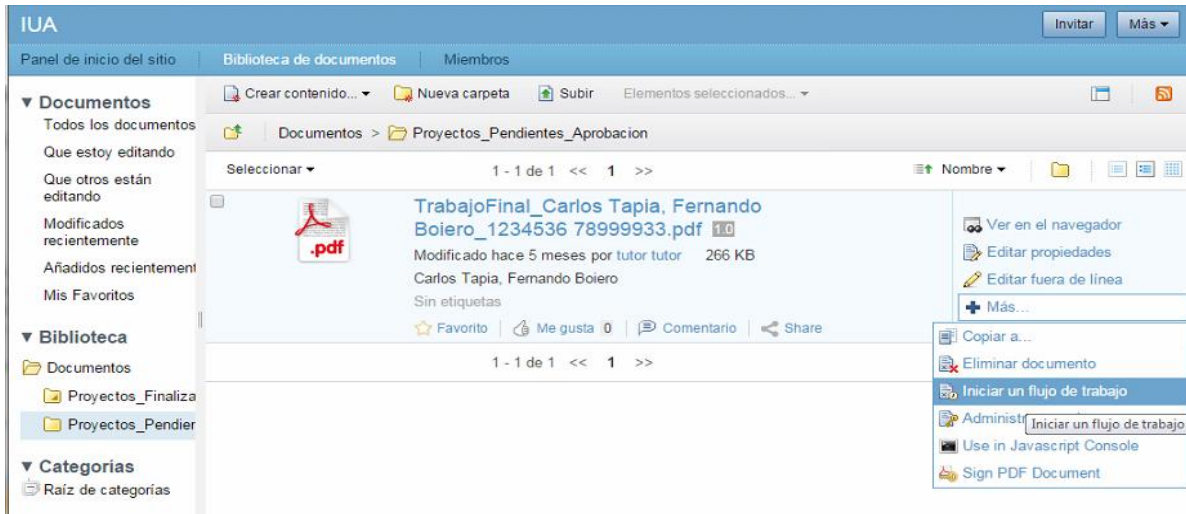


Figura N° 10 - Flujo de aprobación en Alfresco



IUA

Panel de inicio del sitio | Biblioteca de documentos | Miembros

Iniciar un flujo de trabajo

Flujo de trabajo: Por favor, seleccione un flujo de trabajo... ▼

- Aprobacion de Trabajo
- Aprobacion de Trabajo

Figura N° 11 - Inicio del flujo de aprobación en Alfresco

c) El Tutor completa los datos asociados a este proceso:

Iniciar un flujo de trabajo

Flujo de trabajo: Aprobacion de Trabajo ▼

* Campos requeridos

Mensaje: TrabajoFinal_Carlos Tapia, Fernando Boiero

Vencimiento: 29/11/2014 DD/MM/AAAA

Prioridad: Media

Elementos

Elementos:

- TrabajoFinal_Carlos Tapia, Fernando Boiero_1234536 78999933.pdf
Descripción: Carlos Tapia, Fernando Boiero
Modificado: Jue 26 Jun 2014 21:17:54
Ver más acciones
Eliminar

Añadir Quitar todos

Otras opciones

Enviar notificaciones de correo electrónico

Iniciar un flujo de trabajo Cancelar

Figura N° 12 - Prueba de datos en el flujo de aprobación en Alfresco



- d) El tutor aprueba el trabajo firmando digitalmente ingresando su PIN, el sistema envía un correo electrónico a la secretaria de alumnos notificando el inicio del proceso.

Editar tarea: AprobacionTrabajo Pedir

Esta tarea está sin asignar.

* Campos requeridos

Aprobacion de Trabajo Tutor

Mensaje: Revisar

Elementos:

TrabajoFinal_Carlos Tapia, Fernando Boiero_1234536 78999933.pdf Ver más acciones

Descripción: Carlos Tapia, Fernando Boiero Eliminar

Modificado: Jue 26 Jun 2014 21:17:54

Añadir Quitar todos

Vencimiento: DD/MM/AAAA

Prioridad: *

PIN:

Approve Reject

Figura N° 13 - Firma Digital dentro del flujo de aprobación en Alfresco



Figura N° 14 - Documento firmado en Alfresco



- e) El flujo se asigna al grupo de Secretaria de Alumnos.
- f) Un usuario del grupo Secretaria de Alumnos ingresa al sistema y le muestra que tiene una tarea activa para revisar.



Figura N° 15 - Acceso de Secretaría de Alumnos en Alfresco

- g) El usuario de Secretaria de Alumnos selecciona la Actividad y corrobora que los Alumnos tengan las condiciones académicas necesarias para presentar la Tesis. En el caso de que efectivamente las cumplan, el usuario ingresa su PIN, lo aprueba y se genera un certificado firmado digitalmente. El sistema notifica por mail a los usuarios del grupo AIT que tienen una tarea asignada.

