PROPUESTA PARA LA IMPLEMENTACIÓN DE UNA ENTIDAD CERTIFICADORA LOCAL PARA LA ADMINISTRADORA DE PENSIONES Y RÉGIMEN DE PRIMA MEDIA COLPENSIONES

JUAN CARLOS NAVARRO CASTILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2019

“PROPUESTA PARA LA IMPLEMENTACIÓN DE UNA ENTIDAD CERTIFICADORA LOCAL PARA LA ADMINISTRADORA DE PENSIONES Y RÉGIMEN DE PRIMA MEDIA COLPENSIONES”

INTEGRANTES:

JUAN CARLOS NAVARRO CASTILLA

TRABAJO DE GRADO PARA OBTENER EL TÍTULO DE ESPECILISTA EN SEGURIDAD INFORMÁTICA

TUTOR:

ING. CHRISTIAN ANGULO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
FACULTAD DE INGENIERIA DE SISTEMAS
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2019

Nota de aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá, abril 2019

Contenido

Página

LISTA DE TABLAS

Página

LISTA DE FIGURAS

Página

ANEXOS

Página

1. GLOSARIO

Este proyecto describirá términos técnicos referentes a certificados digitales y entidades certificadoras que permiten la ejecución del trabajo que se describirá más adelante.

El glosario que se utilizará a lo largo del proyecto es:

Active Directory Certifícate Servicess: El active Directory Certificate Servicess es el rol del sistema Windows que permite configurar una entidad certificadora o CA dentro de un dominio determinado.

Certificado Digital: Un certificado digital es un archivo electrónico el cual posee una firma reconocida por otras entidades como legítimo y que le da validez y legalidad a los documentos que estén firmados por este.

Entidad de certificación o CA: Es una organización o sistema que proporciona certificados digitales con reconocimiento y aceptación reconocidos por un grupo. Una entidad certificadora local proporciona certificados digitales aceptados dentro de un dominio u organización únicamente, mientras que una CA externa entrega certificados digitales reconocidos por la comunidad de internet completa.

Infraestructura de llave pública o pki: Una pki es el conjunto de todos los elementos de hardware y software que componen un sistema de llaves y cifrado de información como lo son la entidad certificadora, los certificados digitales, los algoritmos de encripción de datos y el sistema de uso y generación de certificados digitales.

Internet Information service: Es el sistema de publicación de páginas web proporcionado por Windows, se conoce más comúnmente por sus siglas en inglés iis, el iis es el módulo o funcionalidad de Windows que permite alojar y publicar una página web dentro de un servidor configurado en sistema operativo Windows.

Protocolo http: El protocolo http, es un protocolo usado por internet para permitir la transferencia de información entre sitios web y usuarios finales, este protocolo de información no encripta la información y es posible capturar datos importantes con solo aplicar un analizador de red en el medio de transmisión.

Protocolo https: El protocolo https, es un protocolo de transferencia de datos entre los sitios web y los usuarios, la diferencia con el http es que el https se cifra a través de certificados digitales y no es posible ver la información que viaja dentro de la red de forma sencilla. -el protocolo https permite dar seguridad a la información que viaja en la red a los sitios que se publiquen con esta modalidad segura.

Rol o característica de Windows server: Un rol de Windows server, es una función específica que se encarga de realizar una actividad específica, un servidor de Windows server se puede configurar como un servidor de aplicaciones web, un servidor de directorio activo, un servidor de archivos entre otros, cada función de las nombradas corresponde a un rol de servidor.

Servidor de Aplicaciones Web: Un servidor de aplicaciones web es aquel servidor que se configura como máquina que despliega y aloja sitios o aplicaciones accesibles a través de un navegador web, generalmente usando como medio de conectividad la internet o la red de datos de una organización o empresa.

Servidor Virtual: Es una parte o fracción de una máquina física que tiene un sistema operativo propio y que comparte recursos de hardware con otros sistemas operativos que actúan como máquinas virtuales y su comportamiento es como el de una máquina física y funcionando simultáneamente.

Windows server 2012 r2: Es un sistema operativo diseñado para servidores que proporciona funciones o roles específicos de acuerdo con el trabajo que se le tenga destinado. Windows requiere de licenciamiento por parte del fabricante y es uno de los sistemas operativos más utilizado.

2. RESUMEN DEL PROYECTO

En este trabajo, se dará a conocer la necesidad que tiene la administradora estatal del régimen de prima media Colpensiones de solucionar un hallazgo de seguridad encontrado en una auditoría de seguridad de la información realizada recientemente. El problema encontrado, radica en que la transmisión de datos de las aplicaciones web se hace en protocolo http, esto significa que los datos que viajan sobre la red pueden ser revisados y capturados por un analizador de red o una técnica básica de ingreso no permitido dentro de la red de Colpensiones.

Un atacante, utilizando un analizador de red como Wireshark, podría obtener datos de usuarios y contraseñas de acceso o información importante como identificaciones y estado de casos de los ciudadanos.

La mayoría de las aplicaciones de la empresa son web, y no se tiene contemplado en el presupuesto un rubro para la compra de certificados digitales de una entidad certificadora externa y de esta manera cifrar las aplicaciones para dar solución al hallazgo encontrado.

Por el motivo anterior, además del hallazgo encontrado, se tiene un nuevo problema de presupuesto para poder dar una solución al problema de publicación insegura de las aplicaciones.

Para solucionar el problema descrito anteriormente, se propone en este trabajo, la implementación de una entidad certificadora local, que permita crear certificados digitales con el fin de publicar sitios web seguros basados en el protocolo https.

Con la puesta en marcha de una entidad certificadora, se podrán publicar de forma cifrada las aplicaciones web de la compañía, la información que viaja en estas aplicaciones estará encriptada y no se podrá detectar por un atacante, con este proyecto se solucionará un problema importante de seguridad de la información que fue detectado por la auditoría sin tener necesidad de comprar certificados digitales

a una entidad certificadora externa generando un ahorro importante en el presupuesto de la gerencia de TI de la empresa.

El proyecto propuesto, pretende entregarle a Colpensiones un sistema completo para proteger las aplicaciones web que actualmente están publicadas de forma insegura, este proyecto estará en capacidad de crear certificados digitales que se instalarán en los servidores de cada aplicación y permitir que las páginas web de los aplicativos se puedan publicar en protocolo seguro cifrando de punta a punta el acceso a cada aplicación.

Después de tener en funcionamiento el proyecto, Colpensiones pasará de tener aplicaciones web inseguras en http a publicaciones seguras y cifradas publicadas en https solucionando una vulnerabilidad importante en la seguridad de la información de los sistemas de la compañía.

Al tener instalada la entidad certificadora local, además de solucionar fallas de seguridad en la información, no será necesario comprar certificados digitales para las aplicaciones locales, pues la empresa estará en capacidad de generar sus propios certificados digitales y proteger las páginas actuales y las que se vayan creando.

En este trabajo describirán los conceptos básicos sobre el significado de una entidad certificadora local, los certificados digitales para páginas web y algunos de los métodos que existen para la creación de una entidad certificadora o CA como es conocida por sus siglas en inglés.

También se tratará el tema de tipos de entidades certificadoras, marco legal colombiano que regula algunos de los delitos más relevantes a nivel de seguridad de la información y la forma como se implementará la entidad certificadora de Colpensiones partiendo de un servidor virtual basado en Windows 2012 r2 y aprovechando el rol de entidad certificadora que proporciona este sistema operativo.

3. INTRODUCCIÓN

Colpensiones es la empresa del estado que administra el régimen pensional a nivel nacional siendo competidor directo de los fondos privados de pensiones. La información que se maneja en esta compañía es privada y muy sensible para los ciudadanos afiliados. Es de vital importancia que el estado brinde protección a esta información para garantizar su uso correcto, es por lo anterior que se realizan auditorías periódicas con el objetivo de identificar posibles vulnerabilidades y dar la solución correcta a estas.

Debido a la importancia de la información que maneja la compañía, se hace necesario crear un sistema que codifique la información de aplicaciones web locales que viajan en la red de Colpensiones y que esta información no se pueda capturar y decodificar de una forma simple. Actualmente, la empresa tiene aplicaciones web para desarrollar los diferentes procesos que se llevan a cabo en la compañía. Estas aplicaciones no se encuentran aseguradas y son un blanco relativamente fácil para un atacante que podría capturar información sensible de los ciudadanos y colaboradores de la compañía.

Por lo anterior, se propone la creación de una entidad certificadora local que permita el cifrado, aseguramiento y publicación segura de las aplicaciones que utiliza Colpensiones a través de certificados digitales válidos dentro del dominio de la empresa y de sus proveedores.

Al poder usar una entidad certificadora local, Colpensiones estará en capacidad de generar sus propios certificados digitales para proteger las aplicaciones sin necesidad de realizar compras a entidades certificadoras externas, esto significa que la implementación de esta entidad certificadora, adicional a proporcionar un entorno cifrado y difícil de capturar, también permite generar una cantidad ilimitada de certificados locales con lo que la compañía ahorrará en términos económicos al

tener que comprar en menor cantidad certificados a entidades de certificación pública.

Colpensiones actualmente, tiene publicadas las aplicaciones web de la compañía publicadas en protocolo inseguro y esto significa que la información que viaja a través de estas aplicaciones está expuesta y podría ser fácilmente extraíble por un atacante que logre ingresar a la red o por algún funcionario que tenga conocimientos medianos sobre sistemas de la información.

El área de Tecnologías de Información encontró esta vulnerabilidad en la seguridad de la información, después de una auditoría realizada por una empresa externa contratada por el área de riesgos.

La forma de mitigar este error fue la propuesta de cifrar y publicar de manera segura todas las aplicaciones web locales que usa la compañía en sus diferentes procesos.

4. TÍTULO

PROPUESTA PARA IMPLEMENTAR UNA ENTIDAD CERTIFICADORA LOCAL PARA COLPENSIONES.

5. ANTECEDENTES DEL PROBLEMA

Colpensiones es la empresa administradora de régimen de prima media de Colombia, para llevar a cabo su misión esta empresa maneja una infraestructura tecnológica bastante robusta y compleja la cual es apoyada por proveedores y colaboradores.

Colpensiones tiene sitios públicos como el portal institucional y el portal transaccional, estas aplicaciones web están protegidas por certificados digitales de última generación y emitidos por una entidad certificadora externa representada por Certicámara en Colombia. Estos portales están bien protegidos y cuentan con diversos y complejos mecanismos de seguridad que mitigan el posible ataque que un hacker pueda realizar.

Dentro de todos los procesos que tiene Colpensiones, existen algunos de control que evalúan permanentemente el estado de seguridad de las aplicaciones implementadas, por este motivo se contratan auditorías para todas las áreas de la compañía con el objetivo encontrar fallas y verificar el correcto funcionamiento de los procesos.

En una auditoría, la cual incluyó una prueba de vulnerabilidad realizada recientemente, se detectó que las aplicaciones web externas de Colpensiones están protegidas y funcionando bajo los lineamientos de leyes y buenas prácticas establecidas, pero las aplicaciones web locales están publicadas en protocolo inseguro y presentan un hallazgo importante la seguridad de la información que circula a través de estos aplicativos.

El hallazgo encontrado significa una vulnerabilidad importante que podría afectar seriamente la permanencia de la empresa en caso de materializarse un ataque informático.

La solución propuesta para mitigar el riesgo encontrado es la publicación de las aplicaciones web locales de Colpensiones a través de protocolo seguro, garantizando el cifrado de los datos que viajan a través de estas por medio de certificados digitales.

Estos certificados digitales, serán creados localmente a través de una entidad certificadora local interna

.

6. DESCRIPCIÓN DEL PROBLEMA

En el momento de realizar los controles de auditoría para las aplicaciones web internas de la empresa, se encontró que, estas están publicadas en texto claro y pueden ser interceptadas de diferentes formas, esto se tradujo en un hallazgo de seguridad.

Estas aplicaciones, están exponiendo a un riesgo importante en la integridad de la información de los ciudadanos y afiliados en general a la ciudadanía, pues al ser atacado un sitio web de estos el atacante podrá obtener información privada de los ciudadanos para ser utilizada con fines delictivos con los graves perjuicios que esto puede causar.

Para poder resolver un problema de este tipo, es necesario cifrar las aplicaciones expuestas y publicarlas a través de protocolos seguros, estas acciones implican la utilización de certificados digitales que encripten los datos para protegerlos de los ataques que puedan sufrir en un momento determinado. Estos certificados usualmente deben ser adquiridos a entidades certificadoras externas que avalan la originalidad y seguridad de una aplicación web.

En la actualidad no se tiene contemplada la compra de certificados digitales con entidades externas para proteger las aplicaciones web de Colpensiones y las páginas web se están publicando bajo protocolo http en texto claro, y debido a esto el transporte de información por las redes de datos se realiza de manera clara y sin mecanismos de encripción, dejando abierto el riesgo de fuga de información sensible de los ciudadanos afiliados o no afiliados al sistema en un eventual ataque informático.

Para poder publicar por el protocolo seguro https se necesitan certificados de seguridad, y por la cantidad de aplicaciones existentes es costoso tener que

comprar dichos certificados a una entidad certificadora externa, teniendo en cuenta que las aplicaciones son internas o de ambientes no productivos, para asegurarlas no es necesario adquirir certificados de una entidad certificadora siempre y cuando Colpensiones esté en capacidad de generar sus propios certificados locales desde una entidad certificadora propia.

Al implementar una entidad certificadora local, la empresa podrá cifrar todas las aplicaciones web internas.

7. FORMULACIÓN DEL PROBLEMA

Una vez descrito lo anterior se puede identificar claramente que Colpensiones no tiene una entidad certificadora local para emitir sus propios certificados digitales para ser aplicados en las aplicaciones web internas que se manejan, y debido a esto la información viaja en texto claro y de forma insegura.

Después de tener claro el panorama de la seguridad de las aplicaciones web locales, se puede plantear el problema de la siguiente manera:

¿Puede la implementación de una entidad certificadora local, solucionar los problemas de seguridad de publicación en texto claro de las aplicaciones web de la administradora nacional de pensiones y régimen de prima media de Colombia Colpensiones?

8. JUSTIFICACION

Colpensiones es la administradora estatal de pensiones de Colombia, la información que se maneja en sus sistemas tecnológicos es de vital importancia para todos los ciudadanos que tienen sus ahorros y esperanzas de una pensión digna cuando lleguen a su vejez y para aquellos pensionados que ya disfrutan de su retiro, la adulteración, manipulación o pérdida de datos para estas personas podría ocasionar un grave daño a su estilo de vida.

Actualmente, la administradora de pensiones y régimen de prima media de la república de Colombia Colpensiones publica las aplicaciones web de los ambientes de integración, calidad, y algunos de producción en texto claro y bajo protocolo http, por la razón anterior se tiene una vulnerabilidad de seguridad que un atacante podría aprovechar para robar o alterar información importante de la compañía. Adicional a la razón anterior en un reciente informe de auditoría se encontró como hallazgo crítico de seguridad la publicación de algunas aplicaciones en http y se requiere dar solución a la problemática encontrada, también se tiene la dificultad de no contar en la actualidad con una asignación presupuestal para comprar certificados digitales con un certificador externo.

Al utilizar las aplicaciones en texto claro se está corriendo un riesgo crítico exponiendo datos de vital importancia de los ciudadanos afiliados y pensionados, pues si se llegara a presentar un fraude vendrían las demandas y las indemnizaciones económicas que al final todos los colombianos a través de los impuestos terminarían pagando.

Se propone por las razones anteriores, la creación de una entidad certificadora local que permita que los sitios vulnerables de la empresa se puedan publicar en protocolo https eliminado las vulnerabilidades encontradas.

Con la implementación de este proyecto, la empresa avanza técnicamente para cerrar la brecha entre fallas de seguridad encontradas protegiendo la valiosa información de los ciudadanos colombianos, esta entidad certificadora se construirá con los más altos estándares y recomendaciones del fabricante de software para proporcionar una plataforma robusta y de calidad que pueda proporcionar la confianza necesaria para transferir información de los ciudadanos, a través de aplicaciones web bajo sitios seguros.

Con la creación de la entidad certificadora local de Colpensiones se está beneficiando la entidad por encriptar los datos vitales de sus afiliados y pensionados, pero también la ciudadanía en general tendría un beneficio al tener la tranquilidad de que Colpensiones maneja de forma reservada y segura la información personal.

Al tener esta entidad certificadora funcionando mejoraría la seguridad y protección de datos, lo que beneficiaría a la toda la comunidad en general, pues se correrían menos riesgos de fraudes y pagos por parte del estado de millonarias indemnizaciones.

Con la implementación del proyecto, los datos que viajan en texto claro y de una forma insegura y fácil de interceptar, podrán ser cifrados de origen a destino y no será fácil su captura, la información estará codificada por medio de certificados digitales generados por la propia compañía.

Adicional a crear una plataforma de cifrado para el transporte seguro de la información de las aplicaciones web locales, Colpensiones estará realizando un ahorro económico importante en el presupuesto, pues los certificados digitales para dichas aplicaciones se generarán por la propia empresa y no se necesitará comprarlos.

Colpensiones, al implementar el proyecto propuesto, mitigará y reducirá los riesgos generados por vulnerabilidad de seguridad de la información de una manera significativamente importante, pues se pasará de tener la información de las aplicaciones web locales expuesta y fácil de extraer por ataques internos o externos, a información cifrada y protegida a través de certificados digitales y publicada en protocolo seguro de extremo a extremo haciendo muy difícil su captura.