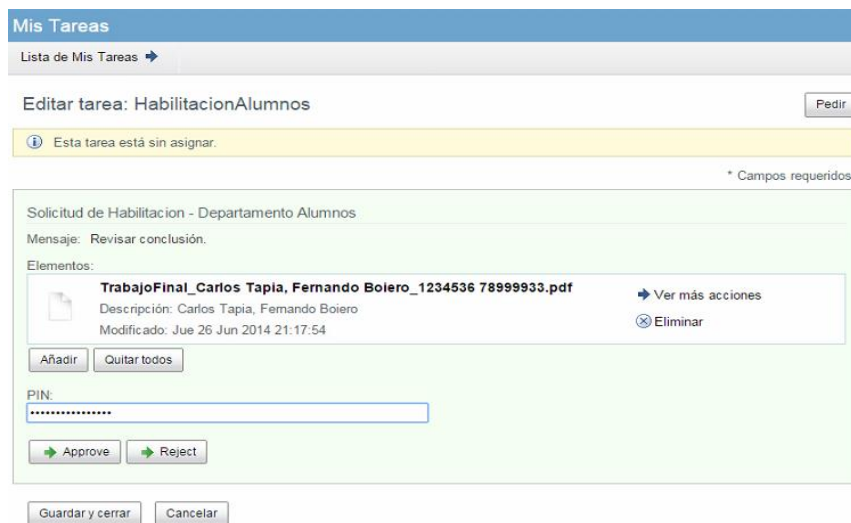


Figura N° 16 - Acceso de Secretaría de Alumnos en Alfresco



- h) Por último el trabajo aprobado por la Secretaría de Alumnos se asigna al grupo AIT. Luego, un usuario del grupo AIT ingresa al sistema, abre la Tarea Asignada corrobora que los alumnos asignados estén con las cuotas al día y de ser así aprueba firmando digitalmente ingresando su PIN. El sistema notifica por correo electrónico al tutor y a la Secretaría de Alumnos respecto de la finalización del proceso.

The screenshot shows the 'Flujos de trabajo que he iniciado' (Workflows I have started) section. On the left, there is a navigation menu with 'Flujos de trabajo' expanded, showing 'Activa' (Active) and 'Completada' (Completed). Below it, 'Vencimiento' (Expiration) is set to 'Hoy' (Today). The main content area shows 'Iniciar un flujo de trabajo' (Start a workflow) and 'Flujos de trabajo activos' (Active workflows). A task is listed with a 'Revisar' (Review) button, a due date of 'Vencimiento: 29 Noviembre, 2014', and a start date of 'Iniciado: 28 Noviembre, 2014'. The task type is 'Aprobacion de Trabajo' (Work Approval).

Figura N° 17 - Tareas activas en el flujo de trabajo en Alfresco

- i) Para corroborar el flujo completo el tutor puede acceder a sus actividades completadas.

The screenshot shows the 'Flujos de trabajo que he iniciado' (Workflows I have started) section. On the left, the 'Completada' (Completed) option is selected under 'Flujos de trabajo'. The main content area shows 'Iniciar un flujo de trabajo' (Start a workflow) and 'Flujos de trabajo completados' (Completed workflows). A task is listed with a 'Revisar' (Review) button, a due date of 'Vencimiento: 29 Noviembre, 2014', a completion date of 'Finalizado: 28 Noviembre, 2014', and a start date of 'Iniciado: 28 Noviembre, 2014'. The task type is 'Aprobacion de Trabajo' (Work Approval) and the description is 'Aprobacion de Trabajo' (Work Approval).

Figura N° 18 - Tareas completadas en el flujo de trabajo en Alfresco



Resumen del flujo de trabajo Ver diagrama de proceso


General

- Flujo de trabajo en curso
- (Sin fecha de vencimiento)
- Prioridad Media

Tarea completada más recientemente Ver las tareas actuales

wfprocesar:start

Completada el: 5 Sep, 2014 Completado por: Administrator Resultado: Tarea hecha

 Comentario de Administrator :
(Sin comentarios)

Información general

Título: Proceso de Reprocesamiento

Descripción: Proceso de Reprocesamiento

Iniciado por: Administrator Vencimiento: (Ninguno) Completada: <en curso>

Iniciado: Vie 5 Sep 2014 16:52:06 Prioridad: Media Estado: Flujo de trabajo en curso

Mensaje: 2da Hoja Rotar

Pedido de reindexacion

Mensaje: 2da Hoja Rotar

Reindexacion: No

Redigitalizar: Si

Cambiar Tipo a: (Ninguno)

Figura N° 19 - Pantalla de resumen del flujo de trabajo en Alfresco

En la carpeta de “Trabajos Finalizados” puede verse la aprobación firmada digitalmente de AIT, del tutor y alumnos.



The screenshot displays the Alfresco document library interface. The top navigation bar includes 'IUA', 'Panel de inicio del sitio', 'Biblioteca de documentos', and 'Miembros'. The left sidebar contains navigation options: 'Documentos' (with sub-options like 'Todos los documentos', 'Que estoy editando', etc.), 'Biblioteca' (with sub-options like 'Documentos', 'Proyectos_Finalizados', etc.), 'Categorías', and 'Etiquetas'. The main content area shows a list of three PDF documents:

- Aprobacion_AIT_Estado-de-Cuenta_Carlos Tapia, Fernando Boiero.pdf**
Creado hace 3 minutos por ait ait 44 KB
Sin descripción
Sin etiquetas
Interactions: Favorito, Me gusta 0, Comentario, Share
- Aprobacion_Dpto.Alumnos_Situacion-Academica_Carlos Tapia, Fernando Boiero.pdf**
Creado hace 13 minutos por dpto alumnos 44 KB
Sin descripción
Sin etiquetas
Interactions: Favorito, Me gusta 0, Comentario, Share
- TrabajoFinal_Carlos Tapia, Fernando Boiero_1234536 78999933.pdf**
Creado hace 16 minutos por tutor tutor 270 KB
Sin descripción
Sin etiquetas

Figura N° 20 - Listado de documentos firmados en el flujo de Alfresco

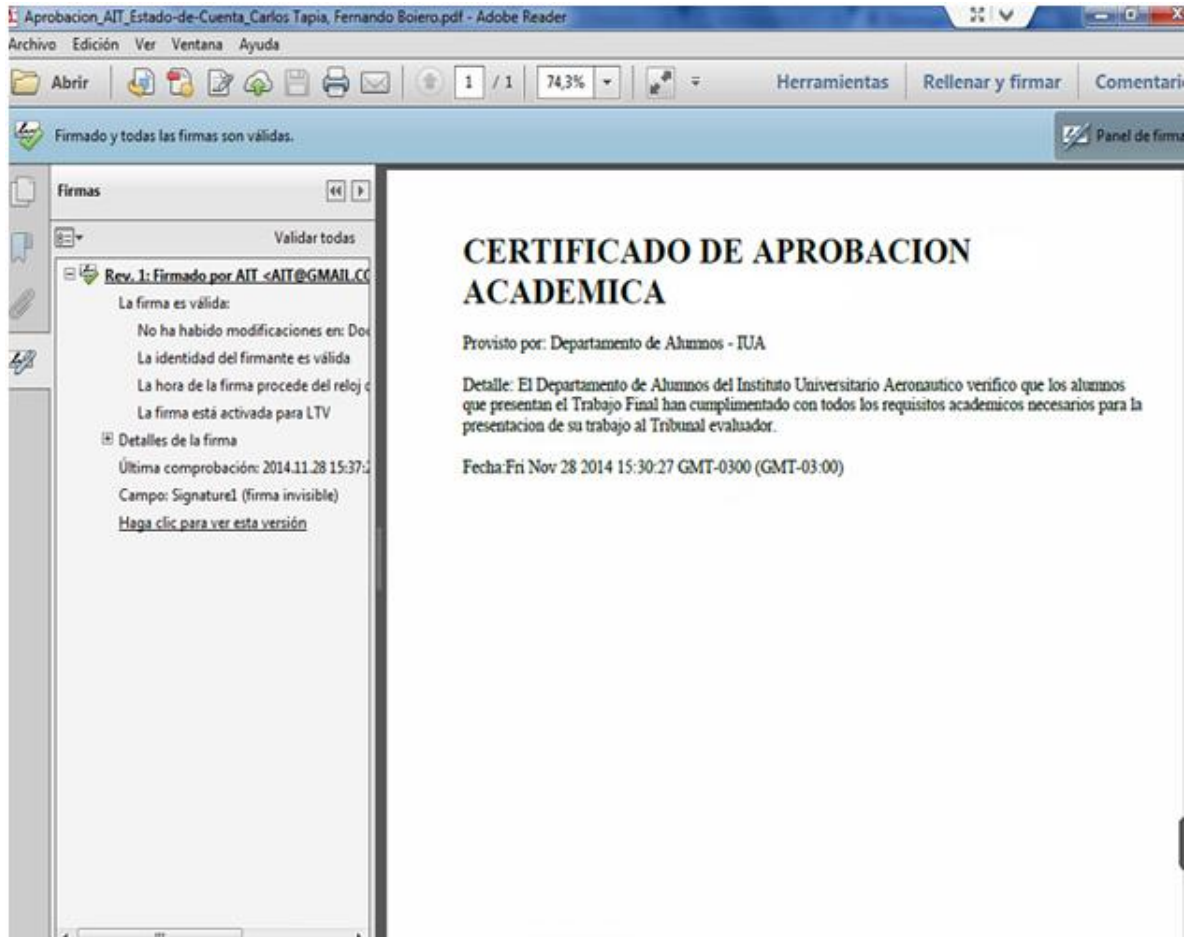


Figura N° 21 - Recibo de firma auto-generado en Alfresco al firmar

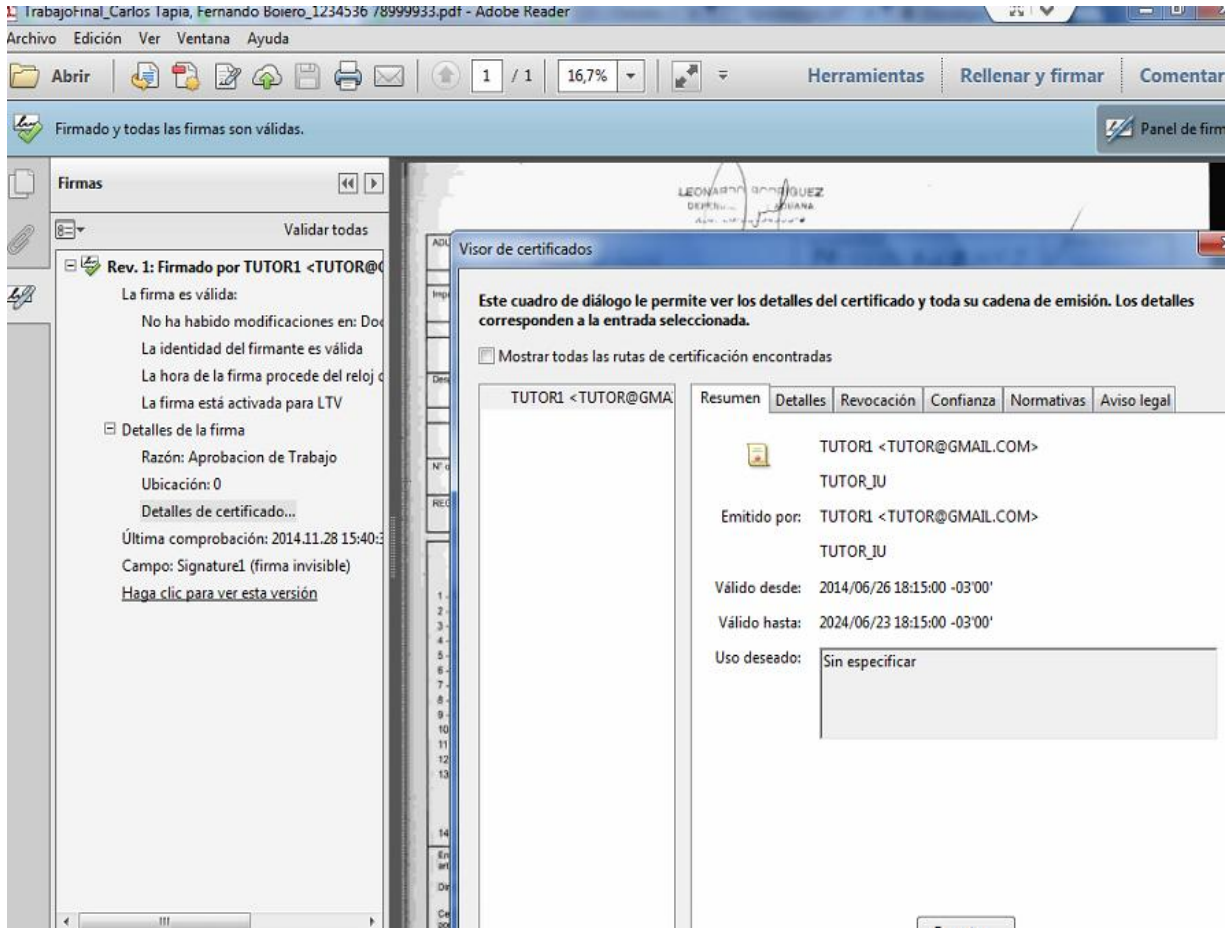


Figura N° 22 - Corroboración de la Firma Digital en el documento

En relación al hardening de seguridad de la plataforma de Alfresco, se efectuó una instalación segura de dicho sistema en su versión Community 4.02. Adicionalmente, agregando la protección del firewall web y dividiendo la implementación en distintos servidores virtuales, se consiguió una implementación aún más reforzada, estable y escalable que eran algunas de las consignas prefijadas al comenzar el trabajo.



10. CONCLUSIÓN

El presente trabajo mostró como es posible efectuar el hardening de un Sistema de Gestión Documental.

Asimismo, también fue posible mostrar el funcionamiento de los workflows dentro de Alfresco, que en conjunción con una infraestructura PKI, entregarían la posibilidad de firma electrónica.

Al modelar un proceso particular y sus actores sobre estas soluciones validamos lo enunciado, consiguiendo alcanzar la seguridad, trazabilidad, estabilidad y escalabilidad buscadas. De esta manera fue posible aplicar los distintos conocimientos adquiridos a lo largo de las materias de la Especialización, mostrando en la práctica las mejoras de seguridad y trazabilidad dadas a partir de la inclusión de las estas tecnologías y plataformas que garantizan el cumplimiento de los principios esenciales de la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

El trabajo desarrollado es adaptable a muchos ámbitos, y puede ser de interés para muchas entidades y compañías que actualmente llevan a cabo sus procesos de manera manual o mixta, especialmente aquellas que cuenten con filiales o sucursales dispersas geográficamente, o que necesiten una forma segura de acreditar sus transacciones electrónicas a un actor determinado. En este caso, el proyecto cobra mayor potencial teniendo en cuenta las distancias geográficas cubiertas por el IUA y sus centros académicos a lo largo del país y Uruguay, observando gran aplicabilidad y expansión hacia futuro.