Este proyecto, permitirá que Colpensiones empiece a publicar por puerto seguro y de forma cifrada la información de las aplicaciones web significando esto un avance importante en la seguridad de la información que circula por la red de la empresa

9. ALCANCE Y LIMITACIONES DEL PROYECTO

Este proyecto pretende crear una entidad certificadora local construida en Windows 2012 r2 tomando como base el rol de entidad certificadora que trae este sistema operativo.

Los certificados que se generarán estarán destinados a proteger los sitios web de la empresa, por lo tanto, la plantilla principal de la entidad certificadora será la conocida como plantilla de certificado web.

El proyecto se encargará de la emisión del certificado raíz de la propia entidad certificadora, y la emisión de certificados web con requerimientos de nombre alternativo generados mediante las opciones personalizadas de la consola de generación de certificados que proporciona Windows.

El sistema de entidad de certificación local de Colpensiones no emitirá certificados de protección a documentos y correo electrónico.

El sistema se desarrollará completamente en sistema operativo Windows y bajo las recomendaciones de mejores prácticas de instalación del fabricante Microsoft.

Si bien los certificados generados podrán ser instalados en aplicaciones web residentes en sistemas operativos diferentes al sistema operativo windows, los requerimientos de certificado de estos sistemas operativos deberán acomodarse a los requerimientos de campos exigidos por la entidad certificadora local funcionando sobre Windows.

10. OBJETIVOS

10.1 OBJETIVO GENERAL

Implementar una entidad certificadora local que permita la generación de certificados ssl para publicación de sitios seguros que administren las aplicaciones web de Colpensiones sobre protocolo https.

10.1.2 OBJETIVOS ESPECÍFICOS

10.2.1 Configurar un servidor en plataforma de sistema operativo Windows con el rol de entidad certificadora y todas las configuraciones relacionadas a este.

10.2.2 Realizar pruebas previas sobre el estado actual de la publicación de aplicaciones web.

10.2.3 Definir el tipo de certificados digitales que mejor se adaptan a la compañía y sus aplicaciones web

11. MARCO REFERENCIAL

11.1 ESTADO DEL ARTE

Dentro del marco referencial, se nombrarán algunos proyectos de características similares al propuesto en este trabajo con los que se pretende dar una visión sobre la importancia que tiene una entidad de certificación local para la protección de las aplicaciones web de las empresas.

Tabla 1 Estado del arte con la comparación de proyectos similares

Referencia	Título	Institución/ País	Resumen
Miguel Solinas, Ricardo Justo Castello, Leandro Tula, Cesar Gallo, Javier Jorge, Daniel Bollo	Implementación de una infraestructura de clave pública con herramientas de software libre	Lab.de Arquitectura de Computadoras, FCEFyN, UNC, Av.Velez Sarsfield 1611, 5000 Córdoba, Argentina.	En este trabajo se relata el proceso de construcción de una infraestructura de clave pública, utilizando software libre, para una fase desarrollo y experimentación en el ámbito académico de la UNC.
Francisco Jesús Marchal Cebador	Creación de una autoridad certificadora de firmas digitales y servidor OCSP. Análisis de ataques MITM	Departamento Ingeniería Telemática Escuela Técnica Superior de Ingeniería Universidad de Sevilla	El objetivo de este proyecto es la puesta en marcha de un sistema que incluya una autoridad de certificación y un servidor OCSP para la validación, de forma que firme los certificados de forma transparente al administrador y éste pueda utilizarlos para su servicio. Se parte de la idea de que en un futuro todas las aplicaciones se comuniquen de forma cifrada
Rodrigo A. Bartels Y Ricardo Villalon-Fonseca	Diseño de un esquema de certificación para las Autoridades Certificadoras del Sistema Nacional de	CITIC, Universidad de Costa Rica, Costa Rica	En una Infraestructura de Llave Pública participan diversos actores, cada uno con roles diferentes dentro del proceso para emitir y usar certificados digitales, por ejemplo, los usuarios,

	Certificación Digital de Costa Rica		las Autoridades de Registro y las Autoridades Certificadoras (CA por sus siglas en inglés). Una CA es una entidad de confianza, responsable de emitir y revocar los certificados digitales utilizados para firmar documentos digitalmente, mitigar riesgos relacionados con el no repudio de las acciones realizadas por parte del poseedor de un certificado digital o autenticar de forma inequívoca a un ciudadano durante una transacción digital
Elizabeth Urrego, Marybel Vargas Aguirre, Verónica Chica Echavarría	Propuesta De Implementación De La Firma Digital Para LaCooperativa Coopserp	Universidad De Medellín Facultad De Ciencias Económicas Y Administrativas	El objetivo de este trabajo es elaborar una propuesta de implementación de la firma digital en los procesos de la Cooperativa Coopserp
Gino Brehan Aguilar Alcarráz	Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos caso de estudio: Municipalidad de Miraflores	Facultad de Ingeniería de Sistemas e Informática, Pregrado, Universidad Nacional Mayor de San Marcos Lima Perú	En este trabajo, se implementará un modelo simplificado de firma digital que se soporta en las tecnologías de la PKI y la invocación por protocolos. 6 con la adaptación de estas tecnologías, se podrá realizar la firma digital haciendo uso de aplicaciones web con total independencia del navegador, sistemas operativos, ActiveX o cualquier tecnología JAVA (applets, máquinas virtuales de JAVA), evitando así las configuraciones complicadas y dependencias de terceros.

Fuente: el autor

11.2 MARCO CONTEXTUAL

Colpensiones, es una empresa del gobierno colombiano que administra el régimen público de pensiones del estado, esta empresa está clasificada como una compañía financiera de carácter especial y vinculada al ministerio de trabajo.

Colpensiones, se crea debido a la necesidad que tiene la sociedad colombiana de mejorar el régimen de pensiones, el cual administraba el instituto de seguros sociales y estaba en una profunda crisis administrativa y financiera.

Con el nacimiento de Colpensiones hace 8 años, el régimen de pensiones del estado colombiano mejoró notablemente y pasó a ser el sistema preferido de la sociedad colombiana convirtiéndose en una verdadera competencia para los sistemas de los fondos de pensiones privados.

Desde los inicios de esta entidad estatal, la sede principal y administrativa de Colpensiones se ubica en Bogotá, tiene presencia en todas las ciudades importantes del país, tiene alrededor de 2300 empleados actualmente y se encuentra en un proceso de fortalecimiento para optimizar sus procesos y mejorar aún más la administración de pensiones estatales.

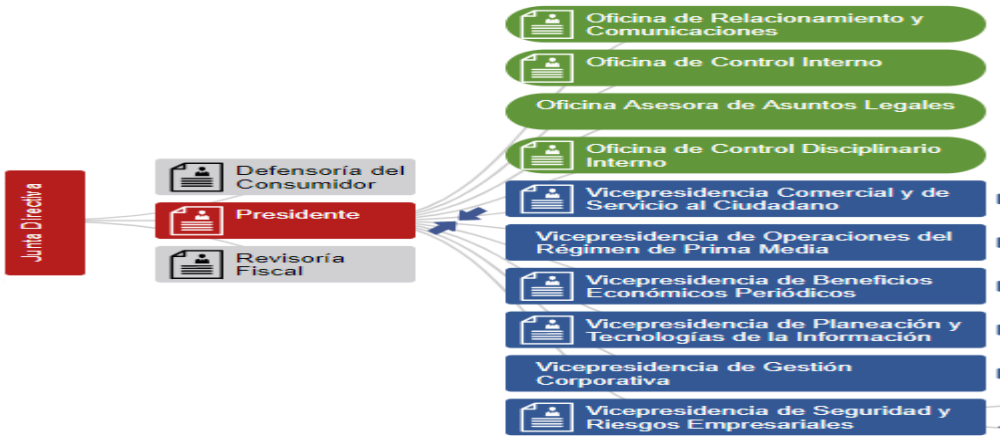
Colpensiones dentro de su marco estratégico tiene formuladas la visión y la misión de la compañía:

Visión: Somos la empresa estatal, que, como parte del sistema de protección para la vejez, administra integralmente el Régimen de Prima Media con prestación definida (RPM), y el servicio social complementario de ahorro de beneficios económicos periódicos (BEPS), generando valor agregado y servicios con innovación para contribuir a mejorar la calidad de vida de los colombianos

Misión: Colpensiones contará en el 2018 con una cultura empresarial caracterizada por el trabajo en equipo, el crecimiento personal y profesional de su talento humano y logrará ser reconocido por la transparencia, excelencia y calidad en la prestación de los servicios, generando confianza de los empleadores y los ciudadanos en la empresa.

El organigrama actual de la empresa que puede verse de forma dinámica en el sitio web de la compañía es:

Figura 1. Organigrama de Colpensiones



Fuente: www.colpensiones.gov.co

Hoy en día, Colpensiones es una de las empresas de mayor recordación y con imagen positiva dentro de las compañías del estado y el cubrimiento que presta es del orden nacional, adicional al sistema de pensión estatal, la administradora colombiana de pensiones creó un sistema de beneficios económicos periódicos para aquellas personas que no tienen un trabajo formal, y ofrecer de esta manera

una ayuda económica para los ciudadanos de menores recursos de nuestra sociedad.

Para llevar a cabo exitosamente cada proceso que emplea la administradora estatal, uno de los pilares fundamentales está cimentado en la tecnología, razón por la cual en Colpensiones se utilizan sistemas informáticos y recursos tecnológicos de última generación. Debido a la naturaleza pública de los dineros con los que se adquieren los servicios tecnológicos, las contrataciones de proveedores y equipos exigen un alto grado de transparencia y costos razonables.

Dentro del marco tecnológico que utiliza Colpensiones, existen auditorías periódicas orientadas a detectar fallas e implementar las correcciones necesarias para resolver los problemas o debilidades encontradas, una de las debilidades halladas en una de estas auditorías, se detectó que las aplicaciones web locales viajaban por la red de datos en texto claro. Para solucionar este problema, se plantea la necesidad de crear entidad certificadora local.

Esta entidad certificadora local se diseña e implementa en la sede principal de Colpensiones en Bogotá, desde la vicepresidencia de planeación y tecnologías de la información, bajo la gerencia de infraestructura tecnológica.

11.3 MARCO TEORICO

Dentro del marco teórico para la propuesta, se define el concepto de una entidad certificadora y sus tipos, también es importante destacar las diferentes formas existentes de instalación de estas plataformas.

Una entidad certificadora, es un sistema tecnológico que se encarga de avalar la identidad de usuarios, equipos y organizaciones, una entidad certificadora también es conocida por sus siglas en inglés CA (certification authority) o entidad

certificadora. Las CA autentican una organización y responden por ella emitiendo un certificado firmado digitalmente. De igual forma, una entidad certificadora o CA conocida por sus siglas, administra, revoca y renueva certificados digitales utilizados para garantizar la autenticidad documental o de sitios web.

Tipos de entidades de certificación:

Una entidad certificadora, puede clasificarse en entidad certificadora local cuando se está haciendo referencia a un servidor que una organización utiliza para emitir y administrar certificados digitales que serán reconocidos exclusivamente dentro del dominio de la empresa.

En una entidad certificadora interna, se pueden emitir certificados digitales para sitios o para documentos y hacerlos reconocidos y válidos dentro de una organización usando los servicios del dominio de la empresa. La ventaja de usar una entidad certificadora interna es que se puede hacer un ahorro económico importante al no tener la necesidad de pagar por cada certificado generado.

La entidad certificadora será una entidad certificadora externa cuando esta se encargue de certificar la veracidad de la documentación, sitios, personas y demás recursos de compañías, entidades, empresas o sociedades privadas o del orden gubernamental.

Una entidad certificadora externa es por lo general una empresa que se encarga de prestar servicios de autenticación digital y tiene una gran infraestructura tecnológica, una de las más reconocidas es VeriSign

Una entidad certificadora externa cobra por cada certificado que emita para dar fe de autenticidad sobre un sitio o página web en particular.

Una entidad certificadora raíz, es aquella ca principal dentro de un conjunto de entidades de certificación que conforman el sistema de certificación de una ca.

Una entidad certificadora subordinada es una ca para la que otra ca de la organización emite un certificado. Normalmente, la ca subordinada emite certificados para usos específicos como la protección del correo electrónico, la autenticación basada en web o la autenticación de tarjeta inteligente. Las entidades certificadoras subordinadas también pueden emitir certificados para otras ca con un nivel superior de subordinación.

11.3.1 Funciones de una CA: Una autoridad certificadora es una organización confiable y reconocida por un grupo o público específico cuya función es entregar certificados de identidad y mantener la información de su estado.
De forma general, las funciones de una entidad certificadora son:

11.3.2 Recepción de solicitudes: Un usuario llena un formulario y lo envía a la entidad certificadora requiriendo un certificado. La generación de las claves pública y privada son responsabilidad del usuario o de un sistema de generación de requerimientos asociado a la entidad certificadora.

11.3.3 Autentificación del usuario: Antes de firmar la información proporcionada por el usuario en el requerimiento previo, la entidad certificadora debe verificar su identidad.

11.3.4 Generación de certificados: Después de recibir una solicitud y validar los datos la entidad certificadora genera el certificado correspondiente y lo firma con su clave privada.

11.3.5 Distribución de certificados: La autoridad certificadora puede proporcionar un servicio de distribución de certificados para ser entregados o descargados por los sistemas interesados en su instalación.

11.3.6 Anulación de certificados: La entidad certificadora mantiene la información correspondiente a una anulación durante todo el tiempo de validez del certificado original.

11.3.7 Almacenes de datos: Almacenar en una base de datos los certificados y la información de las anulaciones.

11.3.8 Generación de documentación: En esta documentación se explican los procedimientos, las prácticas y políticas de certificación de la entidad certificadora.

11.3.9 Creación de una CA: Una entidad certificadora, se puede crear de diferentes maneras dependiendo del tipo de sistema operativo que se esté usando, o del proveedor de software que se use para el montaje de la entidad certificadora, por ejemplo, puede configurarse un rol de ca para Microsoft Windows, para Linux, u otro sistema operativo.

Uno de los métodos más usados para la creación de una entidad certificadora local, es el método de creación mediante openSSL.

11.3.10 El openSSL es un conjunto de herramientas criptográficas que permiten la configuración y generación de certificados digitales y la puesta en marcha de una entidad certificadora local, su uso se basa en la ejecución de comandos para la creación de la entidad certificadora y también para el requerimiento de certificados digitales. Normalmente el openSSL es utilizado en ambientes con sistemas operativos Linux.

Para instalación de entidades certificadoras en sistemas operativos Windows, se utiliza el rol que proporciona el sistema operativo en la versión de directorio activo configurando las plantillas y lo sitios de almacenamiento de los certificados a generar.

La administración de la entidad certificadora desde Windows se puede realizar de manera gráfica utilizando el entorno del rol de ca configurado. Para poder utilizar certificados propios en los diferentes servicios que se requieran proteger, se puede usar una entidad certificadora montada en Windows Server para tener control total sobre la propia infraestructura sin depender de terceros.

11.3.11 Entidades de Certificación: Adicionalmente a una entidad certificadora local, existen entidades certificadoras externas quienes son las encargadas de avalar un sitio web público y certificar la originalidad de dicho sitio. En Colombia existen entidades que representan de alguna forma certificadoras internacionales como Symantec. Entre estas están empresas como Certicamara, entidad de certificación digital abierta autorizada por la Superintendencia de Industria y Comercio, constituida por las cámaras de comercio del país con el fin de proveer la seguridad jurídica y tecnológica en entornos electrónicos cumpliendo el marco legal, las normas y estándares internacionales de certificación digital.

También se encuentran entidades como ANDES SCD S.A, Autoridad de Certificación Digital Abierta autorizada en Colombia, provee a sus interesados servicios de certificación digital y soluciones integrales sostenibles a nivel económico y ambiental. Garantizando validez jurídica, seguridad, oportunidad y calidad en la entrega de sus productos y servicios; aportando el talento nacional a la sociedad de forma innovadora a través de tecnologías de la información.

Una vez explicados los conceptos sobre una entidad certificadora y su funcionamiento, y para el caso específico del que trata el tema, se propone la instalación de una entidad certificadora basada en el sistema operativo Windows 2012 r2 usando el rol de entidad de certificación que provee el fabricante Microsoft. Se propone el montaje en este sistema operativo por conveniencia de la compañía debido a que su infraestructura se basa en tecnología Microsoft

Se tratará a continuación la forma en cómo se puede configurar una CA basada en Windows.

En Windows, el rol de instalación se realiza a través de un administrador de dominio, y la instalación debe hacerse siguiendo las recomendaciones del fabricante, se procede entonces en el servidor a instalar el rol Active Directory Certifícate Services.

En Windows Server existe un rol incluido entre los roles de Directorio Activo que permite la instalación y configuración de una entidad certificadora privada que usa el propio directorio activo para generar y gestionar los certificados. Se debe tener en cuenta que estos certificados serán reconocidos únicamente por los dispositivos unidos al dominio o aquellos a los que manualmente se les instale el certificado raíz de la entidad certificadora

Después de haber tratado los conceptos fundamentales sobre entidades certificadoras, es importante describir lo que es un certificado digital.
Un certificado digital podría entenderse como un archivo de datos que contiene información verificable al respecto de la identificación de una persona o un sitio web en especial. Esta información verificable se usa para asegurar a terceros o usuarios externos que un sitio web es quien dice ser o una persona tiene la identidad que informa en un correo o firma digital.