11. TRABAJOS FUTUROS

Ya habiendo realizado una implementación inicial Alfresco, el trabajo a futuro para mejorar las presentes propuestas es:

- Conjunción completa con la implementación de una PKI a los efectos de poder efectivamente aprovechar al máximo ambas tecnologías.
- Incorporación gradual de más procesos internos del IUA para utilizar estas tecnologías, desplazando la utilización del teléfono y el e-mail.
- Incremento en la documentación de los procesos, para facilitar la adaptación de los usuarios a los mismos.
- Lograr apoyo de las máximas autoridades del IUA para difundir la utilización de estas tecnologías entre los usuarios.
- Organizar reuniones de capacitación con los usuarios para entrenarlos en la utilización de las herramientas y explicar los fundamentos y beneficios.
- Impulsar o participar en el desarrollo de nuevas herramientas de software que funcionen en la arquitectura propuesta.



12. REFERENCIAS BIBLIOGRÁFICAS

- [01]** OWASP, OWASP Documentation, 2014
<http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf>
Fecha de consulta: Julio 2014
- [02]** Alfresco Software, Alfresco Documentation, Alfresco Community 5.0, 2014 [https:// docs.alfresco.com/](https://docs.alfresco.com/)
Fecha de consulta: Junio 2014
- [03]** Nuxeo, Nuxeo Documentation Center Home - Installation, 2014
<http://doc.nuxeo.com/display/ADMINDOC/Installation>
Fecha de consulta: Julio 2014
- [04]** José Pereira, Proxy Security para Apache y Alfresco, 2011
<http://www.jpereira.net/gestion-documental/alfresco-y-apache-proxy-security>
Fecha de consulta: Agosto 2014
- [05]** Scott Mead, OpenSCG, 2013
<http://www.openscg.com/wp-content/uploads/2013/04/SecurityHardeningPostgreSQL.pdf>
Fecha de consulta: Agosto 2014
- [06]** Apache Project, Documentación de Tomcat Apache, 2014
<http://tomcat.apache.org/tomcat-7.0-doc/security-howto.html>
Fecha de consulta: Agosto 2014
- [07]** Blog Manuales-Linux, INSTALACIÓN DE POSTGRESQL – UBUNTU, 2013
<http://manuales-linux.blogspot.com.ar/2013/07/instalacion-de-postgresql.html>
Fecha de consulta: Agosto 2014



13. GLOSARIO

- **C++:** es un lenguaje de programación diseñado a mediados de los años 1980 por Bjarne Stroustrup. La intención de su creación fue el extender al exitoso lenguaje de programación C con mecanismos que permitan la manipulación de objetos. En ese sentido, desde el punto de vista de los lenguajes orientados a objetos, el C++ es un lenguaje híbrido.
- **Eclipse:** es un programa informático compuesto por un conjunto de herramientas de programación de código abierto multiplataforma para desarrollar lo que el proyecto llama "Aplicaciones de Cliente Enriquecido", opuesto a las aplicaciones "Cliente-liviano" basadas en navegadores. Esta plataforma, típicamente ha sido usada para desarrollar entornos de desarrollo integrados (del inglés IDE), como el IDE de Java llamado Java Development Toolkit (JDT) y el compilador (ECJ) que se entrega como parte de Eclipse (y que son usados también para desarrollar el mismo Eclipse).
- **Java:** es un lenguaje de programación de propósito general, concurrente, orientado a objetos que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible. Su intención es permitir que los desarrolladores de aplicaciones escriban el programa una vez y lo ejecuten en cualquier dispositivo (conocido en inglés como WORA, o "write once, run anywhere"), lo que quiere decir que el código que es ejecutado en una plataforma no tiene que ser recompilado para correr en otra. Java es, a partir de 2012, uno de los lenguajes de programación más populares en uso, particularmente para aplicaciones de cliente-servidor de web, con unos 10 millones de usuarios reportados.
- **NIST:** El Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), llamada entre 1901 y 1988 Oficina Nacional de Normas (NBS por sus siglas del inglés National Bureau of Standards), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida. Como parte de esta misión, los científicos e ingenieros del NIST continuamente refinan la ciencia de la medición (metrología) creando una ingeniería precisa y una manufacturación requerida para la mayoría de los avances tecnológicos actuales.
- **Open-source:** Código abierto es la expresión con la que se conoce al software distribuido y desarrollado libremente. Se focaliza más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre.
- **Perl:** es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado bourne shell



(sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

- **SQL**: El lenguaje de consulta estructurado o SQL (por sus siglas en inglés Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas.
- **Workflow**: flujo de trabajo (workflow en inglés) es el estudio de los aspectos operacionales de una actividad de trabajo: cómo se estructuran las tareas, cómo se realizan, cuál es su orden correlativo, cómo se sincronizan, cómo fluye la información que soporta las tareas y cómo se le hace seguimiento al cumplimiento de las tareas.



ANEXOS

ANEXO I: DETALLES DE INSTALACIÓN Y CONFIGURACIÓN DE ALFRESCO

- A. Primero se detalla la instalación del Sistema Operativo, en este caso el elegido fue GNU/Linux en su distribución CentOS usando la versión 6.5.
- B. Se realiza una instalación mínima configurando la red según lo que se detalló en el punto 4.1
- C. A modo de evidencia, se incorporan las pantallas de la instalación pertinentes:

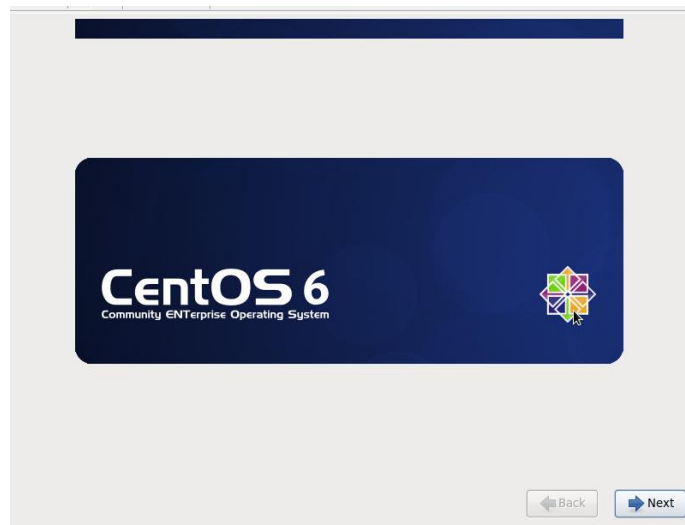


Figura N° 23 – Pantalla inicial de intalación de CentOS 6

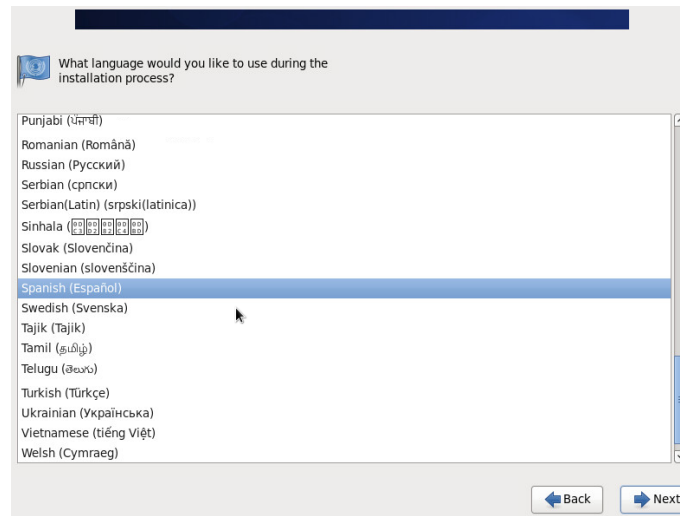


Figura N° 24 – Selección de idioma en la instalación de CentOS 6

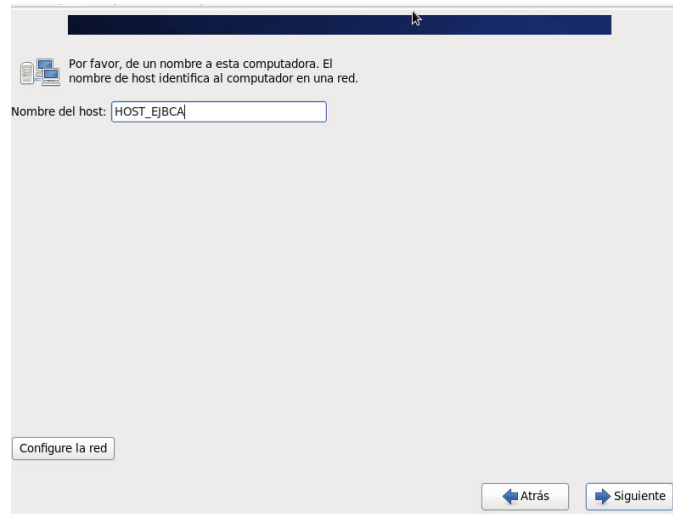


Figura N° 25 – Elección del hostname para la máquina

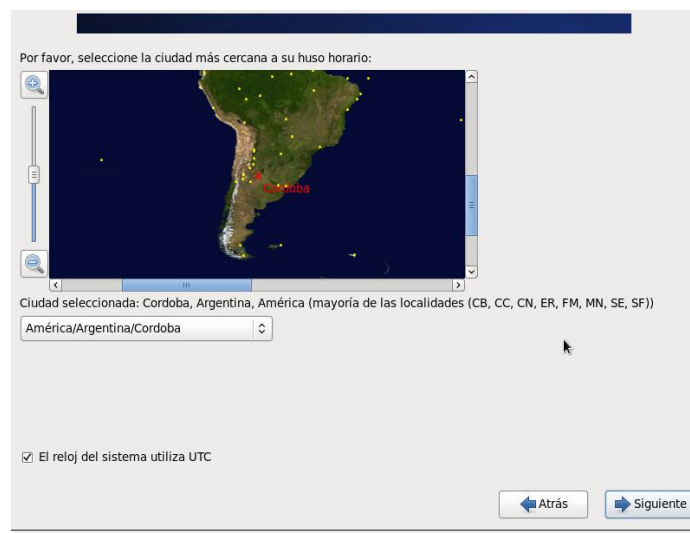


Figura N° 26 – Elección del huso horario

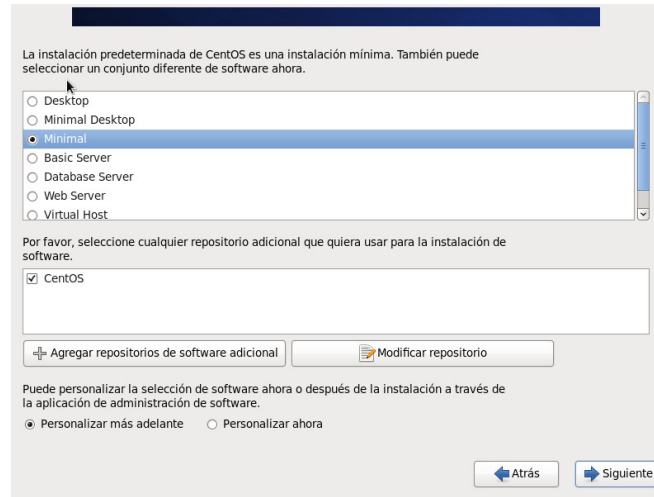


Figura N° 27 – Selección del tipo de instalación

D. Al finalizar la instalación del sistemas operativo se ingresa a la máquina virtual y con derechos de administrador se ejecutan los siguiente comandos para instalar Alfresco:

```
[root@sgd01 opt]# chmod +x alfresco-community-4.2.c-installer-linux-x64.bin  
[root@sgd01 opt]# ./alfresco-community-4.2.c-installer-linux-x64.bin
```