Una entidad certificadora acepta requerimientos de certificados generados desde los servidores remotos y verifica la identidad del servidor de acuerdo a las políticas configuradas en la ca. Después de esto usa sus credenciales digitales para firmar los certificados creados dejándolos óptimos y reconocibles para ser usados dentro de la red que cubre la entidad certificadora. La ca también se puede usar para revocar certificados que por algún motivo no se usan o hayan ingresado a una lista de certificados inválidos.

Ahora, es necesario definir algunos conceptos sobre los componentes de software requerido una entidad certificadora o CA por sus siglas en inglés (certification authority) específicamente para el sistema operativo Windows.

11.3.12 En sistemas operativos Windows, una entidad certificadora se instala a partir de un rol o función específica proporcionada por el servidor. En Windows se encuentran diferentes roles, el rol de directorio activo o active directory en inglés el cual es el encargado de proporcionar servicios de gestión de accesos y administración de recursos del sistema como unidades de almacenamiento, impresión etc. También existen roles de generación de direccionamiento ip como dhcp, resolución de nombres como dns, gestión de archivos dfs y otros más.
Dentro de los roles que competen directamente con la entidad certificadora, están los roles de servidor web o web server (iis) en inglés, el servicio de certificados de directorio activo o directory certificate services, entidad certificadora o certification authotity y autoridad de certificación de inscripción en la web ó certification authority web enrollment.

11.3.13 El servidor web o web server (iis) permite publicar aplicaciones o páginas web a través del servidor

11.3.14 El servicio de certificados de directorio activo o directory certificate services, permite realizar las configuraciones de plantillas de certificados a generar en la entidad

11.3.15 Entidad certificadora o certification authotity permite configurar el servidor con las características propias para que se comporte como entidad certificadora interna y genere los certificados de raíz de confianza y avale todos los certificados locales generados e instalados en los servidores web

11.3.16 El rol autoridad de certificación de inscripción en la web o certification

authority web enrollment permite realizar las renovaciones o revocaciones de los certificados generados en la entidad certificadora.

11.3.17 Para crear una entidad certificadora en un servidor Windows 2012, se requiere entonces escoger el rol de entidad certificadora y configurar las opciones que el sistema operativo va entregando, al finalizar la generación de la entidad, el sistema entrega tres servicios o funciones, la de entidad certificadora propiamente dicha, la de generación de certificados y la de servidor web para alojar la agina que recibirá y entregará certificados digitales

11.4 MARCO CONCEPTUAL

Colpensiones es la empresa estatal encargada de regular el régimen de prima media con prestación definida, es decir, esta empresa es la encargada de administrar todo el régimen pensional de los ciudadanos que se encuentren afiliados a esta.

La administradora Colpensiones, nace para satisfacer las necesidades relacionadas con los trámites de afiliación y pensiones de los ciudadanos afiliados al antiguo instituto de seguros sociales conocido como ISS, esta entidad gubernamental, lleva más de 6 años de creación y se encuentra atendiendo a los ciudadanos desde hace 5 reemplazando al ISS en todas sus funciones mejorando y potenciando el servicio pensional para los ciudadanos afiliados.

Actualmente la sede principal de Colpensiones se encuentra domiciliada en Bogotá, cuenta con oficinas de atención al público en todas las ciudades principales de Colombia, dentro de su estructura organizacional, la empresa es dirigida a través de una junta directiva compuesta por altos cargos del gobierno, tiene un presidente y varias vicepresidencias encargadas de sincronizar y ejecutar los lineamientos y

ordenes gubernamentales.

En cuanto al organigrama, la compañía se encuentra organizada jerárquicamente y se rige por las decisiones que tome la junta directiva compuesta por funcionarios de altos cargos estatales, después de la junta sigue la presidencia que a su vez gobierna las vicepresidencias, las vicepresidencias tienen gerencias por cada área importante de la empresa y las gerencias cuentan con directores de área los cuales dirigen los diferentes cargos profesionales, técnicos y asistenciales que tiene la empresa.

Debido a la información confidencial que se maneja en los diferentes aplicativos webs de la compañía, se hace fundamental poder contar con la publicación de dichos programas a través de protocolo seguro https, debido a esta exigencia, surge la necesidad de crear una entidad certificadora local para emitir certificados y publicar las aplicaciones en https de forma segura.

Debido a la naturaleza técnica del proyecto, este será desarrollado en las instalaciones de la dirección general de Colpensiones las cuales se encuentran localizas geográficamente en Bogotá, dentro de la vicepresidencia de planeación y tecnología de la información, dentro de esta vicepresidencia, se encuentra la gerencia de infraestructura, dentro de la cual se maneja toda la parte de TI de la compañía, y es en esta área de ti donde el proyecto tomará forma.

Figura 2 Organigrama de la vicepresidencia

Fuente:www.colpensiones.gov.co

Dentro del marco conceptual se definirán los términos y conceptos con los que una entidad certificadora se identifica:

Entidad de certificación o CA: Es una organización o sistema que proporciona certificados digitales con reconocimiento y aceptación reconocidos por un grupo. Una entidad certificadora local proporciona certificados digitales aceptados dentro de un dominio u organización únicamente, mientras que una CA externa entrega certificados digitales reconocidos por la comunidad de internet completa.

Certificado Digital: Un certificado digital es un archivo electrónico el cual posee una firma reconocida por otras entidades como legítimo y que le da validez y legalidad a los documentos que estén firmados por este.

Infraestructura de llave pública o pki: Una pki es el conjunto de todos los elementos

de hardware y software que componen un sistema de llaves y cifrado de información como lo son la entidad certificadora, los certificados digitales, los algoritmos de encripción de datos y el sistema de uso y generación de certificados digitales.

Active Directory Certifícate Servicess: El active Directory Certificate Servicess es el rol del sistema Windows que permite configurar una entidad certificadora o CA dentro de un dominio determinado

11.5 MARCO LEGAL

Dentro del marco legal colombiano, existen varias leyes que regulan las actividades ejecutadas sobre recursos informáticos y penaliza los delitos que se contemplan en diversas tipificaciones, las leyes más importantes sobre las que de alguna manera existe una incidencia con el proyecto propuesto son:

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

Dentro del marco legal se tratarán los artículos de la ley 1273 de 2009 la cual trata los siguientes puntos:

LEY 1273 DE 2009 16: Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la protección de la información y de los datos", del siguiente tenor:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos

dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

De los atentados informáticos y otras infracciones
Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral, así:
Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:
17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

11.6 DISEÑO METODOLOGICO.

Dentro del diseño metodológico, este trabajo describirá la forma o metodología empleada para el diseño y ejecución del proyecto de entidad certificadora, se describirá el tipo de investigación, las fases del proyecto y las fuentes de investigación utilizadas.

En el diseño metodológico, se describirá la forma que se realizará el proyecto, dividiéndolo por fases para para una compresión más fácil sobre los procedimientos necesarios para que el proyecto funcione.

Cada una de las fases en las que se divide el proyecto tiene por finalidad la satisfacción y cumplimiento de los objetivos específicos formulados para la creación de la entidad certificadora.

Dentro del diseño metodológico, y por la naturaleza del proyecto aplicado que propone el trabajo, el tipo de investigación se enmarca en la investigación aplicada, pues en este caso se trata de encontrar una solución a un problema específico dentro del ámbito de seguridad de la información dentro de la red de datos de una empresa.

Las fuentes de investigación primarias utilizadas para el desarrollo de la investigación, son todos aquellos manuales técnicos emitidos por los fabricantes de las entidades certificadora, para este caso en particular se han utilizado los

manuales de referencia publicados por los fabricantes Microsoft e Ibm, dentro de estos libros se encuentra publicada la información referente a las características de las entidades certificadoras de cada fabricante, su instalación, requisitos de harware y software y las mejores prácticas para la puesta en marcha de la entidad y su administración.

Como fuentes de información secundarias, se tiene la documentación sintetizada de las instalaciones de la entidad certificadora resumidas por el proveedor de infraestructura de Colpensiones, pues el proveedor entrega documentación técnica e informes de configuraciones en los reportes periódicos para la empresa, basados en la información de los manuales del fabricante.

Para el caso particular de este proyecto, la población son todas aquellas aplicaciones web que trabajan de forma local dentro de la red de datos de Colpensiones, y la muestra son aquellas aplicaciones que se tomaron para realizar la configuración de cifrado en la que se basó la investigación.

Se utilizaron técnicas de investigación como reuniones de trabajo y foros con el proveedor de tecnología y sus ingenieros para obtener la mayor cantidad de información sobre las metodologías de generación de entidades de certificación sobre Windows, como instrumentos de investigación se utilizaron varias máquinas de Windows 2012 con las que se probó de forma inicial la forma de generación de roles para entidades certificadoras.

Para el análisis de la información, se utilizaron los datos obtenidos del estudio hecho al problema existente y las diferentes formas de resolverlo, entendiendo como datos cualitativos esa información de métodos de construcción de entidades certificadoras.

Una vez obtenidos cualitativamente los datos, se procede a realizar su codificación, clasificación y reducción permanentes para llegar finalmente al método de creación

de la entidad certificadora de forma óptima y funcional adaptada exclusivamente para Colpensiones.

11.6.1 Fase 1

Configurar un servidor en plataforma de sistema operativo Windows con el rol de entidad certificadora y todas las configuraciones relacionadas a este

La primera fase para dar inicio al proyecto, consiste en la asignación de un nuevo servidor virtual con sistema operativo Windows 2012 R2, debido a que esta máquina solo se empleará para la generación de los certificados y el almacenamiento de la entidad certificadora, no se requiere de prestaciones de hardware especiales o de gran tamaño, por lo anterior se ordena la creación de una máquina virtual en sistema operativo Windows 2012 R2 con un solo procesador Xeon a 2.5 ghz, capacidad de memoria de 2 gb y un solo disco de almacenamiento con 50gb de espacio.

El método de generación será el establecido en la empresa en donde a través de un formato se realiza la solicitud al área de capacidad para que el proveedor de infraestructura genere la máquina.

Una vez el proveedor entrega la máquina solicitada, se procede con la inclusión de esta al domino de Colpensiones.loc y la verificación de las capacidades solicitadas en el requerimiento.

Posterior a la verificación de la máquina y su inclusión en el dominio se establecen los permisos de red necesarios en firewall para que la nueva máquina tenga acceso a todos los ambientes de trabajo de la empresa y que la entidad certificadora pueda generar certificados confiables en ambientes productivos y de pruebas.

11.6.2 Fase2

En la fase 2, después de tener el servidor creado y adicionado al domino junto con los permisos de red necesarios para que la máquina alcance toda la red de Colpensiones, de se procede a configurar el rol de entidad certificadora.

Se selecciona entonces el rol de entidad dentro de los roles que ofrece el sistema operativo y se configura la ca, debido a que el sistema operativo es Windows, la configuración puede realizarse completamente desde el entorno gráfico.

Dentro de los ítems de configuración se escogen las plantillas de certificados a utilizar, para el caso en mención es muy importante configurar la plantilla de certificados web, pues esta es a que se encarga de emitir los certificados para las aplicaciones que se van a asegurar.

11.6.3 Fase 3

Realizar pruebas previas sobre el estado actual de la publicación de aplicaciones web

La fase 3 permite empezar con las pruebas de publicación de sitios web en formato https, pues una vez configurado el servidor virtual en Windows en la etapa 1, y la correspondiente configuración y puesta en marcha de la entidad certificadora en la fase 2 es posible empezar a crear certificados digitales para que sean instalados en las aplicaciones web que se asegurarán.

En esta etapa, también se realiza la emisión de un certificado raíz de confianza el cual es expedido por la entidad certificadora que se ha creado, este certificado de confianza se instala en los dominios productivos y de pruebas de Colpensiones y

algunos proveedores para que la entidad sea reconocida como una certificadora local de confianza en todo el ámbito tecnológico de Colpensiones.

Las pruebas consisten básicamente, en realizar requerimientos de certificado desde los servidores que contienen las aplicaciones publicadas hasta ahora en http, estos requerimientos de certificado se envían al administrador de la entidad certificadora, a partir de los requerimientos de las aplicaciones, se generan los certificados ssl en formato web y se entregan a cada aplicación.

Una vez expedido el certificado digital ssl por la entidad certificadora, se instala en la aplicación y se realiza la publicación de esta a través de ssl, se crean permisos de firewall para acceder a través de los puertos ssl previamente convenidos y después de tener pleno acceso, se procede a ingresar a la aplicación en https para probar toda la funcionalidad de esta.

Todas las pruebas se realizarán en los ambientes de calidad e integración que Colpensiones tiene destinados para las pruebas.

11.6.4 Fase 4

Definición del tipo de certificados digitales que mejor se adaptan a la compañía y sus aplicaciones web.

Después de la realización de las pruebas de certificación se revisa el tipo de certificación apropiado para los sitios web de Colpensiones. Debido a que los certificados se instalarán en aplicaciones web, la plantilla del certificado debe ser la plantilla web, es necesario tener especial cuidado en el requerimiento o request como se conoce más comúnmente al requerimiento de certificado con el que la entidad certificadora genera los certificados.

El requerimiento de certificado debe tener además del campo de nombre del certificado o nombre común, un campo conocido como nombre alternativo de dominio dns y la clave debe estar configurada con longitud de 2048 para proporcionar soporte de sha2 para soportar los formatos más actuales admitidos por los navegadores en sus últimas versiones.

Después de terminada la fase 4, se procede con la implementación de la publicación de los sitios de aplicaciones web https en el ambiente productivo de Colpensiones.

12 DESARROLLO DEL PROYECTO

De acuerdo con los puntos tratados en el diseño metodológico, se procede con la construcción de la entidad certificadora propuesta partiendo desde la fase 1 en donde se crea un servidor, en la fase 2 se configura la entidad certificadora, en la fase 3 se realizan las pruebas necesarias y en la fase 4 se publican las aplicaciones web locales en forma cifrada usando certificados digitales.

12.1 Fase 1 Creación De Un Servidor Virtual De Windows 2012

Se solicita al área de capacidad la creación de un servidor Windows 2012 virtual para ser usado como entidad certificadora, las características de instalación solicitadas al área de capacidad fueron:

Tabla 2. Servidor Virtual Entregado Por El área De Capacidad

Características	Valor
Procesador	1 core Intel xeon
Memoria	2gb
Sistema operativo	Windows 2012 R2 estándar 64x

Fuente: el autor

12.1.1 Fase 1 Aseguramiento Del Servidor Virtual De Windows 2012

En cuanto al aseguramiento de la máquina, el proveedor crea los servidores que solicita Colpensiones bajo una plantilla de aseguramiento o hardening establecida para todos los equipos de aplicaciones de la compañía, dentro de esta plantilla de aseguramiento, se desactivan los accesos de lectores usb, discos ópticos, se limita

el compartir archivos a estados controlados, se realiza la configuración de red, el comportamiento del cortafuegos y varios puntos más que restringen accesos a recursos de las máquinas. Una vez que se crea el servidor, el área de seguridad de la empresa lo examina y posteriormente es entregado a infraestructura para la implementación del proyecto.

La plantilla de aseguramiento utilizada y sus características son:

Tabla 3. Contraseñas Plantilla De Aseguramiento

Servicio/Función	Valor	Descripción	Valor recomendado	Valor acordado
Requerimientos de contraseña	6	Longitud de contraseña	12	8

Fuente: el autor

En requerimientos de contraseña, se fija que las contraseñas tengan un valor de 8 dígitos, la recomendación del fabricante es de 12 para proporcionar un acceso seguro, por defecto en el momento de la instalación de la máquina, la longitud de contraseña es de 6 dígitos.

Se determinó dejar una contraseña de 8 dígitos debido a que, al tener una credencial de acceso de 12 dígitos, podrían incrementarse de manera significativa las llamadas a la mesa de ayuda para la recuperación debido al olvido de esta.

Adicionalmente, se implementó una política en el directorio activo del dominio Colpensiones.loc que utiliza un diccionario de términos prohibidos en donde se controla que las contraseñas no lleven números seguidos, no tengan nombres propios, o el número de año actual para prevenir que se usen accesos con nombres de familiares, lugares, equipos deportivos y otros que suelen ser comunes y de fácil acceso.

Al tener una contraseña de 8 dígitos con números, caracteres especiales y letras mayúsculas y minúsculas se mitiga el riesgo de ataque de fuerza bruta, pues una contraseña de esta complejidad tardaría años en ser descifrada usando una computadora normal en un eventual ataque.

Tabla 4. Servicios Plantilla De Aseguramiento

Servicio/Función	Valor	Descripción	Valor recomendado	Valor acordado
Telnet	Deshabilitar	Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como TEXTO PLANO	Deshabilitar	Deshabilitar

Fuente: el autor

El servicio de telnet, es utilizado para ingresar remotamente a una máquina, este protocolo normalmente es potencialmente inseguro, pues sus conexiones se hacen a través de texto claro y el ingreso de credenciales es fácilmente obtenido a través de un analizador de red, por defecto este protocolo viene inactivo en el servidor y la recomendación es dejarlo de esta manera.

El protocolo ssh cumple con la misma función del ftp, pero a diferencia de este, el ssh usa conexiones cifradas que mitigan el problema de seguridad inherente al ftp

Tabla 5. Bloqueos De Contraseñas Plantilla De Aseguramiento

Servicio/Función	Descripción	Valor recomendado	Cantidad
Inicio de sesión Contraseña reintento de bloqueo	Permite bloquear una cuenta de usuario local después de un número configurado de intentos de conexión fallidos.	Habilitar	5

Fuente: el autor

Reintento de contraseña, este parámetro configura la cantidad máxima de contraseñas fallidas que se pueden ingresar en una cantidad de tiempo determinada antes de bloquear un usuario.

Este parámetro se configura para mitigar la posibilidad de que un usuario no autorizado intente ingresar al servidor tratando de adivinar la contraseña usando diferentes métodos como el ataque de fuerza bruta o aprovechando descuidos del usuario titular del acceso.

En el caso del servidor, después de 5 intentos de contraseña errónea, el sistema deshabilita la cuenta y el usuario no podrá ingresar hasta que sea activada de nuevo por un administrador del sistema. Esta configuración se hace por medio de políticas de gpo del directorio activo sobre la máquina

Tabla 6. Recursos Compartidos Plantilla De Aseguramiento

Servicio/Función	Descripción	Valor recomendado
Verificación de recursos compartidos	Se deben deshabilitar los recursos compartidos que no son necesarios	Desactivar recursos compartidos y accesos periféricos como lectores de usb

Fuente: el autor

Se verifica que la máquina no tenga habilitados recursos compartidos como carpetas, discos y archivos con el objetivo de cerrar las posibilidades de fuga de información y que a través de un dispositivo periférico o archivo compartido se pueda descargar información sobre los certificados que se generan dentro de la entidad certificadora.

Tabla 7. Recursos de netbios y enumeración Plantilla De Aseguramiento

Servicio/Función	Descripción	Valor recomendado
Configurar NetBIOS/SMB	Fijar en los servicios NetBIOS/SMB los parámetros RestrictAnonymous=2 en el registro del sistema	Do not allow anonymous enumeration of SAM accounts Enable Do not allow anonymous enumeration of SAM accounts and shares Enable

Fuente: el autor

NetBios es un protocolo de red que permite que las aplicaciones que se ejecutan dentro de un entorno de red se comuniquen entre sí, y smb es el protocolo que permite compartir recursos de red como impresoras y archivos, estos protocolos deben estar controlados por medio de políticas de seguridad locales que eliminen la posibilidad de tener sesiones de conexión con usuarios no autenticados configurando el parámetro restrictanonymous=2 en la ruta

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters del registro del servidor.

Windows tiene la particularidad de permitir enumerar recursos del sistema o del dominio en donde se encuentra ubicado el servidor, por este motivo se hace necesario prevenir que los usuarios enumeren recursos deshabilitando la función en las políticas locales de la máquina.

Es importante realizar la configuración descrita, pues si los usuarios pueden enumerar los recursos del dominio, estos datos pueden ser usados en la construcción de un ataque para forzar elevación de permisos o denegación de servicio en los servidores de la red.

Tabla 8. Protección Contra DDS y DOS Plantilla De Aseguramiento

Servicio/Función	Descripción	Valor recomendado		
Protección contra ataques DoS	Modificar las configuración del protocolo TCP/IP	Modificar la llave		
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\		
		EnableICMPRedirect	DWORD	0
		SynAttackProtect	DWORD	1
		EnableDeadGWDetect	DWORD	0
		EnablePMTUDiscovery	DWORD	0
		KeepAliveTime	DWORD	300,000
		DisableIPSourceRouting	DWORD	2
		TcpMaxConnectResponseRetransmissions	DWORD	2
		TcpMaxDataRetransmissions	DWORD	3
		PerformRouterDiscovery	DWORD	0
		TCPMaxPortsExhausted	DWORD	5

Fuente: el autor

Los ataques de denegación de servicio dos o ataques de denegación de servicio distribuido ddos son aquellos que inhabilitan el uso de un sistema determinado consumiendo todos los recursos, la diferencia en dre el ataque dos y el ddos radica en que el primero se hace desde una sola máquina atacante, y el ddos utiliza varis equipos para atacar un objetivo determinado, en el servidor se configuran los parámetros tcpip de acuerdo a las recomendaciones del fabricante Microsoft.

Tabla 9. Asegurando Cuentas Comunes Plantilla De Aseguramiento

Servicio/Función	Descripción	Valor recomendado
Deshabilitar la cuenta GUEST	No debe existir la cuenta guest	En Local Security Policy\Security Settings\ Local Policies\Security Options, Account Settings, verificar que Guest account status esté deshabilitada
Renombrar la cuenta de Administrador	Bloquee la cuenta auténtica de Administrador y cree un señuelo y cuando la enumeración sea posible).	En Local Security Policy\Security Settings\ Local Policies\Security Options, Accounts: Rename administrator account y cambiar el nombre de la cuenta

Fuente: el autor

Una de las formas más comunes de ataques en los servidores de Windows, es el intento de elevación de permisos en cuentas con pocos privilegios como la de invitados y la obtención de la contraseña de la cuenta administrador, es muy conocido que por defecto este sistema operativo trae activas estas cuentas. Al

eliminar la cuenta de invitado, y renombrar la cuenta de administrador se mitiga en gran medida el riesgo de un ataque exitoso en la elevación de permisos u obtención de la contraseña del administrador.

12.1.2 Fase 1 Aseguramiento De Dispositivos Redes

Adicionalmente al aseguramiento de la máquina, existen otros mecanismos de seguridad que protegen al servidor de diferentes modalidades de ataques informáticos dentro de los cuales se tienen clasificadas por seguridad en redes y seguridad distribuida en directorio activo, dentro de la seguridad en redes se tienen:

Configuración de redes virtuales específicas por tipo de uso: se tienen vlans específicas para servidores que controlan aplicaciones, controladores de dominio, pasarelas de correo y otras funciones, es decir que un servidor destinado a un uso diferente del previamente establecido no funcionará en otra vlan que no esté configurada para dicho fin.

Configuración de listas de acceso en los enrutadores: los enrutadores tienen una configuración específica con listas de acceso que no permiten la adición de máquinas nuevas que no se hayan inscrito previamente.

La plantilla de configuración de enrutadores y switchs es la siguiente:

Se configura inicialmente la longitud de la contraseña de acceso al enrutador con el valor de 8 caracteres para no tener un incremento de fallas de contraseña de los usuarios de redes que ingresan a los enrutadores:

Tabla 10. Asegurando Contraseñas De Dispositivos De Red

Servicio / Función	Valor	Descripción	Valor recomendado	Valor acordado	Comando

Requerimientos de Password	6	Password Length	12	8	username usuario privilege 15 contraseña

Fuente: el autor

El telnet es un protocolo de conexión entre dispositivos que permite agregar o descargar datos y configurar un recurso remotamente, es conocido ampliamente que este protocolo es inseguro y en el enrutador se deshabilita el servicio de telnet en el enrutador

Tabla 11. Asegurando servicio Telnet En Dispositivos De Red

Servicio/Función	Descripción	Valor recomendado	Valor acordado	Comando
Telnet	Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano	Deshabilitar	Deshabilitar	line vty 0 4 transport input ssh line vty 5 15 transport input ssh

Fuente: el autor

Se bloquea la cuenta de un usuario que haya intentado repetidamente ingresar con una contraseña inválida.

Tabla 12. Reintento de Bloqueos En Dispositivos De Red

Servicio/Función	Descripción	Valor recomendado	Valor acordado	Comando
Inicio de sesión Contraseña reintento de bloqueo	Permite bloquear una cuenta de usuario local después de un número configurado de intentos de	Habilitar	5	ip ssh version 2 ip ssh authentication-retries 5

	conexión fallidos.		

Fuente: el autor

Se encriptan las contraseñas usadas para el ingreso a los enrutadores

Tabla 13. Encriptando Contraseñas En Dispositivos De Red

Servicio/Función	Descripción	Valor recomendado	Comando
Encriptacion Password	Password no visibles al mostrar la configuracion (passw para los usaurios que no tienen privilegios)	Habilitar	enable password encription

Fuente: el autor

Snmp es un protocolo de administración de redes, con este protocolo, los dispositivos de una red como enrutadores o switchs pueden intercambiar información de administración, adicionalmente, un administrador puede hacer labores de planeación y crecimiento gracias al snmp, existe la versión v3 de este protocolo la cual proporciona el módulo criptográfico de seguridad, función no presente en las v1 y v2, la versión v3 puede encriptar la información y mejora el acceso remoto para gestionar la red de una manera más segura, por lo anterior, la plantilla indica que es necesario inactivar las versiones v1 y v2 y dejar habilitada la v3.

Tabla 14. Configurando Snmp v3 En Dispositivos De Red

Servicio/Función	Descripción	Valor recomendado	Valor acordado	Comando
SNMPv1/2c	Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red	Deshabilitar	Deshabilitar	no snmp-server community public RO no snmp-server community admin RW ! disable SNMP trap and system-shutdown no snmp-server enable traps no snmp-server system-shutdown no snmp-server trap-auth disable the SNMP service no snmp-server
SNMPv3	Posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad	habilitar y deshabilitar la comunidad Publica	Habilitar	snmp-server group grupo v3 priv snmp-server user cacti grupo v3 auth md5 C0lp3ns10n3s priv aes 128 1nf0m3d14. Nota: clave creada xxxxxx

Fuente: el autor

Para aumentar la seguridad de acceso a los dispositivos de red, se crean listas de acceso, estas listas contienen las direcciones de los dispositivos que pueden comunicarse, esto se hace con el objetivo de mitigar el riesgo de acceso de intrusos en la red, pes no se podrán conectar máquinas diferentes a las que la lista de acceso tiene descritas.

Tabla 15. Configurando Snmp v3 En Dispositivos De Red

Servicio/Función	Descripción	Valor recomendado	Valor acordado	Comando
Authorized IP Managers	En los casos en que la configuración de gestión en forma de segura de VLAN es demasiado restrictiva, es	Hasta 10 direcciones IP se deben permitir el acceso para administración	Habilitar	access-list 88 permit xxx.xxx.xxx.xxx access-list 88 permit xxx.xxx.xxx.xxx access-list 88 permit xxx.xxx.xxx.xxx access-list 88 permit xxx.xxx.xxx.xxx - VPN

	posible identificar hasta 10 direcciones IP o grupos de direcciones que se les permite el acceso de administración al Gw de Voz a través de la red.	line vty 0 4 access-class 88 in

Fuente: el autor

12.1.3 Fase 1 Aseguramiento A través Dispositivos Cortafuegos

Se tienen dos cortafuegos o firewall ubicados dentro de la red, estos dispositivos tienen normalmente todos los puertos y aplicaciones cerrados y se abren únicamente los puertos y aplicaciones necesarias que requieran las aplicaciones y máquinas para su interconexión, uno de estos firewalls atiende peticiones de acceso para aplicaciones y equipos y el otro atiende peticiones de bases de datos.

También se tiene configurada una zona desmilitarizada en donde se encuentran las máquinas que tienen conexión directa con internet, estas máquinas pertenecen a otro dominio y tienen restricciones de acceso a los recursos de la red para mitigar ataques desde el exterior, para esta zona también el cortafuegos hace filtrado de datos y aplicaciones y deja pasar solo la información permitida previamente.

12.1.4 Fase 1 Aseguramiento A través Del Directorio Activo

Dentro de la seguridad distribuida por directorio activo, se cuenta con políticas de seguridad de acceso que limitan los recursos de las máquinas de los usuarios y las

conexiones entre ellos. También se tiene un proveedor que monitorea constantemente los cambios de permisos en los perfiles de los usuarios de servidores el cual informa cada vez que se sospecha de la detección de intrusos sobre la red o la modificación de recursos.

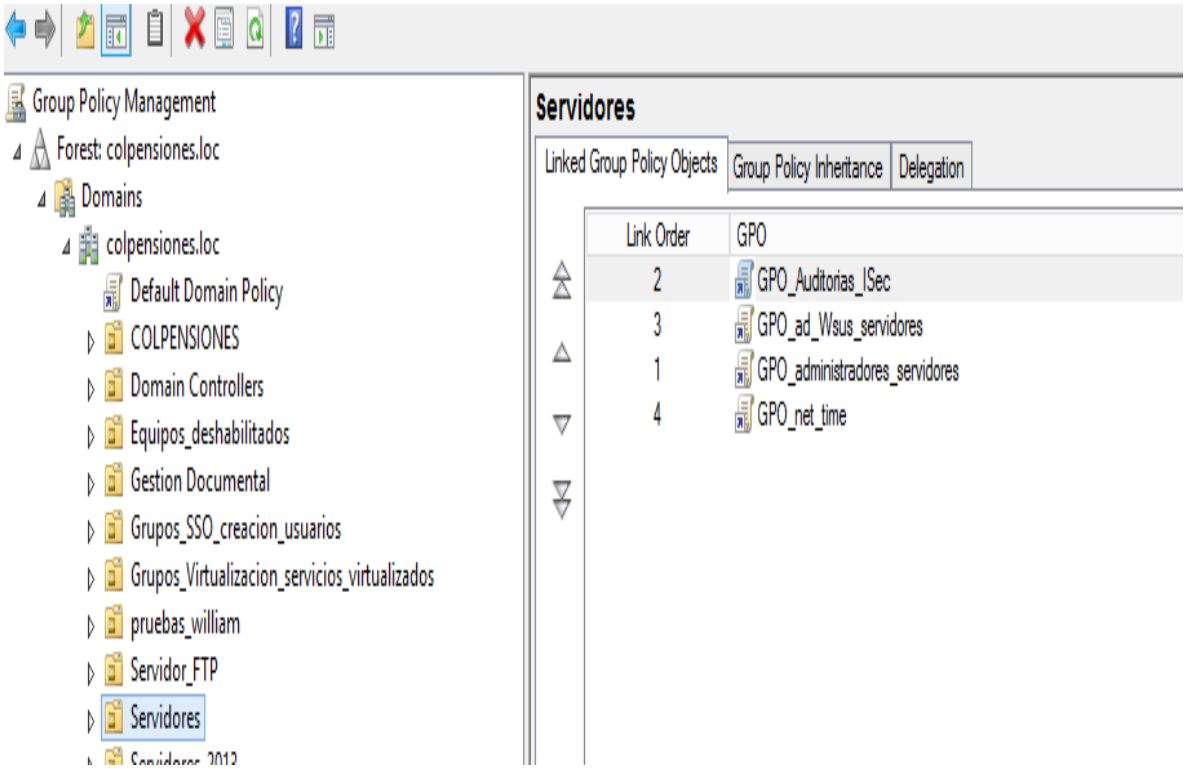
En resumen, Después de recibir la máquina creada y asegurada por el proveedor de parte de seguridad, esta es ingresada al dominio de Colpensiones, el servidor se ubica dentro de una unidad organizativa destinada para contener máquinas del tipo servidor.

En esta unidad organizativa, se aplican políticas de gpo que restringen aún más el acceso a la máquina y sus recursos certificando que el acceso al servidor se hará únicamente por los usuarios autorizados y bajo los roles establecidos.

La compañía tiene contratado un servicio con un proveedor externo que constantemente monitorea las cuentas de los usuarios de las máquinas y notifica los cambios que se puedan dar pudiendo detectar intrusos o elevación de permisos en un momento determinado, si aparece un cambio que no está dentro de los estándares establecidos una alarma es reportada de inmediato al administrador de directorio activo o al encargado del servidor de aplicaciones en donde se detectó el cambio.

En la siguiente imagen se puede apreciar la ubicación de políticas que aplican en la unidad organizativa correspondiente a los servidores:

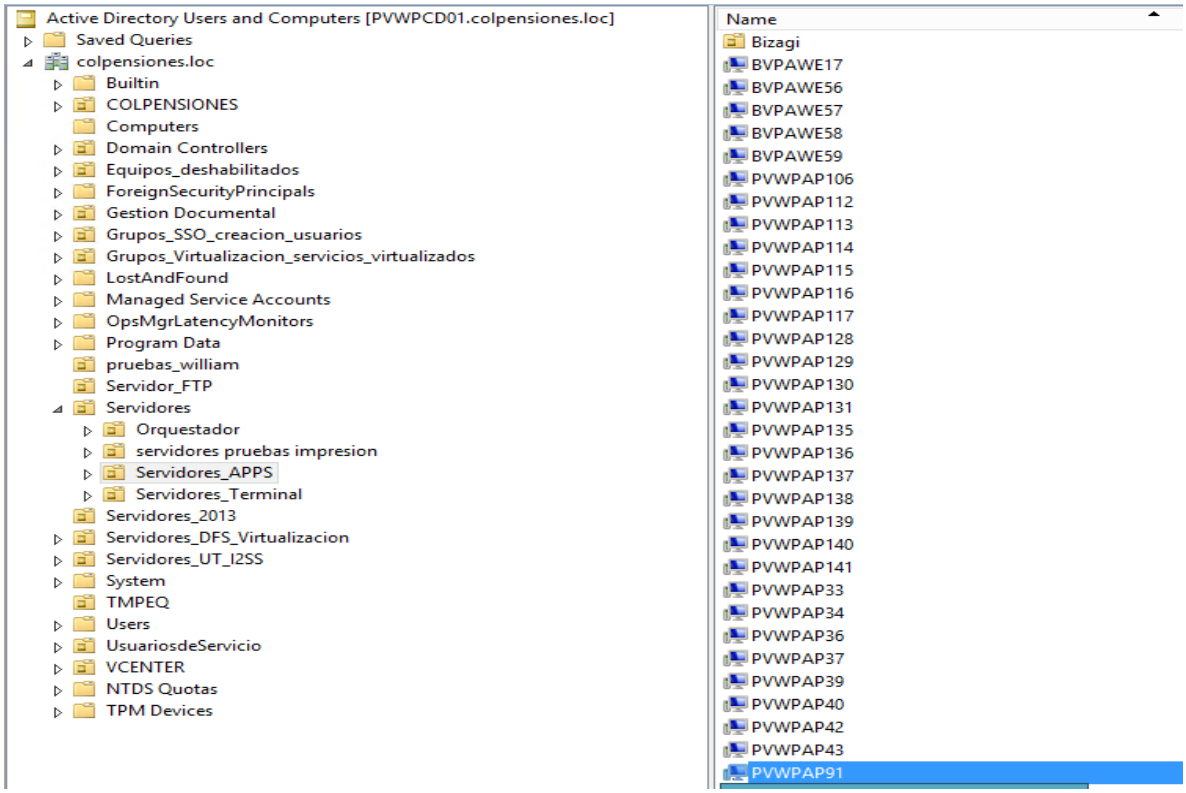
Figura 3. Políticas de seguridad aplicadas a los servidores



Fuente: el autor

En esta imagen se puede ver la ubicación del servidor entregado dentro de la unidad organizativa a la que aplican las políticas vistas en la imagen anterior

Figura 4. Ubicación de la máquina pvwpap91 en la unidad organizativa

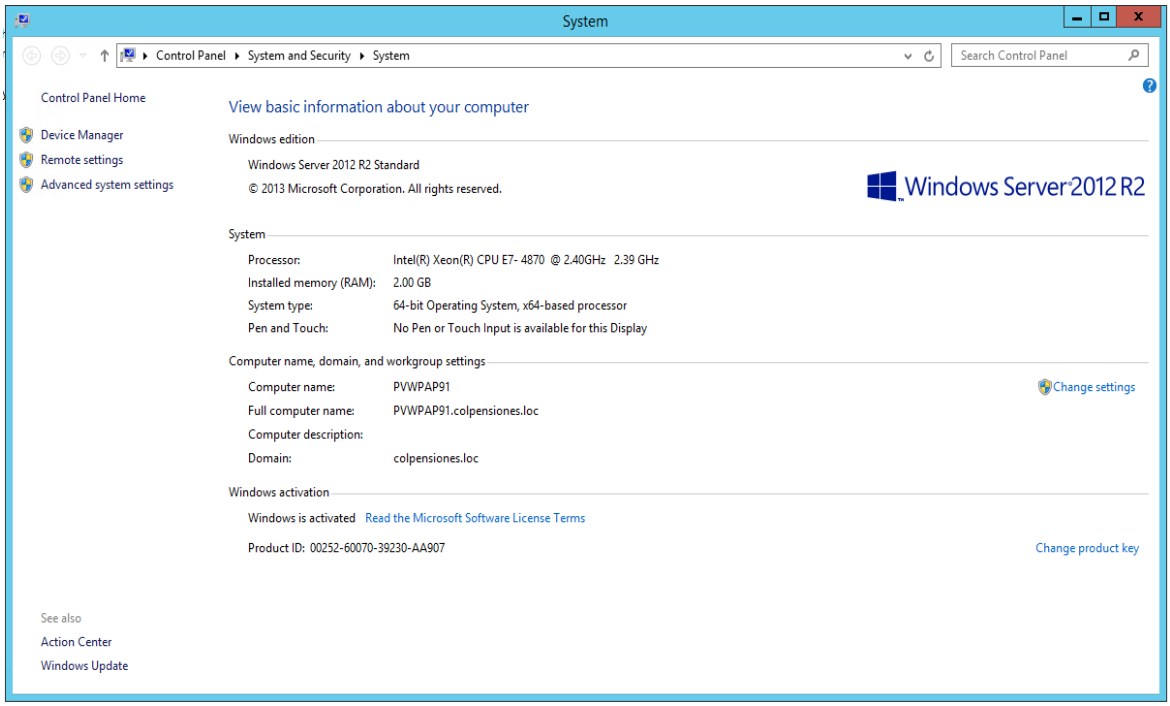


Fuente: el autor

12.3 Fase 2 Configuración Del Rol De Entidad Certificadora En El Servidor Windows Entregado En La Etapa Previa.

El área de capacidad entrega la siguiente máquina:

Figura 5. Máquina entregada por el área de capacidad para el montaje de la CA



Fuente: el autor

Un servidor configurado en Windows 2012 R2 utiliza una licencia de programa adquirida a la empresa Microsoft, con la instalación de este sistema operativo, Windows entrega la posibilidad de configurar el servidor con los roles que se necesiten para cumplir con las tareas necesarias de acuerdo al uso que se le dará a la máquina. Para instalar un sistema operativo Windows, se deben seguir las indicaciones que entrega el fabricante a través de manuales de instalación, para el caso de Colpensiones se tiene un contrato con el proveedor por el cual se proporciona personal técnico calificado quien es finalmente el que realiza la instalación del sistema operativo. Para este caso en particular, después de tener

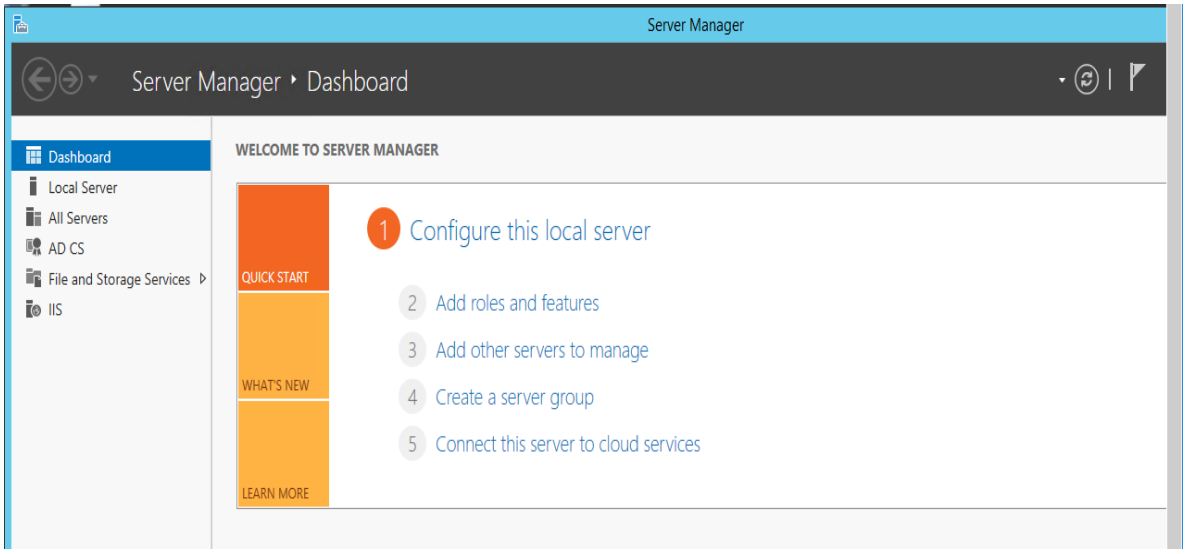
configurado el sistema operativo, se procede a darle el rol o tarea de entidad certificadora.

En Windows 2012 r2, el rol de ca es una función que viene incluida en el sistema operativo instalado, esta función permite configurar el servidor como una entidad certificadora local.

Para configurar la entidad certificadora, no se necesita instalar un programa aparte al del sistema operativo, se hace necesario realizar configuraciones y parametrizaciones de windows2012 que permiten el funcionamiento de la entidad certificadora.

En la siguiente imagen se describe el acceso a la adición de roles de sistema operativo en donde se encuentra el de entidad certificadora del sistema operativo windows

Figura 6. Adicionando roles al sistema operativo

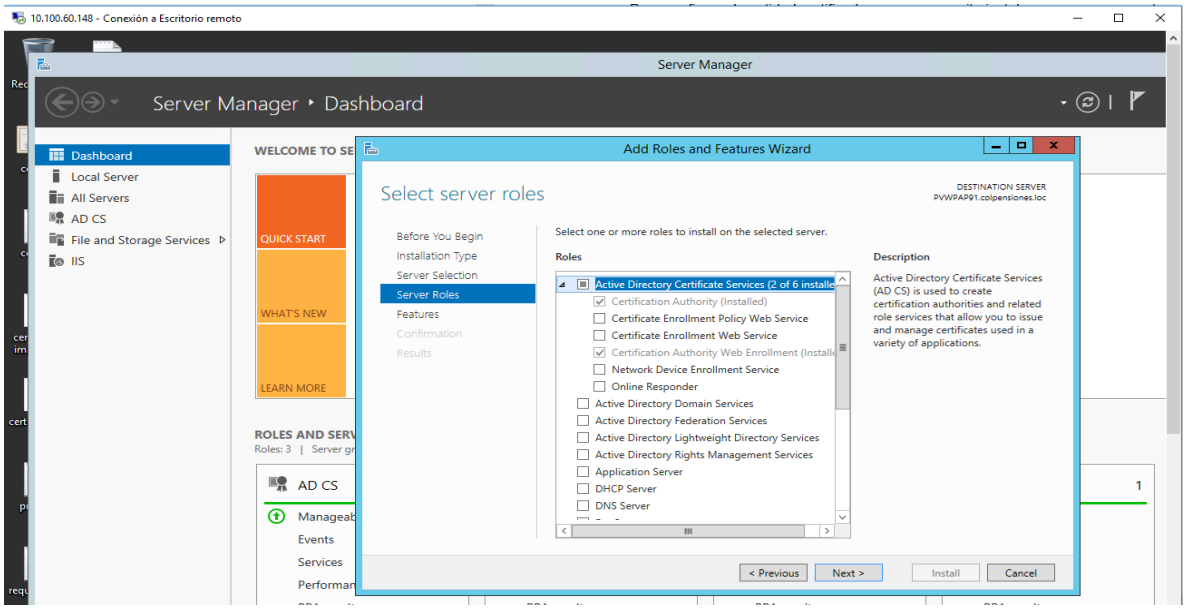


Fuente: el autor

Para configurar el rol de ca, se ingresa al servidor con un usuario que tenga permisos de administrador sobre la máquina, se busca el ítem de configuración de roles del sistema operativo, se le indica al sistema que se instalará un nuevo rol.

Posteriormente, se escoge la función de entidad certificadora o active directory certificated services en inglés como se aprecia en la imagen y el sistema empieza a realizar las preguntas necesarias con las que se va configurando la función. La entidad certificadora ofrece opciones de entidad certificadora que es la que está seleccionada y es la apropiada para los sitios, web, las otras opciones son para la generación de matrículas de certificados de servicios soa, también se puede apreciar en la imagen otro tipo de rol como dhcp, dns directorio activo y otros que para el caso no son necesarios y no se configuran, pues le servidor configurado prestará únicamente el servicio de entidad certificadora.

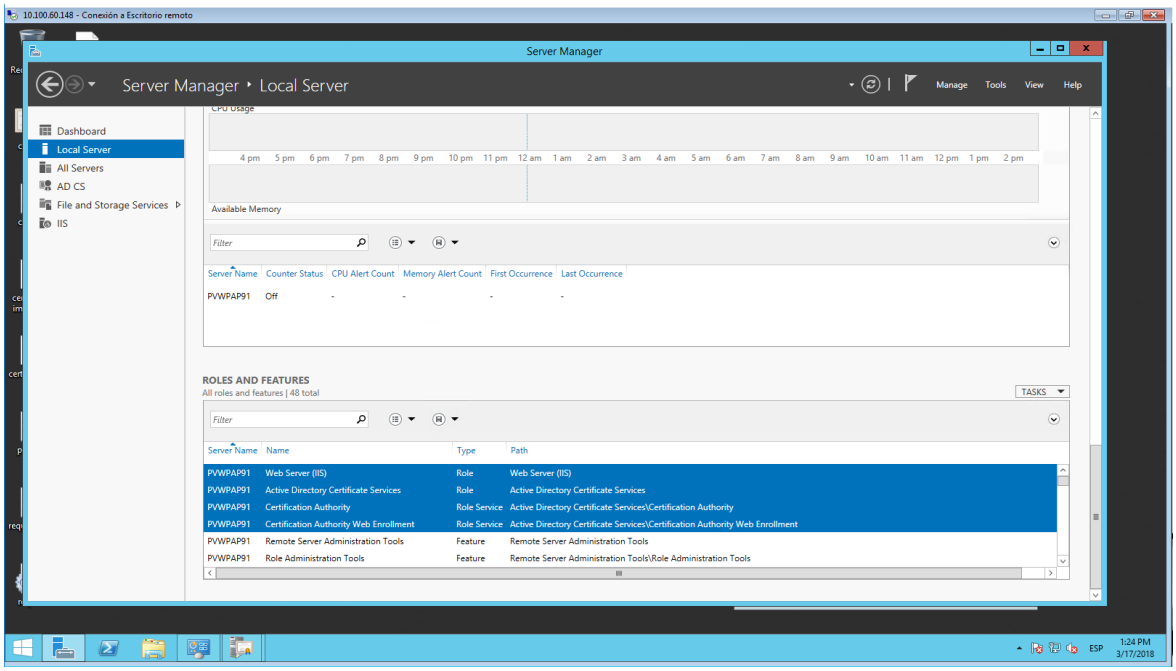
Figura 7. Configurando la entidad certificadora



Fuente: el autor

Después de escoger el rol de entidad certificadora, el sistema configura el rol específico escogido y reportará al finalizar el proceso que ya ha configurado la característica o función de entidad certificadora, en el texto resaltado en azul de la imagen siguiente, se aprecia la función de entidad certificadora, en inglés active directory certificate services, esto significa que la entidad se ha configurado y sin contratiempos.

Figura 8. Confirmando el rol de entidad certificadora

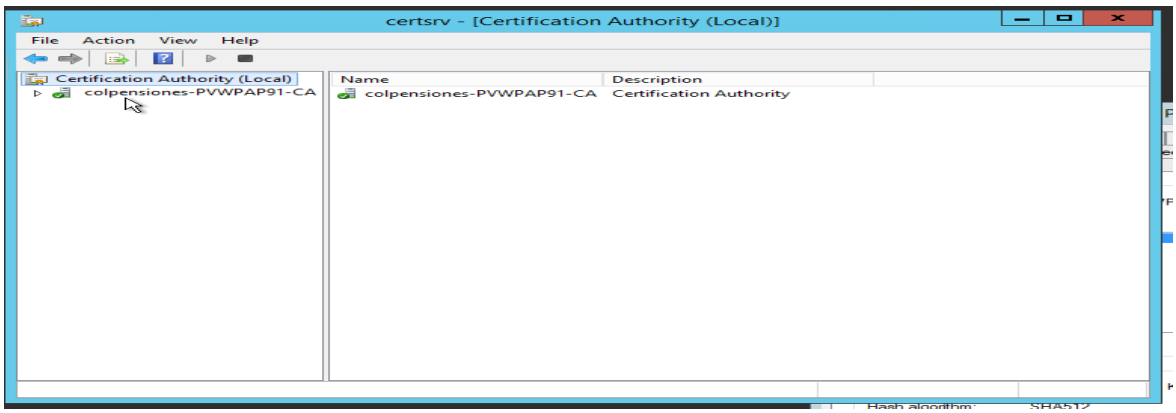


Fuente: el autor

La imagen anterior muestra el rol de entidad certificadora configurado, adicionalmente, ya que los requerimientos de certificados se hacen vía web, el servidor configura automáticamente el rol de web server (ii) el cual permite alojar el sitio o página web que permitirá la generación y descarga de los certificados solicitados por los servidores de aplicaciones

Después de verificada la instalación del rol de entidad certificadora, se revisa el estado del servicio de entidad certificadora, en la imagen presentada a continuación, se evidencia que el servidor virtual presenta el nombre de máquina y el estado en verde indica que la CA está operativa

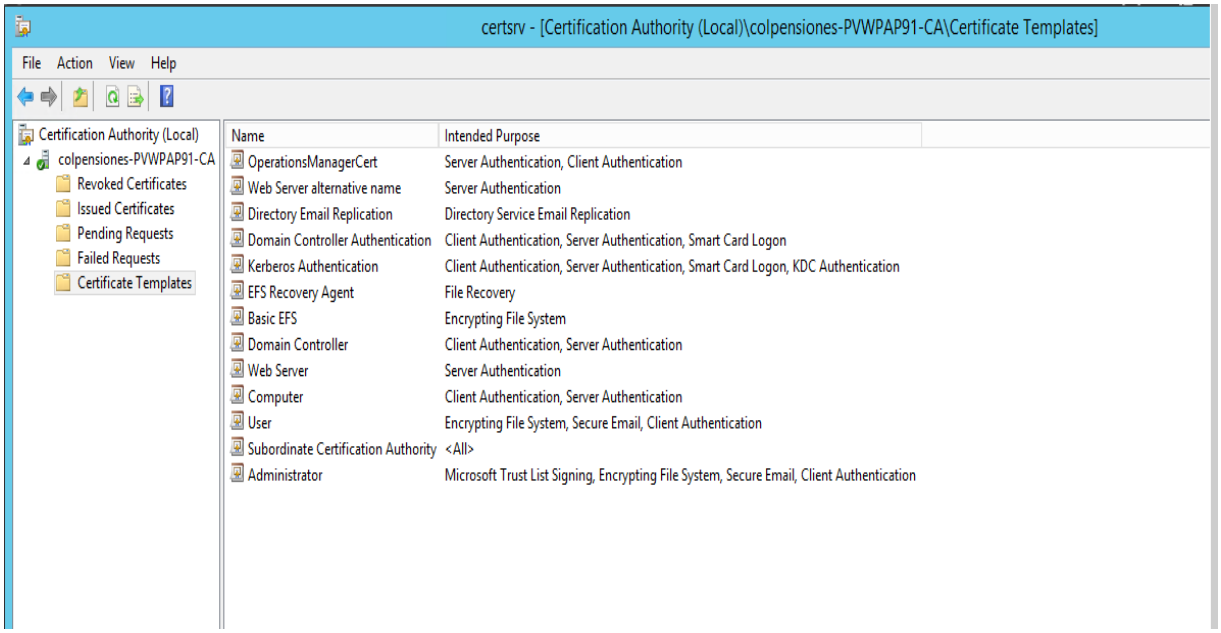
Figura 9. Confirmando la configuración en el servidor



Fuente: el autor

Después se confirma el estado de certificaciones y plantillas de certificación, en la imagen se describe el estado de los servicios que tiene la entidad certificadora, ingresando por plantillas certificadas o certificate templates, se verifica que la plantilla de servidor web esté disponible, pues esta es la que se usará para la generación de los certificados. En las otras carpetas se pueden ver los certificados generados, los que se encuentran pendientes de generar, los revocados

Figura 10. Estado de Plantillas y certificaciones

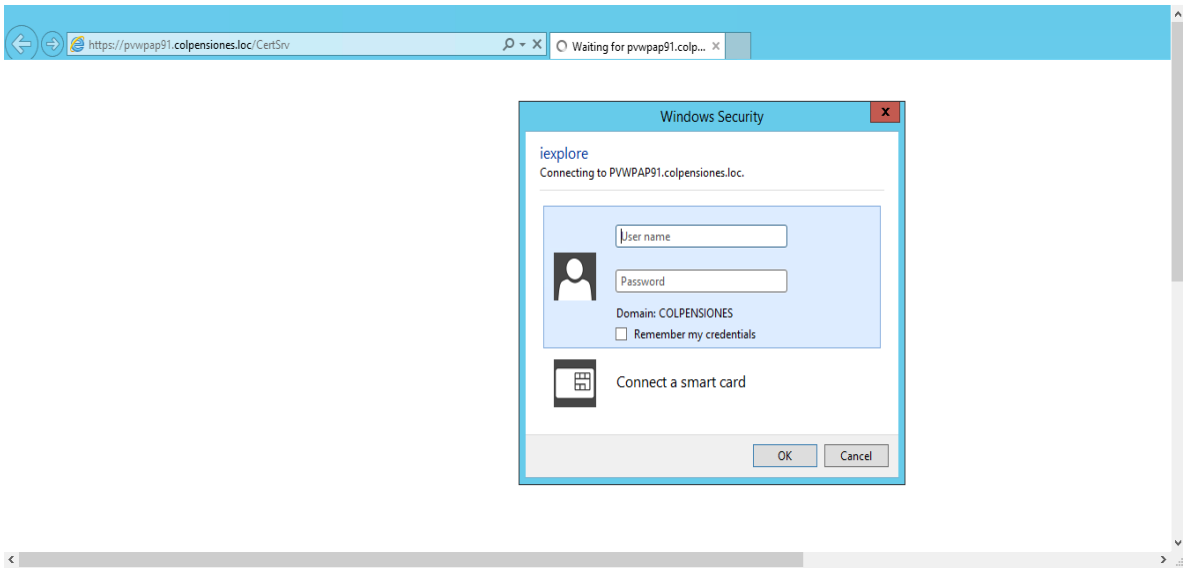


Fuente: el autor

Después de comprobar el funcionamiento y la configuración de la entidad certificadora, se procede a ingresar vía web para validar los servicios, pues a partir de esta página es de donde se empezarán a emitir los certificados digitales a partir de un requerimiento hecho por cada uno de los servidores que se va a publicar en modo seguro

Se ingresa con la url del sitio web y se usan las credenciales de administrador como se observa en la imagen

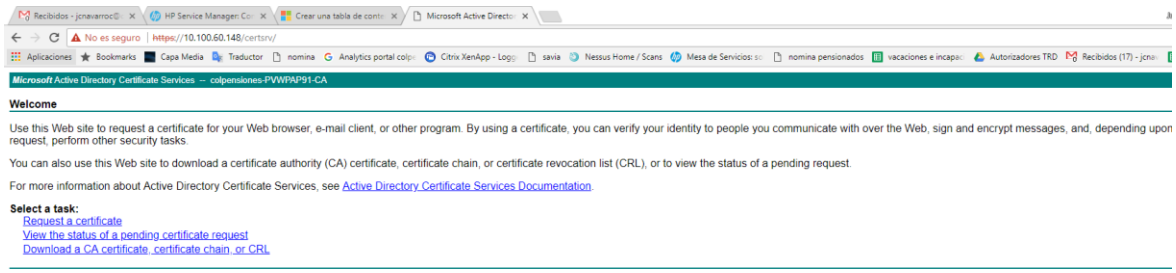
Figura 11. Ingresando a la entidad certificadora



Fuente: el autor

Después de que el sistema valida las credenciales de acceso se ingresa al menú de servicios de la entidad certificadora

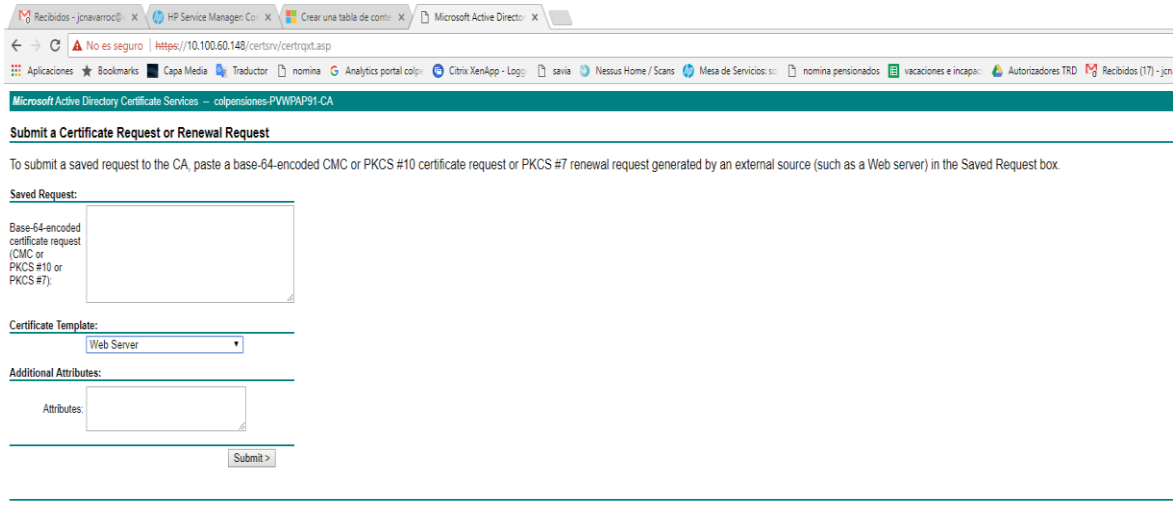
Figura 12. Desplegando menús de CA



Fuente: el autor

Después de navegar por el menú de funciones, se llega a la herramienta generadora de certificados, en esta se copia en el recuadro de requerimiento o request, el requerimiento generado por los servidores de aplicación y se procede a generar el certificado para instalar en la aplicación y publicarla de forma segura después de esto

Figura 13. 13 validando el acceso



Fuente: el autor

Después de realizar las acciones de configuración, la máquina queda operativa como CA y el paso siguiente es la solicitud de permisos de acceso para que las estaciones y máquinas de trabajo puedan ver la entidad de certificados en la red de la empresa. Después de la generación de permisos de firewall, la máquina queda con acceso a la red completa de Colpensiones.

12.4 Fase 3 Pruebas Previas Sobre la Publicación Actual de Aplicaciones

Una vez se tiene la entidad certificadora, antes de dejarla operativa y en producción, es necesario generar pruebas de seguridad para certificar que no se podrá duplicar la máquina, duplicar la entidad certificadora o emitir certificados falsos que puedan engañar o verificar sitios sin que sean emitidos desde la CA real.

12.4.1 Fase 3 Duplicando un servidor dentro del dominio

La empresa tiene un proveedor de servidores y equipos que crean las máquinas y las entregan a las diferentes áreas solicitantes, las máquinas entregadas son virtuales, el sistema operativo de estos servidores genera un código de identificación único y los equipos entregados ya vienen con dirección ip y mac instaladas y adaptadas a la vlan que pertenezcan.

Sin embargo, por ser máquinas virtuales, eventualmente se podría hacer una copia del archivo de la máquina más conocido como snapshot y emplear este después para hacer un clon de la máquina.

Se supone entonces, que un usuario mal intencionado con acceso a la red y a virtualización vmware del proveedor, crea un snapshot de la máquina PVWPAP91 la cual es la entidad certificadora entregada.

Al activar la máquina clonada, un error de red por nombre de máquina y dirección ip duplicada aparece en la red. Para solucionar el error es necesario apagar alguna de las dos máquinas, en este caso se apaga la máquina original y los errores de duplicidad en la red desaparecen, sin embargo, como cada equipo tiene un identificador único llamado objectSid, este código no coincide con el matriculado en directorio activo que conserva el objectSid del servidor original que se encuentra

apagado. Al intentar ingresar al dominio, el sistema arroja un error de acceso indicando que se ha perdido el nivel de confianza entre la máquina y el dominio.

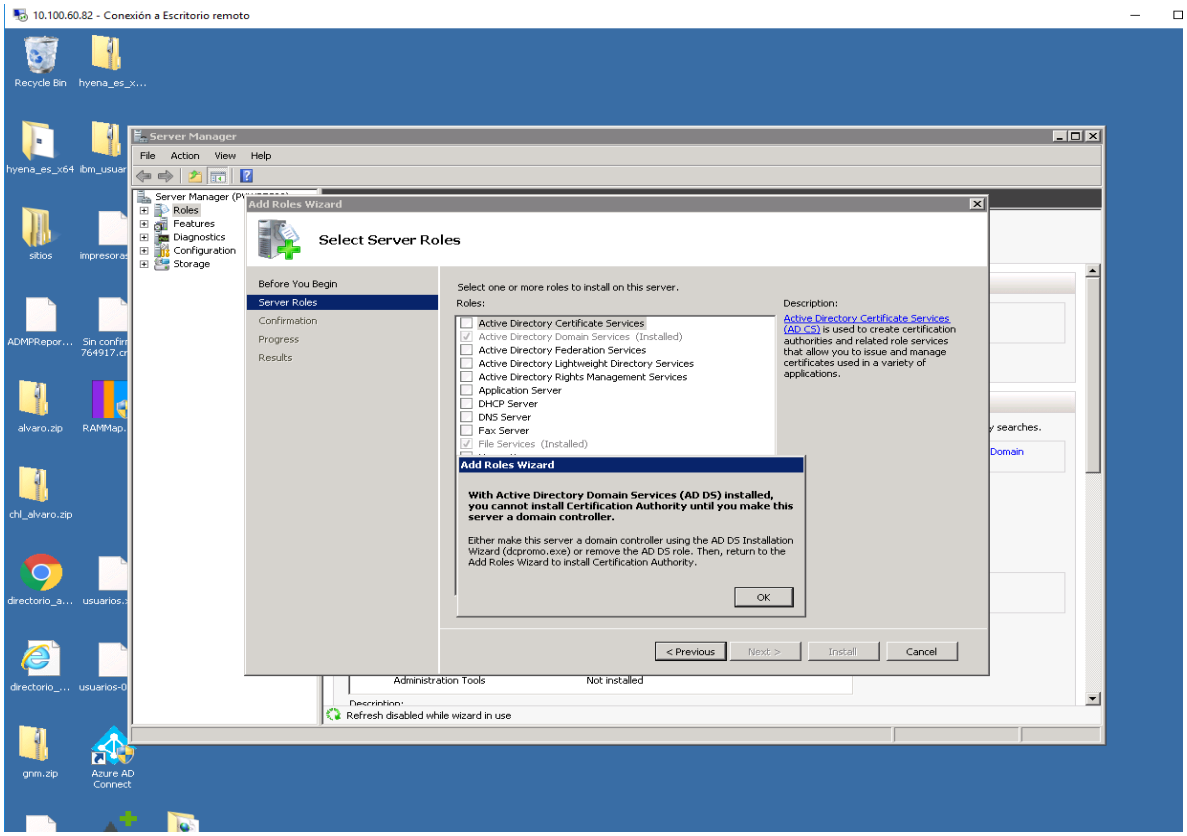
En esta actividad, hay varios puntos de control, en el evento de tener duplicidad de direcciones en la red, un reporte es enviado de inmediato a al área de redes y firewall para que se determine el origen de la falla y se detectaría el intento.

En caso de que se lograra apagar la máquina original e intentar usar el clon sin que no se detectara el usuario mal intencionado, al querer ingresar a la máquina, el directorio activo detecta que el objectSid no es el mismo y se rompe la relación de confianza con la máquina y no se permite el acceso.

Contando con que el atacante tenga éxito en apagar la máquina original, y pueda obtener claves de administrador del directorio activo, la virtualización de vmware también tiene puntos de control para evitar la suplantación de las máquinas de trabajo, vmware tiene una función llamada spoofGuard, que está diseñada para prevenir este tipo de ataques mediante la comparación de la dirección mac de las máquinas relacionadas con su respectiva dirección ip asignada.

Por último, un atacante puede intentar simplemente asignar el rol de entidad certificadora desde otro servidor válido en la red, pero al intentar realizar la acción, el sistema de Windows indicará que la máquina debe estar dentro del dominio, si el servidor está ya matriculado dentro del dominio, el rol de instalación configura esta máquina como una entidad certificadora subordinada a la original, pero n o la duplica o la suplanta.

Figura 14. Intentando duplicar la Entidad Certificadora



Fuente: el autor

12.4.2 Fase 3 Solicitud de Permisos de Acceso y Apertura de Puertos en Cortafuegos.

Después configurado el servidor con el rol de entidad certificadora, y asegurada la máquina usando la plantilla de aseguramiento establecida, es necesario proteger aún más la máquina de intentos de acceso no deseados.

Colpensiones tiene instalados varios cortafuegos de la marca Palo Alto, la configuración de estos dispositivos tiene restringido el acceso a todos los lugares de la red, y se abren puertos y protocolos previa solicitud del área interesada para

ir dando acceso controlado a los recursos y conectividad con otras máquinas de la red.

En este caso se procede a solicitar permisos desde las direcciones ip de las máquinas de trabajo de los funcionarios que estarán encargados de administrar la entidad certificadora. Para estas personas se solicita acceso a través del puerto tcp 3389, este puerto es por donde generalmente se solicita la conexión de escritorio remoto para máquinas Windows, al tener abierto este puerto los administradores de la entidad, podrán ingresar al servidor para realizar las labores propias del sistema.

En caso de existir un intento de acceso no autorizado al servidor de CA desde una dirección ip no autorizada en el firewall, el dispositivo cortafuegos no permite la conexión asegurando el acceso solo a los administradores desde la estación de trabajo establecida.

Las conexiones de escritorio remoto adicionalmente se encuentran protegidas con certificados digitales ssl usando las opciones de configuración de huella digital de certificado con lo cual se asegura que la escucha de rdp es segura y el acceso se asigna únicamente a una máquina previamente establecida y uno una que esté intentando suplantar el acceso.

Adicionalmente, es necesario tener abiertos en cortafuegos los puertos tcp : 88, 389, 445, 443

El puerto 88 es usado por el protocolo de autenticación kerberos, para dar mayor seguridad de acceso al servidor de la entidad certificadora, la autenticación se hace a través del protocolo kerberos el cual es usado por el directorio activo de Colpensiones.

Kerberos es un protocolo de autenticación seguro que hace un cifrado de datos y usa las credenciales de usuario para desencriptar los datos cifrados sin tener la necesidad de que la contraseña de usuario viaje por la red y esta sea usada solo por el programa de login ubicada en el cliente.

El puerto 389 es usado para las conexiones ldap normales y el 445 para compartir archivos.

Ldap es una interfaz utilizada para poder hacer validaciones de acceso o escritura del directorio activo, la entidad certificadora está ligada al dominio de Colpensiones y eventualmente podría necesitar este tipo de servicio de autenticación por lo cual es necesario dejar el puerto abierto desde un segmento de direcciones de red determinado.

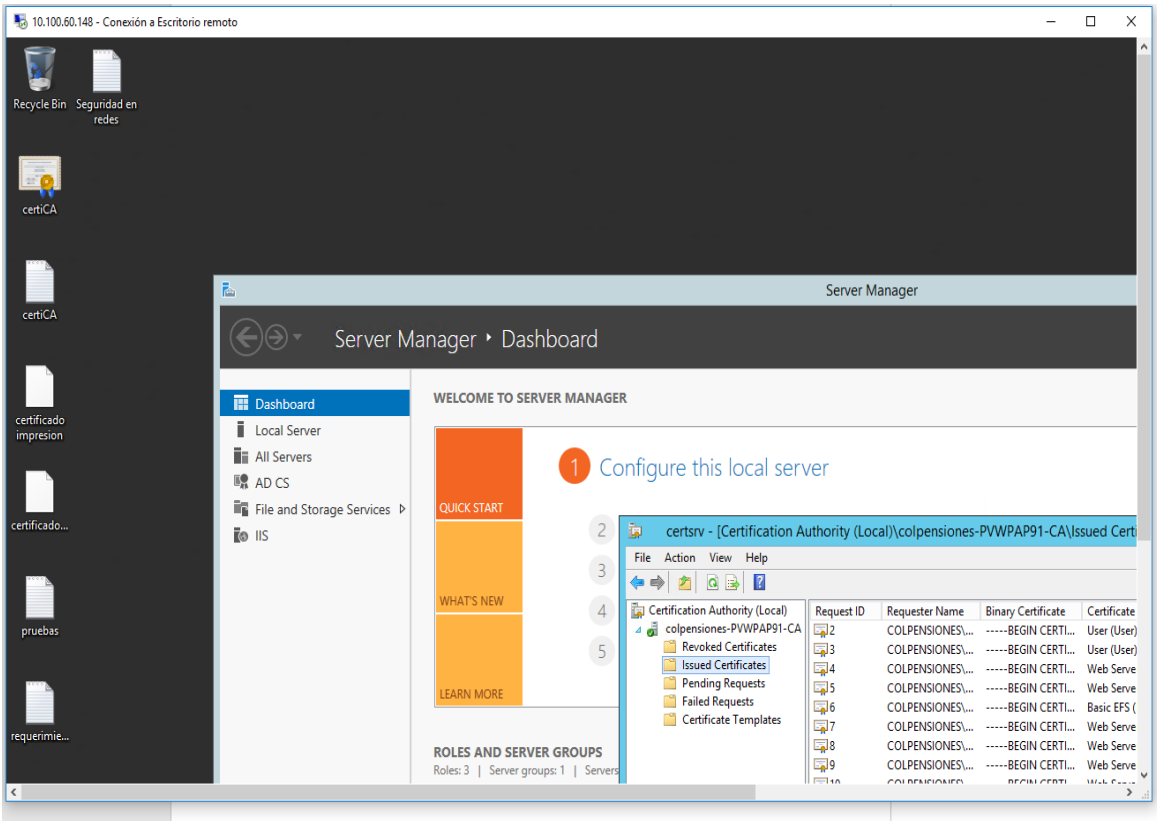
Se solicita también tener abierto el puerto 443, este puerto tcp es utilizado para proporcionar conexiones seguras a sitios o aplicaciones web, este permiso es habilitado desde un rango de direcciones para que las personas encargadas de emitir los certificados, puedan ingresar vía web a la entidad certificadora y hacer el requerimiento y descarga de los certificados digitales desde una plataforma cifrada

Una vez confirmados los puertos y url abiertos, por el área de seguridad se ingresa al servidor desde una de las máquinas de red para probar su correcto funcionamiento.

Los permisos de acceso son requeridos para que los servidores de aplicaciones puedan conectarse con la CA y sea posible identificar los certificados como válidos, de lo contrario una aplicación no podría validar el certificado digital.

En esta imagen se puede apreciar la entidad de certificación completa con el listado de certificados que se han generado para la implementación de https en algunas aplicaciones web de la entidad.

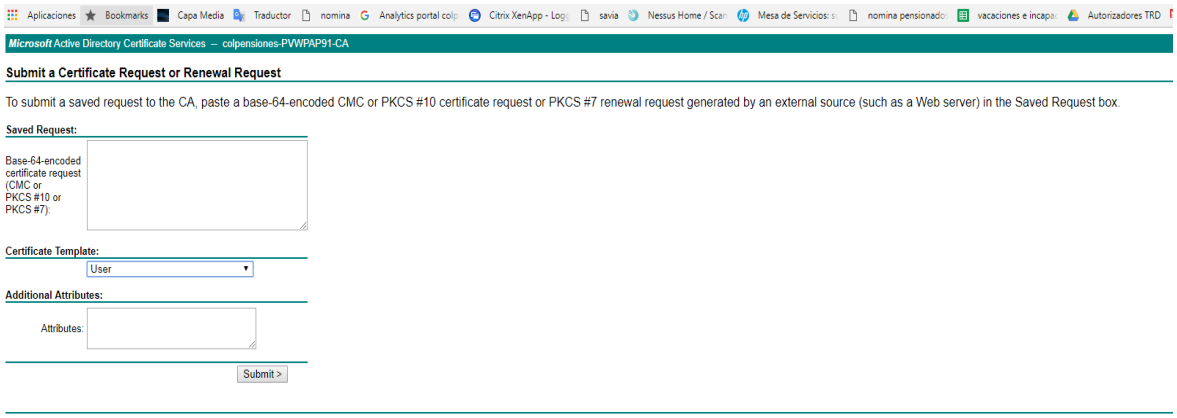
Figura 15. Validando el listado de certificados



Fuente: el autor

Después de los afinamientos respectivos, la Ca queda lista para la generación de certificados web que sean reconocidos en la entidad como seguros:

Figura 16. Entidad certificadora lista para emitir certificados



Fuente: el autor

Fase 4 Publicar las aplicaciones web locales cifradas a través de certificados digitales y en formato https.

Después de tener instalada la entidad certificadora, es posible empezar a configurar todas las aplicaciones web que el área de infraestructura requiera que operen sobre sitio seguro ssl.

La importancia que tiene la instalación de la entidad certificadora, es que las aplicaciones a las que se les cree un certificado digital y se publiquen por https, viajarán de manera cifrada sobre la red de Colpensiones y los valores y datos privados no podrán ser detectados por analizadores de red puesto de forma voluntaria o involuntaria, lo anterior, garantiza que las contraseñas y todos los datos sensibles de una aplicación web predeterminada estarán viajando de manera segura sobre la red si son publicados en https.

Todo el trabajo de la creación de un servidor virtual, una entidad certificadora local y la expedición de certificados digitales enmarca dentro del trabajo de seguridad de

la información completamente, pues para poder llevar a cabo este proyecto, fue necesario profundizar conocimientos sobre cifrado, certificados digitales, aseguramiento de hardware, solicitud de requerimientos especiales de certificados, leyes y normas de seguridad en Colombia y otros temas más relacionados con la seguridad y aseguramiento de la información.

13 RESULTADOS OBTENIDOS

Una vez instalada la entidad certificadora de Colpensiones, los resultados obtenidos fueron los siguientes:

No fue posible clonar la máquina de entidad certificadora a través de la suplantación del servidor, pues se implementaron varios controles que aportan seguridad y protección en cuanto a ataques de este tipo.

Dentro de los controles implementados, está el aseguramiento de la máquina usando una plantilla establecida previamente para reforzar el acceso y manejo de contraseñas y recursos compartidos dentro de la máquina.

Aseguramiento de enrutadores, se usó una plantilla de aseguramiento de dispositivos de comunicaciones, en este caso del enrutador de salida de red, esta plantilla fija configuraciones de accesos de contraseñas y reforzamiento de funciones para evitar ataques de ransomware entre otros.

Filtrado de tráfico a través de cortafuegos, se configuró el filtrado de datos para el servidor de la entidad certificadora con todas las salidas bloqueadas y se habilitaron los puertos, direcciones ip y protocolos exclusivamente para los servicios requeridos evitando dejar huecos de acceso que pudieran ser aprovechados por atacantes.

Aseguramiento a través de reglas de directorio activo, se crearon políticas de acceso y manejo de los recursos de la entidad certificadora mediante creación de reglas de acceso desde el directorio activo de la entidad, esto proporciona seguridad y exclusividad en los accesos y privilegios de las acciones que pueden realizar los usuarios que usan la máquina virtual de entidad certificadora

Después de implementar la CA local para Colpensiones, se mitigó la vulnerabilidad encontrada en donde los datos viajaban en texto claro por la red, pues desde el momento en que se publica una aplicación, esta se configura de modo seguro cifrando los datos que se usan en las conexiones y transferencias de información.

Enfocado dentro de la seguridad de la información, la aplicación de este proyecto está garantizando que la confidencialidad, integridad y disponibilidad de la información implicada en cada aplicación web que se publique de manera segura se encuentre protegidas y mitigando riesgos que puedan poner en peligro los datos que viajan en dichas aplicaciones.

Los resultados obtenidos, permiten afirmar que, con el uso de la entidad certificadora, Colpensiones está en la capacidad de publicar sitios web seguros protegidos con certificados digitales que permiten la conexión segura entre usuarios y aplicaciones conservando las premisas de seguridad de la información como lo son su disponibilidad, integridad y confidencialidad.

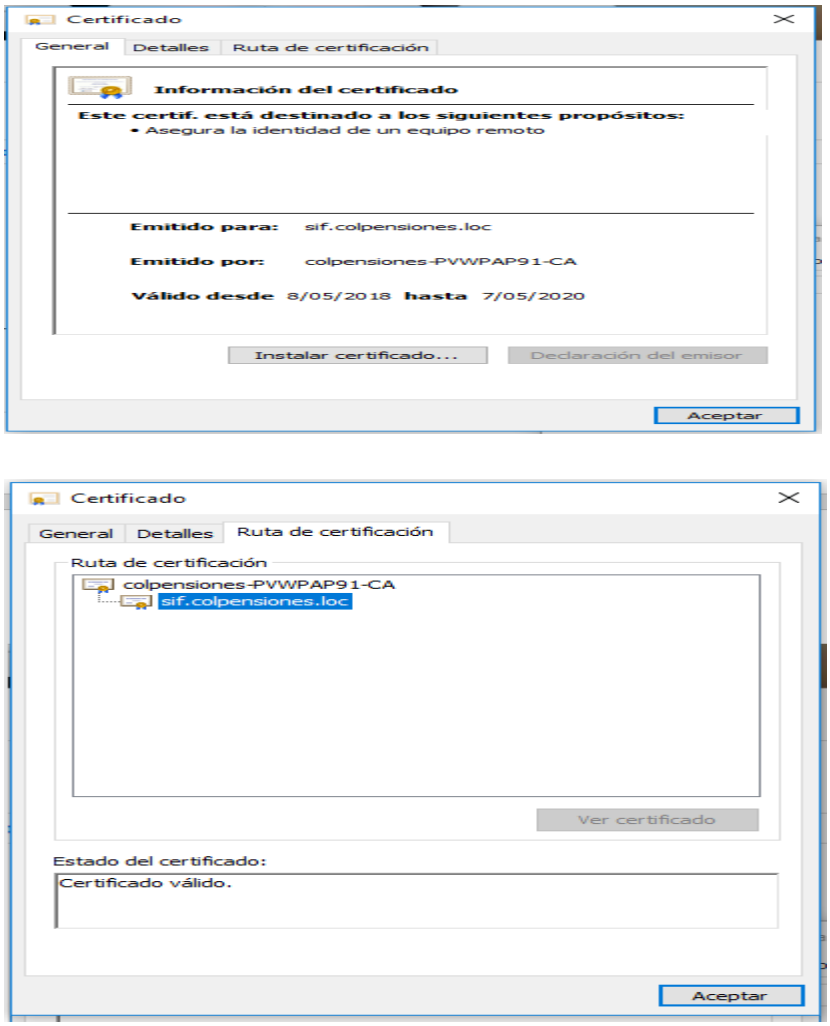
Después de generar la entidad certificadora local, y realizadas las pruebas de funcionamiento descritas anteriormente, se procede a crear certificados y publicar las aplicaciones en formato https para que estas sean seguras.

En esta etapa, el problema inicial en donde las aplicaciones viajaban por la red en texto claro se ha resuelto, pues al configurarse la publicación de estas sobre ssl, ya no es posible obtener información sensible con un analizador de red protegiendo los datos que viajan en la red pertenecientes a la aplicación protegida.

De esta manera y gracias a las medidas de seguridad informática aplicadas se resolvieron los problemas de vulnerabilidad encontradas en los hallazgos de auditoría.

Recientemente se generó un certificado para la aplicación sif de Colpensiones usando el certificado generado por la ca montada:

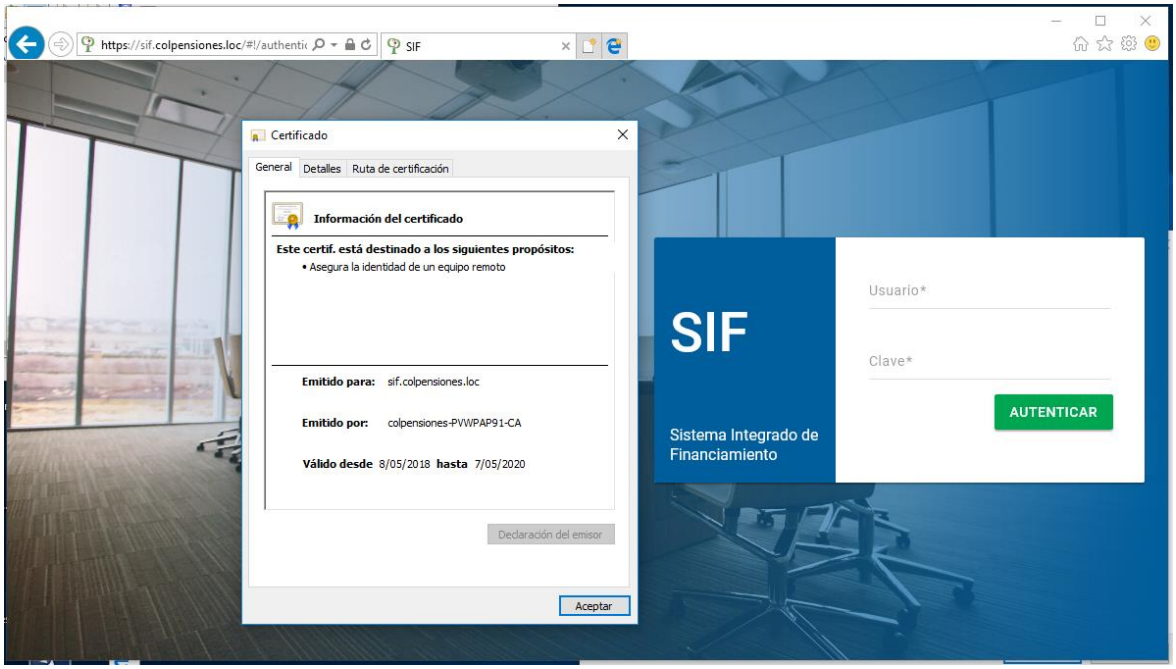
Figura 17. Certificado generado para una de las aplicaciones web



Fuente: el autor

En la siguiente imagen se aprecia la aplicación funcionando con el certificado creado por la entidad certificadora montada:

Figura 18. Aplicación funcionando de manera cifrada



Fuente: el autor

Después de la implementación y puesta en marcha de la entidad certificadora se han configurado varios sitios seguros con lo que la entidad se ha ahorrado el costo económico de la compra de certificados digitales a entidades ca externas, adicionalmente, los sitios locales en los ambientes de producción, calidad e integración pueden ser publicados en protocolo https eliminando el hallazgo de vulnerabilidad encontrado en las auditorías de seguridad realizadas y cumpliendo con las expectativas propuestas.

Los sitios publicados de forma segura hasta la fecha son:

Manual de funciones integración: esta aplicación web es usada por los jefes de área para interactuar con la aplicación sap y llevar informes detallados de las funciones de cada empleado a su cargo en el ambiente de integración

Manual de funciones Calidad: esta aplicación web es usada por los jefes de área para interactuar con la aplicación sap y llevar informes detallados de las funciones de cada empleado a su cargo en el ambiente de Calidad

Manual de funciones producción: esta aplicación web es usada por los jefes de área para interactuar con la aplicación sap y llevar informes detallados de las funciones de cada empleado a su cargo en el ambiente de producción

Indicadores de presidencia calidad: este aplicativo web permite consultar los indicadores de quejas y reclamos generados por los ciudadanos desde el portal de Colpensiones en el ambiente de calidad

Indicadores de presidencia integración: este aplicativo web permite consultar los indicadores de quejas y reclamos generados por los ciudadanos desde el portal de Colpensiones en el ambiente de integración

Indicadores de presidencia producción: este aplicativo web permite consultar los indicadores de quejas y reclamos generados por los ciudadanos desde el portal de Colpensiones en el ambiente de producción

Sif calidad: la aplicación web de sif maneja el sistema integrado de financiamiento en calidad

Sif Integración: la aplicación web de sif maneja el sistema integrado de financiamiento en integración

Sif producción: la aplicación web de sif maneja el sistema integrado de financiamiento en producción

Con los resultados obtenidos, la creación de la entidad certificadora local cumplió con las expectativas y objetivos propuestos en el presente trabajo, pues después de la implementación de la entidad certificadora local de Colpensiones, la compañía está en la capacidad de ofrecer las aplicaciones locales completamente cifradas, y

las que se han configurado por ssl viajan de forma protegida sobre la red de la empresa.

Adicionalmente a tener las aplicaciones web protegidas después de la implementación de este trabajo, Colpensiones ha ahorrado recursos económicos importantes en la compra de certificados digitales, pues ahora se compran exclusivamente aquellos certificados que, por fuerza mayor o circunstancias legales, deben ser expedidos por un organismo especializado en estas tareas.

Antes de la instalación de la entidad certificadora, Colpensiones debía publicar todas las aplicaciones web internas a través de texto claro en http, la información sensible como contraseñas y datos de ciudadanos se podía capturar de una forma relativamente fácil, en una auditoría de seguridad se encontró un hallazgo y un riesgo de seguridad por este hecho.

Con la implementación de la entidad certificadora local de Colpensiones, se cambió la publicación de las aplicaciones en un protocolo inseguro, a la publicación de estas mismas aplicaciones sobre un protocolo seguro https con lo que se mejoró notablemente la seguridad de la información sobre las aplicaciones web locales de la empresa.

Lo anterior, evidencia la importancia de la implementación de la entidad certificadora y el mejoramiento sustancial que tuvo la compañía sobre la seguridad de los datos que viajan por la red, razón más que sustentada para afirmar que las acciones ejecutadas para hacer una realidad la implementación de la propuesta de creación de la ca en Colpensiones fue un trabajo efectivo gracias a la aplicación de los conocimientos adquiridos del componente de seguridad informática del autor.

Con la implementación de este proyecto, la empresa obtuvo beneficios muy importantes en cuanto a la seguridad de la información de las aplicaciones web, pues actualmente la compañía está en la capacidad de publicar en protocolo seguro

y de forma cifrada las aplicaciones web locales haciendo más robusta y segura la plataforma web de la empresa.

Se pasó de tener aplicaciones web publicadas de forma insegura a contar con una plataforma completa de generación de certificados digitales locales que permiten publicar en protocolo https y de forma cifrada estas mismas aplicaciones sin tener la necesidad de compras a entes externos de los certificados.

14 RECOMENDACIONES

Después de tener la entidad certificadora funcionando y las aplicaciones anteriormente descritas trabajando de forma cifrada, se recomienda publicar la totalidad de las aplicaciones web locales en https con certificados digitales emitidos por la entidad certificadora implementada.

Es necesario crear un manual de generación de certificados para que los líderes técnicos encargados de cada una de las aplicaciones web tengan los conocimientos necesarios y pueda crear un requerimiento de certificado digital apropiado para el funcionamiento correcto del sitio una vez se haya cifrado.

Es necesario generar un certificado digital raíz de confianza de la entidad certificadora creada y entregar este a los proveedores, con el objetivo de que este certificado sea instalado en los dominios de cada empresa y extender el cubrimiento de los certificados que permiten la protección de los sitios a los dominios de proveedores.

Se requiere un escaneo de vulnerabilidades periódicamente, para asegurar que la entidad certificadora está protegida contra ataques.

15 CONCLUSIONES

Se creó una entidad certificadora local, cuya plataforma base es un servidor virtual Windows 2012 con el objetivo de proporcionar certificados digitales reconocidos por la empresa Colpensiones y sus sistemas tecnológicos, para poder publicar las aplicaciones web en ambiente https

Se realizaron pruebas de seguridad intentando clonar la máquina de entidad certificadora usando varios métodos sin éxitos

Se intentó suplantar un certificado digital en un servidor diferente al del requerimiento normal, pero al ser instalado no es exitoso su funcionamiento.

Después de la instalación de la entidad certificadora, se estableció un formato base para el requerimiento de certificados que debe hacer una aplicación de manera estándar ante la cd de Colpensiones, optimizando la longitud, orden y campos a contener en un certificado y dejando los parámetros de manera uniforme para todas las aplicaciones

La entidad certificadora generó certificados de raíz de confianza que se instalaron en los dominios de otros proveedores, lo cual permitió extender el funcionamiento de la ca y evitar la compra de certificados externos para autenticarse frente a estos proveedores

La generación de certificados, además de permitir la publicación de aplicaciones de forma segura, también permitió implementa el acceso ldap de usuarios a los servidores del portal institucional de manera encriptada a través de certificados digitales mejorando la seguridad de acceso de estos sitios web

16 BIBLIOGRAFIA

AD CS CERTIFICATION AUTHORITY {en línea} {consultado 2017) Disponible en https://technet.microsoft.com/en-us/library/cc726345(v=ws.10).aspx

AUTORIDADES CERTIFICADORAS (CA) {en línea} {consultado noviembre 2017}. Disponible en: http://www.fundacionaccesible.org/biblioteca/certificado/pdf/AUTORIDADES%20CERTIFICADORAS.pdf

CERTIFICATION AIJTHORITY GUIDANCE {en línea} {consultado 2017) Disponible en https://technet.microsoft.com/en-us/library/cc726345(v=ws.10).aspx

Creación de una autoridad certificadora {en línea} Disponible en: http://bibing.us.es/proyectos/abreproy/90354/fichero/Memoria+Francisco+J.+Marchal+Cebador.pdf

Creación de una autoridad certificadora de firmas digitales {en línea} Disponible en: https://idus.us.es/xmlui/handle/11441/34524

CREAR UNA ENTIDAD CERTIFICADORA PRIVADA {en línea} {consultado Noviembre 2017}. Disponible en: www.ibm.com/support/knowledgecenter/es/SS8JFY_9.0.0/com.ibm.lmt.doc_.9.0/com.ibm.license.mgmt.doc/security/t_ca_private.html

Diseño de un esquema de certificación {en línea} Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/65814/Documento_completo.pdf-PDFA.pdf?sequence=1

ENTIDAD CERTIFICADORA {en línea} {consultado Noviembre 2017}.Disponible en: https://www.jmsolanes.net/es/entidad-certificadora

ENTIDADES DE CERTIFICACION INDEPENDIENTES {en línea} {consultado 2017) Disponible en https://technet.microsoft.com/es-es/library/cc755290(v=ws.11).aspx

FIRMA DGITAL EN COLOMBA {en línea} {consultado noviembre 2017} Disponible en: http://colombia.isigmaglobal.com/entidades-de-certificacion

GUÍA DE LA ENTIDAD DE CERTIFICACION {en línea} {consultado noviembre

2017}. Disponible en:
https://technet.microsoft.com/es-es/library/hh831574(v=ws.11).aspx

GUÍA DE LA ENTIDAD DE CERTIFICACION {en línea} {consultado noviembre 2017}. Disponible en:
https://technet.microsoft.com/es-es/library/cc732368(v=ws.11).aspx

Implementación de un modelo simplificado de firma digital basado en la tecnología PKI {en línea} Disponible en:
http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/4993/Aguilar_ag.pdf;jsessionid=04CEF8EFDC3369A2547A1C095AF4BAFC?sequence=1

Implementación de una infraestructura de clave pública con herramientas de software libre {en línea} Disponible en:
https://www.researchgate.net/publication/303212115_Implementacion_de_una_PKI_con_herramientas_de_software_libre

INSTALAR Y CONFIGURAR ENTIDAD DE CERTIFICACIÓN {en línea} {consultado noviembre 2017} Disponible en:
http://blogs.itpro.es/jairgomez/2013/12/16/instalar-y-configurar-entidad-de-certificacion-ca-en-windows-server-2012

INSTALAR Y CONFIGURAR ENTIDAD DE CERTIFICACIÓN {en línea} {consultado noviembre 2017} Disponible en:
https://www.gruposothis.com/entidad-certificadora-windows-parte-i-conceptos-e-instalacion-del-servicio

LEY 527 DE 199 {en línea} {consultado 2017) Disponible en
http://www.acaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

Propuesta De Implementación De La Firma Digital Para La Cooperativa Coopserp {en línea} Disponible en:
http://repository.udem.edu.co/bitstream/handle/11407/335/Propuesta%20de%20implementaci%C3%B3n%20de%20la%20firma%20digital%20para%20la%20Cooperativa%20Coopserp.pdf?sequence=1

SERVICIOS DE CERTIFICACIÓN DIGITAL {en línea} {consultado noviembre 2017} Disponible en:
https://www.andesscd.com.co/index.php?option=com_content&view=article&id=2ltemid=109

17 ANEXOS

Carta de aprobación de la propuesta firmada por el responsable del área

A continuación, se anexa la carta de aprobación de la propuesta por parte de la empresa Colpensiones:

Bogotá D.C. 21 de noviembre de 2017

Doctora:
ALEXANDRA APARICIO RODRÍGUEZ
Coordinadora Nacional Cadena de Sistemas UNAD
Bogotá D.C.

Asunto: APROBACIÓN PROYECTO ESTUDIANTE JUAN CARLOS NAVARRO

Por medio de la presente me permito informar que el señor **JUAN CARLOS NAVARRO CASTILLA** identificado con cédula de ciudadanía Nº **79.455.175** quien labora para la Administradora Colombiana de Pensiones – COLPENSIONES, tal como se establece en certificado laboral adjunto, en calidad de estudiante de la especialización de Seguridad Informática que cursa en esa institución planteó la implementación de una entidad certificadora local (CA) con tecnología Microsoft, es importante resaltar que la solución propuesta por el señor NAVARRO CASTILLA cumple con lineamientos institucionales necesarios para publicar localmente los sitios web seguros con certificados propios, de los cuales estamos en proceso de implementación.

Agradezco de antemano la atención prestada

Cordialmente,

Alberto Barajas Ramón
Asesor de Vicepresidencia
Coordinador Grupo de Seguridad Informática, SQA y Gestión de Accesos
Vicepresidencia de Planeación y Tecnologías de la Información
Calle 73 No. 10 – 70 Piso 4
Tel. (+571) 2170100 Ext. 1516
E-mail: abarajasr@colpensiones.gov.co
www.colpensiones.gov.co
Bogotá D.C. - Colombia

RESUMEN ANÁLITICO RAE

Título de Documento.	PROPUESTA PARA IMPLEMENTAR UNA ENTIDAD CERTIFICADORA LOCAL PARA COLPENSIONES.
Autor	JUAN CARLOS NAVARRO CASTILLA
Palabras Claves	Entidad, certificadora, certificado, cifrar, http, https, rol, sistema, requerimiento, hardware, red, ataque, vulnerabilidad, portal, aplicación, protocolo, web, Seguridad, integridad, datos, ciudadanos, pensionados, afiliados, transporte, información, puertos, windows.

CONTENIDO:

PROPUESTA PARA IMPLEMENTAR UNA ENTIDAD CERTIFICADORA LOCAL PARA COLPENSIONES

- **DESCRIPCIÓN DEL PROBLEMA:**

En el momento de realizar los controles de auditoría para las aplicaciones web internas de la empresa, se encontró que, estas están publicadas en texto claro y pueden ser interceptadas de diferentes formas, esto se tradujo en un hallazgo de seguridad.

Estas aplicaciones, están exponiendo a un riesgo importante en la integridad de la información de los ciudadanos y afiliados en general a la ciudadanía, pues al ser atacado un sitio web de estos el atacante podrá obtener información privada de los ciudadanos para ser utilizada con fines delictivos con los graves perjuicios que esto puede causar.

Para poder resolver un problema de este tipo, es necesario cifrar las aplicaciones expuestas y publicarlas a través de protocolos seguros, estas acciones implican la utilización de certificados digitales que encripten los datos para protegerlos de los ataques que puedan sufrir en un momento determinado. Estos certificados usualmente deben ser adquiridos a entidades certificadoras externas que avalan la originalidad y seguridad de una aplicación web.

En la actualidad no se tiene contemplada la compra de certificados digitales con entidades externas para proteger las aplicaciones web de Colpensiones y las páginas web se están publicando bajo protocolo http en texto claro, y debido a esto el transporte de información por las redes de datos se realiza de manera clara y sin mecanismos de encripción, dejando abierto el riesgo de fuga de información sensible de los ciudadanos afiliados o no afiliados al sistema en un eventual ataque informático.

Para poder publicar por el protocolo seguro https se necesitan certificados de seguridad, y por la cantidad de aplicaciones existentes es costoso tener que comprar dichos certificados a una entidad certificadora externa, teniendo en cuenta que las aplicaciones son internas o de ambientes no productivos, para asegurarlas no es necesario adquirir certificados de una entidad certificadora

siempre y cuando Colpensiones esté en capacidad de generar sus propios certificados locales desde una entidad certificadora propia.

Al implementar una entidad certificadora local, la empresa podrá cifrar todas las aplicaciones web internas.

OBJETIVO GENERAL.

Implementar una entidad certificadora local que permita la generación de certificados ssl para publicación de sitios seguros que administren las aplicaciones web de Colpensiones sobre protocolo https.

OBJETIVOS ESPECÍFICOS.

1. Configurar un servidor en plataforma de sistema operativo Windows con el rol de entidad certificadora y todas las configuraciones relacionadas a este.

2. Realizar pruebas previas sobre el estado actual de la publicación de las aplicaciones web.

3. Definir el tipo de certificados que mejor se adaptan a la compañía y sus aplicaciones web.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

- **Fase 1.**

Configurar un servidor en plataforma de sistema operativo Windows con el rol de entidad certificadora y todas las configuraciones relacionadas a este. Posterior a la verificación de la máquina y su inclusión en el dominio se establecen los permisos de red necesarios en firewall para que la nueva máquina tenga acceso a todos los ambientes de trabajo de la empresa y que la entidad certificadora pueda generar certificados confiables en ambientes productivos y de pruebas.

- **Fase 2.**

En la fase 2, después de tener el servidor creado y adicionado al domino junto con los permisos de red necesarios para que la máquina alcance toda la red de Colpensiones, de se procede a configurar el rol de entidad certificadora. Se selecciona entonces el rol de entidad dentro de los roles que ofrece el sistema operativo y se configura la ca, debido a que el sistema operativo es Windows, la configuración puede realizarse completamente desde el entorno gráfico

- **Fase 3**

En esta etapa, se realiza la emisión de un certificado raíz de confianza el cual es expedido por la entidad certificadora que se ha creado, este certificado de confianza, se instala en los dominios productivos y de pruebas de Colpensiones y algunos proveedores para que la entidad sea reconocida como una certificadora local de confianza en todo el ámbito tecnológico de Colpensiones.

- **Fase 4**

Definición del tipo de certificados digitales que mejor se adaptan a la compañía y sus aplicaciones web. Después de la realización de las pruebas de certificación se revisa el tipo de certificación apropiado para los sitios web de Colpensiones. Debido a que los certificados se instalarán en

aplicaciones web, la plantilla del certificado debe ser la plantilla web, es necesario tener especial cuidado en el requerimiento o request como se conoce más comúnmente al requerimiento de certificado con el que la entidad certificadora genera los certificados. Después de terminada la fase 4, se procede con la implementación de la publicación de los sitios de aplicaciones web https en el ambiente productivo de Colpensiones.

METODOLOGÍA DE DESARROLLO

Dentro del diseño metodológico, este trabajo describirá la forma o metodología empleada para el diseño y ejecución del proyecto de entidad certificadora, se describirá el tipo de investigación, las fases del proyecto y las fuentes de investigación utilizadas.

En el diseño metodológico, se describirá la forma que se realizará el proyecto, dividiéndolo por fases para para una compresión más fácil sobre los procedimientos necesarios para que el proyecto funcione.

Cada una de las fases en las que se divide el proyecto tiene por finalidad la satisfacción y cumplimiento de los objetivos específicos formulados para la creación de la entidad certificadora.

Dentro del diseño metodológico, y por la naturaleza del proyecto aplicado que propone el trabajo, el tipo de investigación se enmarca en la investigación aplicada, pues en este caso se trata de encontrar una solución a un problema específico dentro del ámbito de seguridad de la información dentro de la red de datos de una empresa.

Las fuentes de investigación primarias utilizadas para el desarrollo de la investigación, son todos aquellos manuales técnicos emitidos por los fabricantes de las entidades certificadora, para este caso en particular se han utilizado los manuales de referencia publicados por los fabricantes Microsoft e Ibm, dentro de estos libros se encuentra publicada la información referente a las características de las entidades certificadoras de cada fabricante, su instalación, requisitos de harware y software y las mejores prácticas para la puesta en marcha de la entidad y su administración.

Conclusiones

1. Se creó una entidad certificadora local, cuya plataforma base eses un servidor virtual Windows 2012 con el objetivo de proporcionar certificados digitales reconocidos por la empresa Colpensiones y sus sistemas tecnológicos, para poder publicar las aplicaciones web en ambiente https.

2. Después de la instalación de la entidad certificadora, se estableció un formato base para el requerimiento de certificados que debe hacer una aplicación de manera estándar ante la cd de Colpensiones, optimizando la longitud, orden y campos a contener en un certificado y dejando los parámetros de manera uniforme para todas las aplicaciones

3. La entidad certificadora generó certificados de raíz de confianza que se instalaron en los dominios de otros proveedores, lo cual permitió extender el funcionamiento de la ca y evitar la compra de certificados externos para autenticarse frente a estos proveedores.

4. La generación de certificados, además de permitir la publicación de aplicaciones de forma segura, también permitió implementa el acceso ldap de usuarios a los servidores del portal

institucional de manera encriptada a través de certificados digitales mejorando la seguridad de acceso de estos sitios web

Recomendaciones.

Las principales recomendaciones realizadas son:

- ✓ Después de tener la entidad certificadora funcionando y las aplicaciones anteriormente descritas trabajando de forma cifrada, se recomienda publicar la totalidad de las aplicaciones web locales en https con certificados digitales emitidos por la entidad certificadora implementada.

- ✓ Es necesario crear un manual de generación de certificados para que los líderes técnicos encargados de cada una de las aplicaciones web tengan los conocimientos necesarios y pueda crear un requerimiento de certificado digital apropiado para el funcionamiento correcto del sitio una vez se haya cifrado.

- ✓ Es necesario generar un certificado digital raíz de confianza de la entidad certificadora creada y entregar este a los proveedores, con el objetivo de que este certificado sea instalado en los dominios de cada empresa y extender el cubrimiento de los certificados que permiten la protección de los sitios a los dominios de proveedores.