Figura N° 28 – Comando de instalación de Alfresco

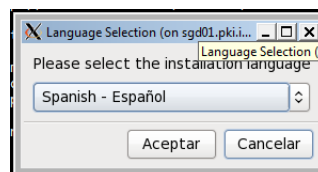


Figura N° 29 – Lenguaje de instalación de Alfresco



Figura N° 30 – Pantalla de bienvenida de instalación de Alfresco

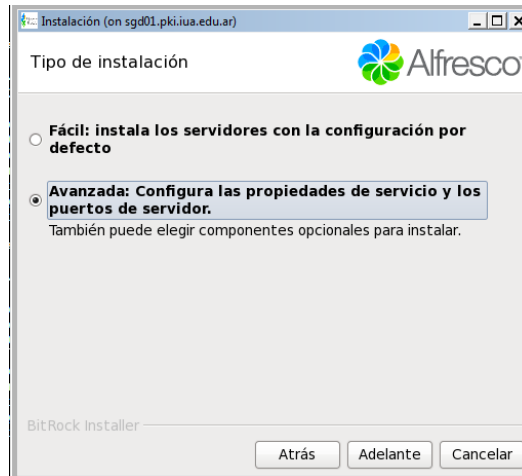


Figura N° 31 – Elección del tipo de instalación de Alfresco

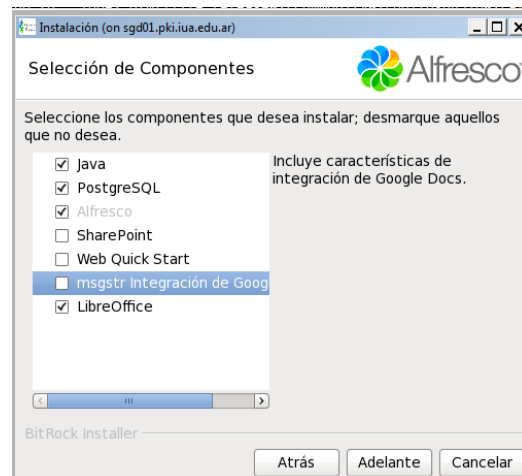


Figura N° 32 – Selección de componentes a instalar en Alfresco

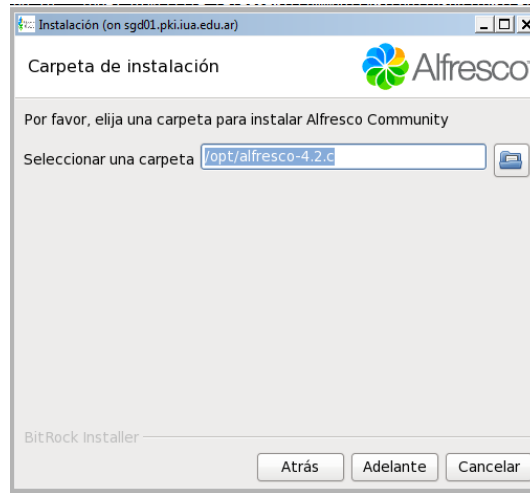


Figura N° 33 – Elección del directorio de instalación para Alfresco



Figura N° 34 – Configuración de Tomcat



Figura N° 35 – Confirmación de la instalación finalizada



- E. Se descargan los AMP del PDF Toolkit y se copian a la carpeta de instalación de AMP de Alfresco y de Share:

```
cp alfresco-share-pdf-toolkit-1.1.1.amp /opt/alfresco/amps
alfresco-share-pdf-toolkit-1.1.1.amp /opt/alfresco/amps_share
```

- F. Se aplican los AMP para que se integren.

```
[root@sgd01 bin]# ./apply_amps.sh
This script will apply all the AMPs in amps and amps-share to the
alfresco.war and share.war files in /opt/alfresco-
4.2.c/tomcat/webapps
Press control-c to stop this script . . .
Press any other key to continue . . .
```

```
Module 'de.fme.alfresco.JavascriptConsole-repo' installed in
'/opt/alfresco-4.2.c/tomcat/webapps/alfresco.war'
```

- Title: fme Javascript Console Repository Extension
- Version: 0.5
- Install Date: Fri Nov 28 17:46:43 ART 2014
- Description: Administration console module to execute arbitrary javascript code.

```
Module 'org.alfresco.extension.pdf toolkit' installed in '/opt/alfresco-
4.2.c/tomcat/webapps/alfresco.war'
```

- Title: Alfresco PDF Toolkit
- Version: 1.1.0
- Install Date: Fri Nov 28 17:46:38 ART 2014
- Description: Alfresco PDF Toolkit adds additional functionality to Alfresco allow you to work with PDF files.

```
Module 'de.fme.alfresco.JavascriptConsole-share' installed in
'/opt/alfresco-4.2.c/tomcat/webapps/share.war'
```

- Title: fme Javascript Console Share Extension
- Version: 0.5
- Install Date: Fri Nov 28 17:46:57 ART 2014
- Description: Administration console module to execute arbitrary javascript code.



Module 'alfresco-share-pdf-toolkit' installed in '/opt/alfresco-4.2.c/tomcat/webapps/share.war'

- Title: Alfresco PDF Toolkit Share Extensions
- Version: 1.1.1.83
- Install Date: Fri Nov 28 17:46:53 ART 2014
- Description: Alfresco PDF Toolkit Share Extensions

About to clean out /opt/alfresco-4.2.c/tomcat/webapps/alfresco and share directories and temporary files...

G. Se descarga e instala el componente wkhtmltox.

```
[root@sgd01 opt]# wget
```

```
http://downloads.sourceforge.net/project/wkhtmltopdf/0.12.1/wkhtmltox-0.12.1_linux-centos6-amd64.rpm
```

```
[root@sgd01 opt]# rpm -i wkhtmltox-0.12.1_linux-centos6-amd64.rpm
```

H. Configuration de reglas Firewall:

Forwarding (redirecciones)

- Se agrega la redirección del puerto de ingreso 80 al puerto local 8080 para el protocolo TCP
- Se agrega la redirección del puerto de ingreso 442 al puerto local 8442 para el protocolo TCP
- Se agrega la redirección del puerto de ingreso 443 al puerto local 8443 para el protocolo TCP



```
vi /etc/sysconfig/iptables.
*mangle
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -i eth0 -p tcp --dport 80 -j MARK --set-mark 0x64
-A PREROUTING -i eth0 -p tcp --dport 442 -j MARK --set-mark 0x65
-A PREROUTING -i eth0 -p tcp --dport 443 -j MARK --set-mark 0x66
COMMIT
*nat
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -i eth0 -p tcp --dport 80 -m mark --mark 0x64 -j DNAT --to-destination :8080
-A PREROUTING -i eth0 -p tcp --dport 442 -m mark --mark 0x65 -j DNAT --to-destination :8442
-A PREROUTING -i eth0 -p tcp --dport 443 -m mark --mark 0x66 -j DNAT --to-destination :8443
COMMIT
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 8080 -m mark --mark 0x64 -j
ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 8442 -m mark --mark 0x65 -j
ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 8443 -m mark --mark 0x66 -j
ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 442 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
service iptables reload
```




ANEXO II: DISEÑO DE WORKFLOWS EN ALFRESCO

Para el diseño de los workflows se utilizaron las siguientes herramientas y complementos:

- Eclipse como IDE de desarrollo.
- Plugin Activiti Eclipse (<http://activiti.org/designer/beta>) - Descargar desde la instalación de plugins de Eclipse (Help/Install New Software). Este plugin, a diferencia del básico (<http://activiti.org/designer/update>) permite crear uno o varios modelos para flujos de trabajo de una manera más intuitiva. Esto creará los .xml necesarios además del diagrama de la primera versión del diseñador.
- wkhtmltopdf - Conversor HTML a PDF – Se lo instaló y se agregaron las variables de entorno en el servidor donde se encuentra Alfresco.

A continuación, se repasa el procedimiento utilizado, una vez instalado el plugin Activiti, desde Eclipse:

1. Crear Proyecto Kickstart Project. (AprobacionTrabajo)
2. En scr/main/resources crear los diagramas: New/Other/Kickstart/Kickstart Process Diagram
3. Los formularios se pueden crear de forma independiente del diagrama de proceso.
4. Finalmente cada tarea de usuario (Human Task) en el diagrama deberá tener un formulario asociado. Si se selecciona una de estas tareas, en una opción abajo a la derecha (Select or create form...) permite seleccionar algún formulario creado o crear un nuevo.
5. Cada Step, deberá tener algún usuario asociado y deberá definir si es fin del flujo o no.
6. Una vez finalizado el flujo básico se deberá exportar (click derecho en el diagrama/ Export/ Kickstart/ Kickstart Process, y si se requiere personalizar, seleccionar Project target folder o Custom location). De no producirse errores, deberían generarse todos los archivos necesarios (Proceso, Modelo, Contexto, Formularios).
7. Si se escogió por ejemplo Project target folder, podremos encontrar estos archivos en la carpeta target al nivel de src. Si se abre el archivo AprobacionTrabajo.bpmn20 desde Eclipse (Open With/Other/Activiti Diagram Editor), se podrá observar el flujo como se vería si hubiese sido creado con el diseñador básico de Activiti.



8. Cada paso del flujo, debería estar asociado a un formulario (Main Config/Form Key). Estos formularios se corresponden con un modelo de datos generado, un iniciador del flujo o usuario/grupo candidato asignado (Main Config/Assignee).
9. El flujo estará listo para modificar y personalizar con parámetros avanzados. Se deberán copiar los cuatro archivos básicos (Proceso, Modelo, Contexto, Formularios) encontrados dentro en target/ repo y target/ share. Del directorio share, el archivo importante es Aprobación Trabajo - config-custom.xml, donde el contenido se copiará a share-config-custom.xml de extensión dentro de la carpeta shared para poder visualizar los formularios.
10. De aquí en más se deberán crear scripts dentro de los procesos, realizar cambios con las asignaciones de grupo o usuario. Básicamente para lograr esto se deben ajustar las variables generadas para los formularios (sólo se ve en el ámbito del script de la tarea de ese formulario) y establecer variables de ejecución (que serán vistas a lo largo de todo el flujo). Además, se deberán ver definiciones de script en create, take y complete. Por otra parte, se puede crear una clase, y con el SDK de Alfresco crear un script delegado a esa clase.

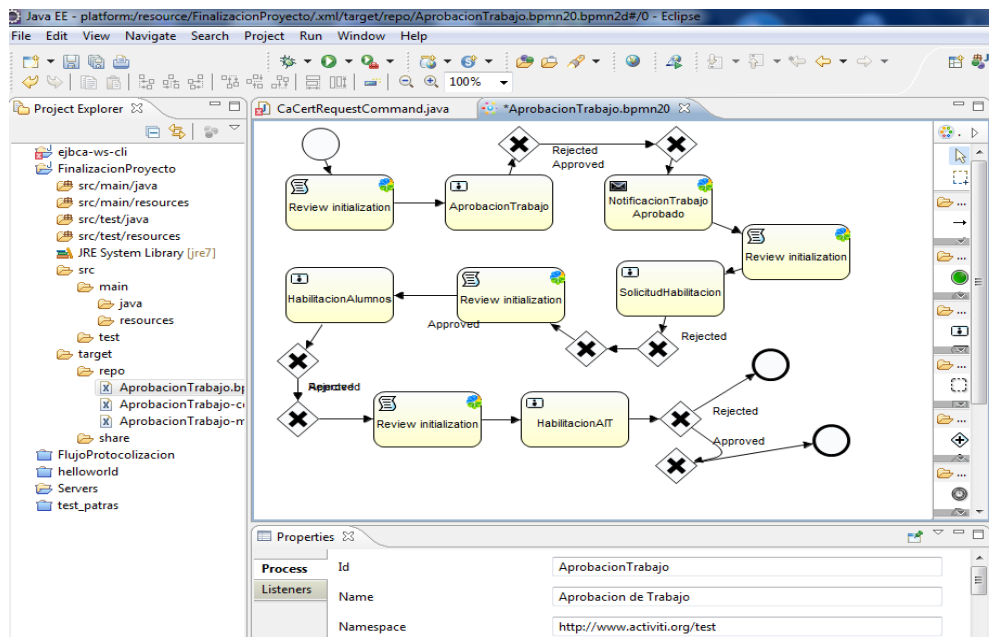


Figura N° 36 – Diagrama de flujo en Eclipse

11. Copiar el Modelo, Proceso, Contexto a extensión de la carpeta de Alfresco.



12. Iniciar la consola de workflow de Alfresco: `http:// IP: PUERTO/ alfresco/faces/ jsp/ admin/ workflow-console.jsp`
13. Mostrar definiciones de workflows: `show all definitions`
14. Si no se encuentra, efectuar el deploy: `deploy activiti alfresco/ extension/ AprobacionTrabajo.20bpm.xml`
15. Debería poder verse desde share y poder iniciar un flujo.



DATOS PERSONALES DE LOS ALUMNOS

Apellidos y nombres: Tapia, Carlos Ignacio.

Documento de identidad: D.N.I. 28.657.987.

E-mail: carlosignaciotapia@gmail.com

Firma: