



Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

**DESARROLLO DE UNA APLICACIÓN PARA LA ENCRIPCIÓN Y
DESENCRIPTACIÓN DE LA INFORMACIÓN DE UN DIRECTORIO
MEDIANTE AUTENTICACIÓN POR PKI UTILIZANDO TECNOLOGÍA
ACTIVE DIRECTORY.**

**Monografía previa a la obtención del título de
Ingeniero de Sistemas**

**Autores: Pablo Jiménez Quezada
Iván Orellana Mendoza**

Director: Ing. Esteban Crespo

Cuenca, Ecuador

2012

DEDICATORIA

Quiero dedicar este trabajo investigativo a dos personas que forjaron mi formación profesional, a las que debo mucho, mi hermano Luis Adolfo Jiménez Quezada y mi hija Camila Alejandra Jiménez Valle, dándoles el ejemplo de superación y agradeciéndoles de corazón por todo el apoyo recibido; les dedico este trabajo anunciando que todo se puede lograr con esfuerzo y dedicación.

-Pablo Jiménez

Dedico este trabajo a mis padres, que me dieron la oportunidad de superarme y llegar a cumplir esta meta de las muchas que me propongo lograr; y a mi hermana, por el cariño y el apoyo que me ha dado.

-Iván Orellana

AGRADECIMIENTO

A Dios por darme sabiduría, entendimiento y comprensión de saber elegir lo bueno y lo malo; a mis padres por todo el apoyo recibido durante toda mi carrera universitaria; y a mi director de monografía Ing. Esteban Crespo que supo ayudar en las buenas y en las malas sobre cualquier adversidad dentro del tema; a mi jefe Juan Carlos que ha sabido ser un apoyo incondicional en mi carrera formativa y a mi hija por darme las fuerzas, aunque inocentemente, me guió para ser la persona que soy ahora, gracias a todos, los llevo y los llevaré siempre en mi corazón.

-Pablo Jiménez

Agradezco a esta honorable institución, por enseñarme los conocimientos necesarios para desenvolverme en el ámbito profesional de mi carrera, a mis padres por los valores que me han inculcado y un agradecimiento especial para mí director Ing. Esteban Crespo por su gran ayuda en el desarrollo de este trabajo.

-Iván Orellana

ÍNDICE DE CONTENIDOS

DEDICATORIA	ii
AGRADECIMIENTO	iii
ÍNDICE DE CONTENIDOS	iv
RESUMEN.....	vii
ABSTRACT.....	viii
CAPÍTULO 1. INTRODUCCIÓN.....	1
CAPÍTULO 2: MARCO TEÓRICO	2
2.1 Encriptación	2
2.1.1 Encriptación simétrica.....	2
2.1.1.1 DES (Digital Encryption Standard)	3
2.1.1.2 3DES (Three DES o Triple DES)	3
2.1.1.3 IDEA (International Data Encryption Algorithm)	3
2.1.1.4 AES (Advanced Encryption Standard)	3
2.1.2 Encriptación asimétrica.....	4
2.1.2.1 RSA (Rivest, Shamir, Adleman).....	4
2.1.2.2 Diffie-Hellman (& Merkle).....	5
2.1.2.3 ECC (Elliptical Curve Cryptography).....	5
2.1.3 Ventajas y desventajas.	5
2.2 PKI (Public Key Infrastructure)	6
2.2.1 Funcionalidad.....	6
2.2.2 Elementos de PKI.....	7
2.2.2.1 Política de seguridad	8
2.2.2.2 Declaración de Práctica de Certificados (CPS).....	8
2.2.2.3 Autoridad de certificación (CA).....	8
2.2.2.4 Autoridad de registro (RA)	8
2.2.2.5 Sistema de Distribución de Certificados	9
2.2.2.6 Repositorios	9
2.2.2.7 La autoridad de sellado de tiempo (TSA)	9
2.2.2.8 Los usuarios y entidades finales.....	9
2.2.3 Ventajas y Desventajas	10
2.3 Certificados digitales.....	11
2.3.1 Funcionalidad de los certificados digitales	11
2.3.2 Tipos de certificados	11

2.3.3 Estructura de un certificado	12
2.4 Active Directory.....	13
2.4.1 Active Directory Domain Services	13
2.4.1.1 Active Directory Certificate Server	13
2.4.1.2 Directivas de Grupo (GPO).....	14
2.4.1.3 Bosque.....	14
2.4.1.4 Estructura Física.....	14
2.4.1.5 Estructuras Lógicas	14
2.4.1.6 Dominio	14
2.4.1.7 Unidades Organizativas	15
2.4.1.8 Árboles	15
2.4.1.9 FQDN (Fully Qualified Domain Name)	15
2.4.2 Funcionalidad.....	15
2.4.2.1 Intercambio de Dominios.....	16
2.4.2.2 Direccionamiento de Recursos.....	16
2.4.3 Compatibilidad.....	17
2.4.4 Reglas	18
2.5 BitLocker.....	19
2.5.1 Difusor	20
2.5.2 Módulo TPM.....	20
CAPÍTULO 3. ANÁLISIS PRODUCTOS EN EL MERCADO: SOLUCIONES ALTERNATIVAS.	22
3.1 Identificación de software de terceros.....	22
3.2 Funcionamientos de software de terceros	22
3.2.1 CryptoForge	22
3.2.2 TrueCrypt.....	23
3.2.3 CryptoStudio	25
3.2.4 BestCrypt	25
3.2.5 AES Crypt	26
3.3 Costos.....	26
CAPÍTULO 4. SOLUCIÓN	27
4.1 Herramientas de desarrollo.	27
4.2 Funcionalidad de la herramienta desarrollada.....	27
4.2.1 Instalación de Active Directory	27
4.2.1.1 Configuración del equipo servidor.....	27
4.2.1.2 Configuración de DNS.....	34
4.2.1.3 Configuración del equipo cliente	37

4.2.1.4 Directivas de grupo	38
4.2.2 Creación de certificados digitales.	42
4.2.2.1 Instalación de Respondedor Online	46
4.2.2.2 Configuración de la CA para emitir certificados	47
4.2.2.4 Configuración de Revocación	53
4.2.2.5 Verificación de la configuración	55
4.2.4 Funcionamiento aplicación Visual Basic .NET	58
4.3 Ventajas.....	59
CAPÍTULO 5. ANÁLISIS ECONÓMICO PARA LA IMPLEMENTACIÓN.....	60
CONCLUSIONES Y RECOMENDACIONES.....	61
Conclusiones	61
Recomendaciones.....	62
ANEXOS.	63
Anexo 1. Manual de Usuario	63
Anexo 2. Código fuente	67
BIBLIOGRAFÍA	69

RESUMEN

La delincuencia informática y los robos físicos de los equipos, hacen necesario desarrollar e investigar técnicas para poder mitigar estos problemas muy serios, donde la información se pone en riesgo. Por ello hemos planteado utilizar la tecnología Microsoft, apoyándonos en Windows Server 2008 R2 y estaciones de trabajo Windows 7.

También se ha propuesto la instalación de un servicio de Directorio Activo y una entidad de certificación, la misma que nos permitirá administrar de una manera centralizada y de forma adecuada a los usuarios y los certificados digitales, con el fin de poder mantener una autenticación segura y la validación de equipos registrados en la organización.

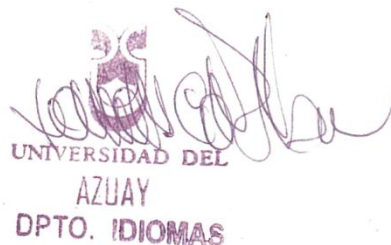
Cada usuario corporativo contará con una aplicación desarrollada en Visual Studio.NET 2010, el mismo que permitirá encriptar o descifrar la unidad o carpeta en la que se encuentra la información, haciendo que esta sea difícil de acceder a un intruso cuando el equipo se encuentre fuera de la organización, aplicando la tecnología BitLocker.

ABSTRACT

Computer-related crimes and physical robbery of the equipments make it necessary to investigate and develop techniques that mitigate these serious problems that put information at risk. Therefore, we have planned to use Microsoft technology with the support of Windows Server 2008 R2 and Windows 7 workstations.

The installation of an Active Directory has also been proposed as well as a certification entity that will allow managing the users and the digital certificates adequately in order to maintain safe authentication and validation of the registered equipment in the organization.

Each corporate user will have an application developed in Visual Studio.NET 2010, which will allow encrypting or deciphering the unit or file that contains the information, making it difficult for an intruder to access when the equipment is away from the organization by applying the BitLocker technology.



Diana Lee Rodas
Translated by,
Diana Lee Rodas

CAPÍTULO 1. INTRODUCCIÓN

Asegurar la información siempre ha sido un tema de gran preocupación para el hombre, en la antigüedad, grandes cantidades de información eran almacenadas en bodegas bajo llave, y aun así, que alguien pueda sustraer esa información podía resultar una tarea muy complicada; con los avances de la informática esto ha ido cambiando cada vez más al momento de almacenar los datos, con la tecnología del microchip se puede almacenar grandes cantidades de información en dispositivos cada vez más pequeños, esto ha brindado mucha facilidad a la hora de transportarlos, pero también ha resultado más difícil mantenerlos seguros. La interconexión de redes de trabajo, si bien han brindado facilidad de acceso a los mismos, representa también un riesgo.

Muchas empresas de desarrollo de software han creado herramientas para controlar los accesos a datos, herramientas como Active Directory del sistema operativo Microsoft Windows Server 2008 R2 Enterprise, esta herramienta brinda una amplia gama de opciones para gestionar el acceso al sistema. Windows también posee algunas herramientas para la encriptación de datos, como es BitLocker que se encuentra en las versiones Enterprise y Ultimate de Windows 7.

El documento está compuesto por cinco capítulos teóricos y prácticos. En el segundo capítulo se detalla las herramientas necesarias que se utilizarán para la solución propuesta. En el tercer capítulo se darán a conocer de soluciones similares o alternativas, con respecto a nuestra solución, veremos algunas soluciones de software libre y otras de pago. En el cuarto capítulo se mostrarán los pasos a seguir para las respectivas configuraciones de las herramientas tanto en el servidor como es Active Directory y Certificados Digitales, como en los equipos clientes la herramienta BitLocker; seguidamente se realizará un programa mediante Visual Studio 2010 Professional que permitirá encriptar y desencriptar la información de una unidad fija (partición de disco). En el quinto y último capítulo se mostrarán conclusiones y recomendaciones que hemos propuesto.

CAPÍTULO 2: MARCO TEÓRICO

Anteriormente habíamos hablado de seguridad de los datos, para esto es necesario abordar conceptos como la encriptación, y que algoritmo se utiliza para lograr esta tarea.

2.1 Encriptación

Existen muchos algoritmos de encriptación, pero vale la pena diferenciar que hay algoritmos que en realidad encriptan, y hay otros que los que hacen es únicamente transformar la información.

La encriptación es el proceso para volver ilegible información considerada importante; en el cual los datos a proteger son traducidos a algo que parece aleatorio y que no tiene ningún significado. Este proceso protege la información para que no pueda ser leída sin una clave. Ahora, los algoritmos que encriptan manejan lo que se denomina llave. La llave es una serie de caracteres de determinado largo, que se utiliza para encriptar y desencriptar la información que se quiere proteger. *Fuente: (Tepper, MSDN).*

2.1.1 Encriptación simétrica

Está basado en la utilización de una sola llave secreta para cifrar y descifrar el mensaje o documento, es decir que la clave es compartida por dos usuarios para poder ver el mensaje cifrado utilizando el mismo algoritmo. El inconveniente de este método es que requiere intercambiar las llaves entre usuarios, por lo que se debe hacer mediante un canal seguro.

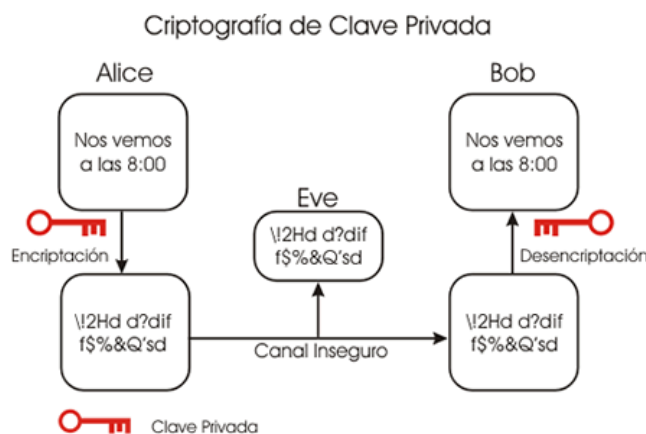


Figura 1. Encriptación simétrica. Fuente: (TextosCientíficos)

Entre los algoritmos que manejan esta encriptación podemos encontrar:

2.1.1.1 DES (Digital Encryption Standard)

Creado en 1975 con ayuda de la NSA (National Security Agency); en 1982 se convirtió en un estándar. Utiliza una llave de 56 bit. En 1999 logró ser quebrado (violado) en menos de 24 horas por un servidor dedicado a eso. Esto lo calificó como un algoritmo inseguro y con falencias reconocidas.

2.1.1.2 3DES (Three DES o Triple DES)

Antes de ser quebrado el DES, ya se trabajaba en un nuevo algoritmo basado en el anterior. Este funciona aplicando tres veces el proceso con tres llaves diferentes de 56 bits. La importancia de esto es que si alguien puede descifrar una llave, es casi imposible poder descifrar las tres y utilizarlas en el orden adecuado. Hoy en día es uno de los algoritmos simétricos más seguros.

2.1.1.3 IDEA (International Data Encryption Algorithm)

Más conocido como un componente de PGP (encriptación de mails), trabaja con llaves de 128 bits. Realiza procesos de shift y copiado y pegado de los 128 bits, dejando un total de 52 sub llaves de 16 bits cada una. Es un algoritmo más rápido que el DES, pero al ser nuevo, aún no es aceptado como un estándar, aunque no se le han encontrado debilidades aún.

2.1.1.4 AES (Advanced Encryption Standard)

Este fue el ganador del primer concurso de algoritmos de encriptación realizado por la NIST (National Institute of Standards and Technology) en 1997. Después de 3 años de estudio y habiendo descartado a 14 candidatos, este algoritmo, también conocido como Rijndael por Vincent Rijmen y Joan Daemen, fue elegido como ganador. Aún no es un estándar, pero es de amplia aceptación a nivel mundial.

El algoritmo más seguro hoy es el AES, aunque 3DES también es muy seguro. Este último se utiliza cuando hay necesidad de compatibilidad. AES 128 es aproximadamente 15% más rápido que DES, y AES 256 sigue siendo más rápido que DES.

2.1.2 Encriptación asimétrica

Este método utiliza dos claves para cada usuario, una para cifrar y otra para descifrar. La clave para cifrar el mensaje se la denomina pública en cambio la clave para descifrar el mensaje se la denomina privada, ya que cualquier usuario puede conocer la clave para cifrar el mensaje, esta llave se la puede hacer pública, de ahí su nombre, y solo el usuario que tenga la clave privada podrá descifrar el mensaje.

Ya que este algoritmo funciona de modo que lo que cifra una clave lo descifra la otra, cuando se requiera verificar la autenticación de un documento, los usuarios a los cuales les ha sido enviado lo pueden descifrar con la clave pública, entonces se comprueba la identidad de la persona que lo envió ya que esta utilizó su clave privada.

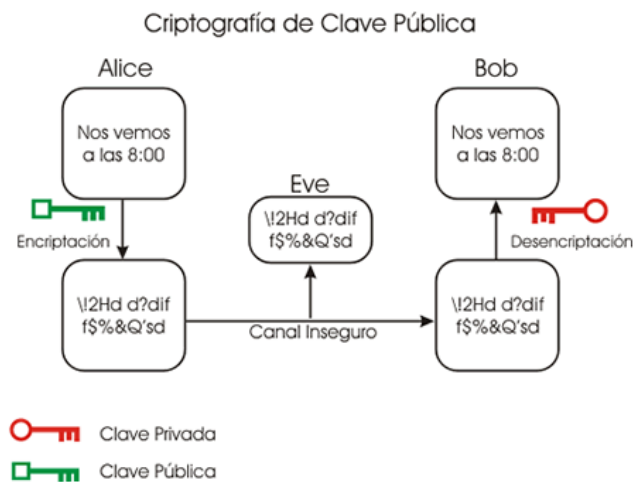


Figura 2. Encriptación asimétrica. Fuente: (TextosCientíficos)

Los algoritmos más conocidos que manejan esta encriptación son:

2.1.2.1 RSA (Rivest, Shamir, Adleman)

Creado en 1978, hoy es el algoritmo de mayor uso en encriptación asimétrica. Tiene dificultades para encriptar grandes volúmenes de información, por lo que es usado por lo general en conjunto con algoritmos simétricos.

2.1.2.2 Diffie-Hellman (& Merkle)

No es precisamente un algoritmo de encriptación sino un algoritmo para generar llaves públicas y privadas en ambientes inseguros.

2.1.2.3 ECC (Elliptical Curve Cryptography)

Es un algoritmo que se utiliza poco, pero tiene importancia cuando es necesario encriptar grandes volúmenes de información. *Fuente: (Tepper, MSDN)*

2.1.3 Ventajas y desventajas.

Algoritmos simétricos	Algoritmos asimétricos
Ventajas	Ventajas
<ul style="list-style-type: none">• Velocidad de encriptación.• La velocidad de encriptación de los algoritmos simétricos tiene una relación 1000 veces más rápido que los asimétricos.	<ul style="list-style-type: none">• Encriptar con una llave pública y desencriptar con una llave privada mejora notablemente la seguridad.• Los algoritmos asimétricos son resistentes a ataques de fuerza bruta.• Los algoritmos asimétricos se usan para la autenticación con firma digital.
Desventajas	Desventajas
<ul style="list-style-type: none">• Requerir medios seguros para enviar la clave al destino para la desencriptación de mensajes.• Los algoritmos simétricos necesitan una gran cantidad de bits para alcanzar un nivel de seguridad similar al de los asimétricos, 3000 bits contra 128 bits.	<ul style="list-style-type: none">• No es recomendable usar un algoritmo asimétrico para encriptar grandes cantidades de información ya que es muy lento.

Fuente: (cryptoforge.com)

Debido a las limitantes que poseen, muchas veces es necesaria una encriptación combinada, encriptar una gran cantidad de información mediante un algoritmo simétrico por su velocidad frente a uno asimétrico, y encriptar la llave mediante un algoritmo asimétrico por su seguridad.

2.2 PKI (Public Key Infrastructure)

Una PKI es una infraestructura de clave pública, se utiliza cuando se requiere la criptografía de la clave pública para realizar comunicaciones electrónicas seguras en un entorno de trabajo.

Para el funcionamiento de esta se requiere el uso de certificados, los cuales necesitan las denominadas autoridades certificadoras, estas pueden ser reconocidas mundialmente como VeriSign o se las puede manejar nivel local, es decir emitir certificados autofirmados por la misma empresa que requiere el servicio por ejemplo, siempre y cuando sea para el manejo interno de información; en el proyecto se propone el manejo de certificados de manera local, es decir, los autofirmados, ya que el objetivo es controlar la información crítica dentro de la propia empresa; así el usuario podrá desencriptar los datos únicamente si está conectado a la red y solo si tiene los permisos necesarios para ello, estos permisos estarán estructurados de acuerdo a la configuración de Active Directory.

2.2.1 Funcionalidad.

Infraestructura de llave pública (PKI) por sus siglas en inglés, es un conjunto de hardware, software, políticas y procedimientos que permiten utilizar la criptografía de llave pública para crear certificados de identificación, con los cuales se puede garantizar que las transacciones sean realizadas de forma segura, evitando accesos de terceros que pudieran perjudicar las operaciones de una organización.

Como se dijo anteriormente, hablar de PKI, es hablar de certificados digitales, esta tecnología permite que los usuarios puedan autenticarse, para cifrar o descifrar información, ya que esto permite identificar a los usuarios, la persona que firmó no puede ser suplantada, así la persona puede hacerse responsable de documentos, información en general o garantizar el acceso a servicios de red.

Con PKI podemos manejar varias funcionalidades:

- Gestión. Podemos crear, revisar o revocar claves, y gestionar el nivel de confianza de las mismas.
- Publicación. Mediante PKI podemos distribuir la clave pública, y también localizar las claves públicas de otros usuarios y consultar su estado.
- Utilización. Luego de conseguida la clave, PKI nos facilita el uso de la misma.

Para realizar las operaciones de encriptación, se utilizan algoritmos de cifrado que son conocidos y están accesibles para todos, la seguridad que da la tecnología PKI depende mucho de la privacidad de la clave privada y de las políticas de seguridad establecidas.

Esta tecnología es utilizada en varios ámbitos del comercio electrónico, o de intercambio de información confidencial como: Identificación de los usuarios que intervienen en la comunicación, el cifrado de información digital, autenticación de software o documentos mediante firmas digitales, garantizar la seguridad en las comunicaciones, el no repudio en las transacciones realizadas.

Ya que estas claves permiten identificar a una persona o entidad en particular, éstas se utilizan para crear certificados, con ellos se puede identificar al usuario empleado de la empresa cuando se conecte al servidor; se pueden crear varios tipos de certificados, más adelante se analizará el tipo de certificado adecuado para este trabajo.

2.2.2 Elementos de PKI

Para montar una PKI son necesarias algunas entidades:

- Política de Seguridad
- Declaración de Práctica de Certificados
- Autoridad de Certificación (CA)
- Autoridad de Registro (RA)
- Sistema de Distribución de Certificados

- Repositorios
- Autoridades de sellado (TSA)
- Usuarios y entidades finales

2.2.2.1 Política de seguridad

Un aspecto muy importante en el uso de esta tecnología, son las políticas de seguridad, pueden ser los dispositivos más seguros, que utilicen los algoritmos de cifrado más complejos, pero resultan inútiles si las claves de encriptación no son guardadas de forma adecuada. Por eso es necesario implantar políticas de seguridad que impidan que otros certificados sean creados, ya que esto podría permitir accesos no autorizados a los equipos.

2.2.2.2 Declaración de Práctica de Certificados (CPS)

Es un documento en cual se encuentran los procedimientos para la ejecución de las políticas de seguridad; indica cómo funciona la CA, como se emiten, aceptan y revocan certificados, y como se generan, registran y certifican las claves, donde se almacenan y están disponibles para los usuarios.

2.2.2.3 Autoridad de certificación (CA)

Se encarga de emitir y revocar los certificados, este sistema es el que se encarga de gestionar los certificados. Los certificados que gestiona deben ser firmados por una CA jerárquicamente superior, entonces se crea una cadena de certificados que se validan unos a otros. Vincula las claves de los usuarios con el certificado, especifica las fechas de expiración y publica listados de revocación de los certificados.

2.2.2.4 Autoridad de registro (RA)

Mediante esta autoridad se evita el congestionamiento en la CA, con el objetivo de agilizar las solicitudes de certificados. Comprueba la veracidad y corrección de los datos de las peticiones de los usuarios y luego las envía a una CA para su procesamiento.

2.2.2.5 Sistema de Distribución de Certificados

Se detalla la forma en cómo deberán ser distribuidos los certificados, esto depende tanto de estructura de la PKI, como del servicio de directorios que se maneje.

2.2.2.6 Repositorios

Es donde se almacena la información relacionada con las certificaciones. Consta del repositorio de certificados y del repositorio de revocación de certificados, en esta última aparecen todos los certificados que han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

2.2.2.7 La autoridad de sellado de tiempo (TSA)

Esta se encarga de firmar documentos con el objetivo de demostrar que existían antes de una fecha o momento determinado.

2.2.2.8 Los usuarios y entidades finales

Estos son los que poseen el par de claves (pública y privada) y un certificado asociado a su clave pública. Y son las que utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI para firmar digitalmente, cifrar o descifrar documentos, etc.

2.2.3 Ventajas y Desventajas

Ventajas	Desventajas
<ul style="list-style-type: none">• Con PKI se evitan varios problemas que pueden surgir al usar usuario/contraseña como roturas de contraseñas mediante fuerza bruta, errores humanos, entre otras.• Resulta más seguro a utilizar solamente un sistema de usuario/contraseña.• PKI no solo brinda un servicio de identificación de usuarios, sino posee varias herramientas de gestión.• Ofrece mejores medios para identificar al usuario ya que los certificados contienen información verificable relacionada con la identidad del usuario, lo cual no ocurre en la autenticación basada en dirección IP del equipo del usuario, o del nombre de dominio o una dirección de mail, dado que las direcciones IP pueden ser dinámicas, y los nombres de dominio y direcciones de mail pueden ser espiadas.• Los certificados basados en tecnología de clave pública poseen un mecanismo de autenticación más fuerte. Sólo el usuario conoce la forma de acceder a su clave privada.• Simplificación en la administración y disminución de costos	<ul style="list-style-type: none">• Ya que se depende de una CA, esta maneja un gran conjunto de procedimientos de seguridad, algunos de los cuales son manejados por personas, por lo tanto algunos pasos no son del todo criptográficos.• El problema de la seguridad de la clave, puede ocurrir que en un descuido del usuario, la clave caiga en manos equivocadas.• No se puede garantizar que la clave privada solo sea utilizada por su dueño, esto depende de la política de seguridad que se maneje en la empresa en cuestión.• Puede existir problemas de interoperabilidad, a pesar de utilizar el estándar X.509.v3, no se puede garantizar que dos certificados generados por dos CA diferentes sean compatibles, de igual manera, no se espera mayores inconvenientes, ya que esto se manejara solo en la empresa, y no por CA ajenas a ella.• El uso de PKI implica un esfuerzo considerable en el desarrollo, implementación y mantenimiento, y sin hablar del tiempo que requiere para su puesta en marcha.

Fuente: Desarrollo del autor

2.3 Certificados digitales

Se entiende por certificado digital reconocido de identificación a la clave pública del usuario firmada por una autoridad certificadora (VeriSign, Ceres –con la Fábrica Nacional de moneda y timbre-, Izenpe del país Vasco, etc.), que identifica a un sujeto reconocido, con nombres y apellidos. Se incluye el periodo de validez, los límites del uso del certificado, si están previstos, y los límites del valor de las transacciones para las que pueden utilizarse, si se establecen. *Fuente: (Areitio Bertolín)*

2.3.1 Funcionalidad de los certificados digitales

Como se había mencionado en el capítulo 2, existen dos tipos de algoritmos, el simétrico y el asimétrico, así también se manejan certificados de clave privada y otros de clave pública que manejan dichos algoritmos respectivamente.

Entonces se pueden manejar dos tipos de certificados:

Mediante llave privada (simétrica), esta podría ser compartida por el equipo cliente y por el servidor con PKI y Active Directory, y será la que se utilice para encriptar y desencriptar información, puede resultar muy útil ya que son utilizadas para grandes volúmenes de información.

Por otro lado tenemos la llave pública (asimétrica), utilizando 2 llaves, una pública y una privada, en este caso el equipo cliente que desee ponerse en contacto con el servidor para desencriptar el directorio, lo tendrá que hacer con un mensaje encriptado con la llave pública del servidor, y así únicamente este, mediante su llave privada podrá identificar y autorizar al usuario en cuestión para poder desencriptar la información y tener acceso a los datos.

2.3.2 Tipos de certificados

Dependiendo del tipo de información que contiene, y del dueño o creador del certificado, se pueden crear varios tipos, que pueden ser: **certificado personal**, que especifica la identidad del emisor, **certificado de empresa**, que identifica al emisor y a la institución a la cual está vinculado, **certificado de persona jurídica**, que identifica una empresa o sociedad cuando se trate de trámites ante las administraciones o instituciones, o **certificado de atributo**, el cual permite

identificar una cualidad, estado o situación, que podría ser de tipo personal, ya que puede ir asociado a este, entre otros.

Podemos clasificarlos en varias categorías dependiendo del uso que se les dé, en este caso se tomará en cuenta el que se menciona al inicio, de tipo **personal**, ya que cada certificado emitirá la CA del servidor identificará de manera individual al directivo para que una vez establecida la conexión y comprobada su identidad, éste pueda descifrar y acceder a la unidad de datos encriptada de su equipo.

2.3.3 Estructura de un certificado

La estructura de un certificado digital viene dado por estándares, para la utilización de PKI se utiliza el denominado X.509 versión 3.

El **X.509 v3**, es un estándar UIT-T para infraestructuras de claves públicas (PKI). X.509 v3 establece formatos para los certificados de claves públicas y un algoritmo de validación de la ruta de certificación para ello utiliza una sintaxis en lenguaje ASN.1 (Abstract Syntax Notation One).

En Active Directory, el rol que maneja la entidad de certificación utiliza el estándar X.509v3, por lo que ésta se utilizará para crear los certificados, la estructura de este estándar consta de:

- Versión
- Número de serie
- ID del algoritmo
- Emisor
- Validez
 - No antes de
 - No después de
- Sujeto
- Información de clave pública del sujeto
- Algoritmo de clave pública
- Clave pública del sujeto
- Identificador único de emisor (opcional)
- Identificador único de sujeto (opcional)

- Extensiones (opcional)
- Algoritmo usado para firmar el certificado
- Firma digital del certificado.

2.4 Active Directory

2.4.1 Active Directory Domain Services

Active Directory es una herramienta de Microsoft para administradores, ayuda a gestionar un gran número de tareas entre las cuales tenemos el control de usuarios, credenciales, protección de información, controlar configuraciones de los sistemas y las aplicaciones de los clientes; aquí se indican algunas características:

- Reducción de los costes de la gestión de redes Windows.
- Simplificar la gestión de identidad, proporcionando una vista única de toda la información del usuario.
- Aumenta la seguridad con la capacidad de permitir que varios tipos de mecanismos de seguridad estén dentro de una sola red.
- Mejora el cumplimiento mediante el uso de Active Directory como una fuente primaria de datos de auditoría.
- Los cambios realizados a objetos de Active Directory se pueden grabar para saber lo que se ha cambiado, así como los valores anteriores y actuales de los atributos modificados.

2.4.1.1 Active Directory Certificate Server

Los Servicios de Certificate Server de Active Directory ofrecen servicios para administrar certificados de clave pública que se usan en los sistemas de seguridad de software basados en tecnologías de clave pública. Se puede usar AD CS para aumentar la seguridad al enlazar la identidad de una persona, un dispositivo o un servicio con la clave privada correspondiente. AD CS también incluyen características que permiten administrar la inscripción y la revocación de certificados en diversos entornos.

Reduce el costo de propiedad mediante el aprovechamiento de la integración de Active Directory para la inscripción y los procesos de revocación en Windows Server 2008 R2.

Aumenta la seguridad de acceso con mayor seguridad que las soluciones de usuario y contraseña, y la capacidad de verificar la validez de los certificados utilizando el Online Certificate Status Protocol (OCSP).

2.4.1.2 Directivas de Grupo (GPO)

Es un conjunto de reglas que controlan el ambiente de trabajo de cuentas de usuario y cuentas de equipo, también proporciona la gestión centralizada y configuración de sistemas operativos, aplicaciones y configuración de los usuarios en un entorno de Directorio Activo.

2.4.1.3 Bosque

Es una configuración jerárquica de uno a mas arboles de dominio distintos e independientes entre sí. Los árboles de un bosque comparten un esquema común, tienen diferentes estructuras de nombre de acuerdo con sus dominios, y existe una relación transitiva de confianza bidireccional entre los dominios y los arboles de dominio.

2.4.1.4 Estructura Física

Los componentes físicos de AD son los sitios y los controladores de dominio, para ello se utilizarán estos componentes para desarrollar una estructura de directorio que refleje la estructura física de la organización.

2.4.1.5 Estructuras Lógicas

Los recursos se organizan mediante una estructura lógica que refleja la misma de una organización, ya que nos permite agrupar recursos lógicamente y encontrar a un recurso mediante su nombre en vez de su localización física. Active Directory hace transparente la estructura física a los usuarios cuando se ha hecho la agrupación de recursos lógicamente.

2.4.1.6 Dominio

Es la unidad Central de la estructura lógica de Active Directory en la que se puede almacenar millones de objetos como impresoras, documentos, direcciones de correo electrónico, bases de datos, usuarios, componentes distribuidos y otros recursos. En cada dominio se almacena información exclusiva sobre los objetos que contiene. AD

se puede componer de uno o más dominios y estos pueden expandirse en más de una localización física.

2.4.1.7 Unidades Organizativas

Es un contenedor que se utiliza para organizar objetos dentro de un dominio en grupos organizativos lógicos que reflejan la estructura funcional y de negocios de una organización. Esta OU puede contener objetos como cuentas de usuario, equipos, impresoras, aplicaciones, archivos compartidos y otras OU del dominio.

2.4.1.8 Árboles

Es una agrupación jerárquica de uno o más dominios que se crean añadiendo uno o más dominios secundarios a un dominio principal. Los dominios en un árbol comparten un espacio de nombres contiguo y una estructura jerárquica de nombres. Todos los dominios dentro de un árbol comparten un esquema común, que es una definición formal de todas las clases de objeto que se pueden almacenar en el desarrollo de AD.

2.4.1.9 FQDN (Fully Qualified Domain Name)

Es un nombre que incluye el nombre de una computadora y el nombre del dominio al cual pertenece, por ejemplo, nombre de la computadora pablojuser y el nombre del dominio servidor.com el FQDN es pablojuser.servidor.com. *Fuente: (Rodriguez)*

2.4.2 Funcionalidad.

Active Directory viene implementado de una manera similar a la de una base de datos en la cual se almacena en forma centralizada la información relativa a un dominio de autenticación. Ya que esto representa una sincronización presente entre los distintos servidores de autenticación de todo el dominio.

Para poder identificarlos cada uno de estos objetos tendrá atributos en modo unívoco, por ejemplo, a los usuarios se les pondría campos como son: nombre, email, etc., en cambio para las impresoras de red tendrían sus campos: nombre, fabricante, modelo, usuarios que pueden acceder, etc. Toda la información que se pueda almacenar tanto de los usuarios como de los recursos que estén dentro de la red queda almacenada en Active Directory replicándose de forma automática entre todos los servidores que controlan el acceso al dominio.

Con todas las facilidades que Active Directory nos brinda es posible crear recursos dentro de una red y mediante este conceder acceso a los diferentes usuarios, ya que la lista de objetos es replicada a todo el dominio de la administración, los cambios eventuales serán visibles en todo el ámbito.

2.4.2.1 Intercambio de Dominios

Active Directory tiene una función llamada relación de confianza (trust) que permite que los usuarios que tienen un dominio puedan acceder a recursos que están en otro dominio, ya que el trust se crea automáticamente cuando se crean nuevos dominios. Los límites del trust son marcados por el bosque al cual pertenece y no por dominio. Dentro de Active Directory hay trust transitivos donde pueden ser:

- Acceso Directo.- une dos dominios en arboles diferentes, transitivo, una o dos vías.
- Bosque.- Transitivo, una o dos vías.
- Reino.- Transitivo o no transitivo, una o dos vías.
- Extremo.- No transitivo, una o dos vías.

Estos trust sirven para conectarse a otros bosques o dominios que no son de Active Directory.

2.4.2.2 Direccionamiento de Recursos

Cada objeto que está en la red posee un nombre que lo distingue (DN) mediante el cual se podrá direccionar cada elemento, por ejemplo, una impresora que se llame Imprime y que este dentro de una Unidad Organizativa (OU) llamada Despachos y un dominio empresa.org, se la direccionaría de la siguiente manera:

- En DN (Distinguished name) CN=Imprime, OU=Despachos, DC=empresa, DC=org. Donde CN es el nombre común y DC es la clase de objeto de dominio
- En forma canónica sería: empresa.org/Despachos/Imprime

Existen otros métodos de direccionamiento que constituyen una forma local de localizar un recurso:

- Distinción de Nombre Relativo (RDN) que busca un recurso solo con el CN.
- Identificador Globalmente Único (GUID) que genera una cadena de 128 bits y es usado por Active Directory para buscar y replicar información.

Algunos objetos poseen un Nombre de usuario principal (UPN) que permite el ingreso abreviado a un recurso o un directorio de la red (objetored@dominio).

Los direccionamientos a recursos de AD son estándares con la Convención Universal de Nombrado (UNC), Localizador Uniforme de Recursos (URL) y nombrado de Protocolo Ligero de Accesos a Directorio (LDAP).

2.4.3 Compatibilidad.

Al hablar de compatibilidad en Active Directory vamos a hablar de Windows Server 2008 R2 con Windows 7 ya que estos han introducido la tecnología más reciente del sistema operativo y la plataforma de desarrollo de software para su uso. Muchas nuevas características se han introducido, las características existentes se las han mejorado y algunas se las han quitado esto como parte de seguir mejorando la seguridad, fiabilidad, rendimiento y experiencia con el usuario de Windows.

Windows Server 2008 R2 y Windows 7 son altamente compatibles con la mayoría de sus respectivas aplicaciones creadas para Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 y sus paquetes de servicio, algunas roturas de compatibilidad son inevitables debido a las innovaciones, fortalecimiento de la seguridad, y una mayor fiabilidad. Hablando en sentido general de la compatibilidad de Windows 7 con Windows Server 2008 R2 con las aplicaciones existentes es alto.

Versiones del Sistema Operativo

Plataforma

Clientes: Windows 7

Servidores: Windows Server 2008 R2

La característica del impacto de la gravedad y la frecuencia es Alta.

El número de versión interno tanto de Windows 7 como de Windows Server 2008 R2 es 6,1. Esto es especialmente importante para antivirus, copia de seguridad, las aplicaciones de los servicios públicos y la protección de la copia.

La mayoría de las aplicaciones funcionarán correctamente ya que la compatibilidad entre estos es muy alta, sin embargo incluyen una vista de compatibilidad para los instaladores y las aplicaciones que comprueban la versión del sistema operativo.

2.4.4 Reglas

- No iniciar una sesión en el equipo con credenciales administrativas ya que esto provocaría que el sistema sea vulnerable a troyanos y a otros riesgos para la seguridad.
- Si se ha iniciado una sesión en el equipo sin credenciales administrativas, puede utilizar Ejecutar como para llevar a cabo las tareas administrativas.
- Para ofrecer protección adicional en Active Directory, se recomienda lo siguiente:
 - Cambiar el nombre o deshabilitar la cuenta Administrador y la cuenta de invitado en todos los dominios para evitar intrusiones en los dominios.
 - Proteger físicamente todos los controladores de dominio en una sala cerrada.
 - Administrar la relación de seguridad entre dos bosques y simplificar la administración de seguridad y la autenticación entre bosques para poder tener una administración simplificada de los recursos entre dos bosques al reducir el número de confianzas externas necesarias para compartir recursos y el uso de autenticación de nombre principal de usuario entre ambos bosques.
 - Quitar todos los usuarios del grupo administradores de esquema y agregar un usuario al grupo solo cuando sea necesario realizar cambios en el esquema esto para dar una protección adicional al esquema de Active Directory. Una vez que se lo realiza el cambio quitar al usuario del grupo.
 - Restringir el acceso a usuarios, grupos y equipos a los recursos compartidos y a la configuración de Directiva de grupo de filtros.

- Procurar no deshabilitar el uso del tráfico LDAP cifrado o firmado para las herramientas administrativas de Active Directory.
- Algunos derechos de usuario predeterminado asignados a grupos predeterminados específicos pueden permitir a los miembros de esos grupos obtener derechos adicionales en el dominio, incluido derechos administrativos, por lo tanto, la organización debe confiar de igual modo en todas las personas que sean miembros de los grupos administradores de organización, administradores de dominio, operadores de cuentas, operadores de servidores, operadores de impresión y operadores de copia de seguridad. Estos grupos predeterminados se crean automáticamente al crear un dominio de Active Directory los mismos que permiten controlar el acceso a los recursos compartidos y delegar funciones administrativas específicas en todo el dominio.
- Utilizar grupos globales o universales en vez de grupos locales de dominio al especificar permisos en los objetos del directorio de dominio replicados en el catálogo global.
- Establecer como un sitio todas las áreas geográficas que requieran acceso rápido a la información de directorio más reciente.
- Colocar al menos un controlador de dominio en cada sitio y hacer que uno de los controladores de dominio del sitio, como mínimo, sea un catálogo global para que sean más eficaces los sitios.
- Realizar copias de seguridad periódicas de los controladores de dominio para conservar todas las relaciones de confianza del dominio.

2.5 BitLocker

El cifrado de unidad BitLocker es una característica de seguridad integral del sistema operativo Windows 7 que ayuda a proteger los datos almacenados en unidades de datos fijas y extraíbles y en la unidad del sistema operativo. BitLocker protege de "ataques sin conexión", que son aquéllos que se realizan deshabilitando o evitando el sistema operativo instalado, o bien, quitando físicamente el disco duro para atacar los datos por separado.

En el caso de las unidades de datos fijas y extraíbles, BitLocker ayuda a garantizar que los usuarios pueden leer y escribir datos en la unidad solo cuando cuentan con la contraseña correspondiente, con credenciales de tarjeta inteligente o cuando usan la unidad de datos en un equipo protegido con BitLocker que tenga las claves adecuadas. *Fuente: (Microsoft)*

BitLocker utiliza el Estándar de cifrado avanzado (AES) como algoritmo de cifrado con longitudes de clave configurables de 128 ó 256 bits, así como un difusor opcional. La configuración de cifrado predeterminada es AES 128 + difusor, pero las opciones se pueden configurar mediante la directiva de grupo.

2.5.1 Difusor

El difusor está diseñado para mitigar un tipo de ataque posible que implica el cambio de información cifrada para introducir una vulnerabilidad de seguridad en el sistema. Con el difusor, los pequeños cambios en el texto cifrado de un sector afectan a todo el sector cuando se descifran los datos. Este comportamiento dificulta aún más la realización de ataques dirigidos.

2.5.2 Módulo TPM

La protección de BitLocker en unidades del sistema operativo admite la autenticación de dos factores mediante el uso del Módulo de plataforma segura (TPM) junto con un número de identificación personal (PIN) o clave de inicio, así como la autenticación de un solo factor mediante el almacenamiento de una clave en una unidad flash USB o mediante el uso solo del TPM. El uso de BitLocker con un TPM proporciona una mayor protección a los datos y ayuda a garantizar la integridad del componente de arranque inicial. Esta opción requiere que el equipo disponga de un microchip de TPM y una BIOS compatibles. Un TPM compatible se define como la versión 1.2 del TPM.

La mayoría de los sistemas operativos utilizan un espacio de memoria compartido y basan la administración de la memoria física en el sistema operativo. Un TPM es un componente de hardware que utiliza su propio firmware interno y circuitos lógicos para las instrucciones de procesamiento, es decir, lo blindo frente a vulnerabilidades de software externo. Para atacar el TPM es necesario disponer de acceso físico al

equipo. Además, con frecuencia las herramientas y las habilidades necesarias para atacar hardware son más caras y, normalmente, no están tan disponibles como las que se utilizan para atacar software. Debido a que cada TPM es exclusivo del equipo en el que está instalado, atacar varios equipos con TPM sería difícil y laborioso.

Fuente: (MSDN)

En equipos que no poseen el módulo TPM, y si la versión de este no es compatible, se puede desactivar la comprobación del mismo modificando las directivas de Windows (gpedit.msc).

CAPÍTULO 3. ANÁLISIS PRODUCTOS EN EL MERCADO: SOLUCIONES ALTERNATIVAS.

3.1 Identificación de software de terceros

Existen en el mercado varios tipos de software de encriptación de datos pagados y gratuitos, que utilizan varios algoritmos de encriptación, pero la implementación puede requerir componentes adicionales, al menos para implementarlos con Active Directory. Algunos de los más conocidos o más utilizados son:

- CryptoForge
- TrueCrypt
- CryptoStudio
- BestCrypt
- AES Crypt

Otra opción puede ser la implementación de políticas en la empresa, que por ejemplo impidan la salida de equipos.

3.2 Funcionamientos de software de terceros

3.2.1 CryptoForge

CryptoForge es un programa de encriptación para seguridad personal y profesional. Permite proteger la privacidad de archivos, carpetas, y mensajes confidenciales encriptándolos (cifrándolos) con hasta cuatro algoritmos de encriptación robustos. Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro, o transmitida por una red insegura (como Internet), y aun así permanecer secreta. Luego, la información puede ser desencriptada (descifrada) a su formato original. CryptoForge es un conjunto de programas para encriptar archivos, carpetas, y email, que le añaden al Windows la más robusta encriptación disponible hoy día. Está diseñado para ocultar la complejidad de la tecnología de encriptación, razón por la cual este programa es realmente muy fácil de usar. *Fuente: (cryptoforge.com)*

Características y beneficios

Las características y beneficios de CryptoForge incluyen:

- Rápido para descargar, simple de instalar, y muy fácil de usar!
- Basado en algoritmos de encriptación de dominio público - La robusta encriptación empleada por CryptoForge es la mejor disponible hoy día.
- Ataque por fuerza bruta impracticable - Con mil millones de ordenadores capaces de probar mil millones de contraseñas por segundo cada uno, y empleando un algoritmo con llave de 168 bits, se necesitarían $10 \cdot 10^{24}$ años de trabajo para probar todas las contraseñas posibles (para comparar, la edad del universo se estima en $10 \cdot 10^9$ años).
- Encriptación múltiple - Sus datos estarán seguros, aún sin el futuro uno de los algoritmos de encriptación fuese atacado con éxito.
- Destructor de archivos incorporado - Cumpliendo y excediendo las especificaciones DoD (Departamento de Defensa de EEUU).
- Protección con contraseña muy fácil y segura.
- Potente compresión incorporada - La compresión refuerza aún más la seguridad criptográfica. Todos los programas de encriptación deberían incluir compresión.
- Desarrollado y compilado fuera de los EEUU - No está sujeto a restricciones para exportación ni a regulaciones internas.
- Ideal para la protección de archivos y carpetas - Funciona en cualquier tipo de medio, incluyendo carpetas de red y dispositivos removibles USB.
- Sin puertas traseras ni llaves maestras - Sea cuidadoso y no olvide su contraseña.
- Módulo para encriptar email - Con el módulo Text es muy fácil la encriptación de email.

3.2.2 TrueCrypt

TrueCrypt es un sistema informático para establecer y dar mantenimiento de cifrado sobre un volumen en tiempo real (dispositivo de almacenamiento de datos). Encriptación de volumen en tiempo real significa que los datos se encriptan automáticamente justo antes de ser guardados y se descifran justo después de que se

han cargado, sin intervención del usuario. Ningún dato almacenado en un volumen cifrado se puede leer (descifrar) sin utilizar la contraseña correcta / keyfile (s) o las teclas correctas de cifrado. Todo el sistema de archivos se cifra (por ejemplo, nombres de archivos y carpetas, el contenido de cada archivo, el espacio libre, metadatos, etc.)

Los archivos se pueden copiar desde y hacia un volumen TrueCrypt montado al igual que se copian desde / a cualquier disco normal (por ejemplo, por la simple función de arrastrar y soltar). Los archivos se descifran de forma automática sobre la marcha (en la memoria / RAM), mientras que están siendo leídos o copiados de un volumen cifrado TrueCrypt. Del mismo modo, los archivos que se graban o copian en el volumen de TrueCrypt se cifran de forma automática sobre la marcha (justo después de que se escriben en el disco) en la memoria RAM. Nótese que esto no significa que todo el archivo que va a ser cifrado / descifrado debe ser almacenado en la memoria RAM antes de que pueda ser encriptada / descifrado. *Fuente: (TrueCrypt)*

Características principales:

- Crea un disco virtual encriptado dentro de un archivo y lo monta como un disco real.
- Cifra toda una partición o dispositivo de almacenamiento como una unidad flash USB o disco duro.
- Cifra una partición o unidad donde está instalado Windows (autenticación previa al arranque).
- El cifrado es automático, en tiempo real (on-the-fly) y transparente.
- Paralelización y la canalización de permitir que los datos se lean y se escriben más rápido que si la unidad no ha sido cifrado.
- El cifrado se puede acelerada por hardware de los procesadores modernos.
- Proporciona una negación plausible, en caso de que un adversario le obliga a revelar la contraseña: Volumen oculto (esteganografía) y el sistema operativo oculto.

3.2.3 CryptoStudio

CryptoStudio es un programa que ofrece diversas utilidades de cifrado. El corazón de la aplicación es OpenSSL, una implementación de código abierto de los protocolos SSL y TLS y uno de los software de seguridad más utilizado. OpenSSL es esencialmente una biblioteca criptográfica de propósito general, disponible para una variedad de plataformas. Junto con esa biblioteca, OpenSSL tiene una gran colección de herramientas de línea de comandos que realiza tareas específicas, como la creación y administración de certificados digitales, la implementación de las funciones hash, los algoritmos de clave pública y secreta, firma digital. Muchas de las funcionalidades CryptoStudio son un mero contenedor de interfaz gráfica de usuario de herramientas de OpenSSL, la intención es de hacer esas herramientas disponibles también para los usuarios no iniciados.

Sin embargo, funciones adicionales se han desarrollado utilizando el código directamente desde las bibliotecas de OpenSSL. *Fuente: (CryptoStudio)*

3.2.4 BestCrypt

BestCrypt es un producto de encripta automáticamente los datos antes de guardar o almacenar en un archivo. La información confidencial está codificada mediante un algoritmo, para que lo que los datos sean ilegibles. BestCrypt descifra de forma transparente el archivo una vez que se ha abierto al proporcionar la contraseña o tecla correcta.

BestCrypt crea y soporta discos virtuales encriptados, que son visibles como discos regulares con las letras de unidad correspondiente (por ejemplo, D:, K:, Z:, es decir, con cualquier letra de unidad que no es utilizado por otro dispositivo del sistema).

BestCrypt encripta los datos usando una variedad de algoritmos de cifrado como (AES, Blowfish, Twofish, CAST y otros). Cada algoritmo se implementa con el tamaño de clave más grande posible, definido en la especificación del algoritmo.

Fuente: (Jetio)

3.2.5 AES Crypt

Es un producto de software que cifra archivos, funciona en varios sistemas operativos y utiliza el estándar de la industria estándar de cifrado avanzado (AES) para cifrar los archivos de forma fácil y segura.

No es necesario ser un experto para utilizar AES cripta, ni tampoco es necesario entender la criptografía. Si utiliza Windows, lo único que necesita hacer es hacer clic derecho sobre un archivo, seleccionar cifrar AES o descifrar AES, introduzca una contraseña, y AES Crypt se encargará del resto. En un Mac, puede arrastrar un archivo con el programa de AES Cripta y proporcionar la contraseña. En la línea de comandos, se puede ejecutar el "aescrypt" comando con el nombre del archivo y la contraseña a utilizar para cifrar o descifrar. Para los desarrolladores de Java, también hay una biblioteca de Java disponible que puede leer y escribir archivos cifrados AES-desde dentro de aplicaciones Java.

El uso de un algoritmo de cifrado de gran alcance de 256-bit AES cripta con seguridad puede proteger los archivos más sensibles. Una vez que un archivo está cifrado, sin la contraseña, simplemente no se puede leer. AES Crypt es un programa total y completamente open source, muchas personas han contribuido en su desarrollo, usable tanto para una implementación particular o de negocios.

3.3 Costos

Algunos de estos software son open source por lo que tendrían cierta ventaja sobre otros, con respecto al presupuesto, aunque implantarlos también conlleva a depender de las actualizaciones que estos publiquen. En el siguiente cuadro se muestran los precios a estas alternativas, consultados en las páginas oficiales de los mismos:

Producto	Precios	Detalles
CryptoForge	\$ 899,00	Da derecho a la organización a instalarlo en todos los ordenadores
TrueCrypt	Gratuito	
CryptoStudio	Gratuito	
BestCrypt	\$ 100,00	Para soporte y mantenimiento, este es el precio individual, así que depende del número de licencias necesarias
AESCrypt	Gratuito	

CAPÍTULO 4. SOLUCIÓN

4.1 Herramientas de desarrollo.

La propuesta que desarrollamos requiere montar una infraestructura entre dos equipos, uno el servidor que utilizará el sistema operativo Microsoft Windows Server 2008 R2 edición Enterprise y otro el cliente que manejará el sistema operativo Microsoft Windows 7 edición Ultimate.

4.2 Funcionalidad de la herramienta desarrollada

La razón por la que se utilizarán estas versiones de sistemas operativos, es debido a que para la gestión de certificados digitales en el servidor, la funcionalidad que maneja esto es parte de la versión Enterprise de Windows Server 2008, además esta versión nos permite manejar el login de los usuarios mediante certificados. En la parte del cliente, la edición Enterprise o Ultimate de Windows 7 maneja la herramienta de encriptación de datos llamada Bitlocker.

Lo primero que se configura en el servidor es la parte de Active Directory, para el manejo de usuarios con directivas de grupo, luego se crea la CA para la gestión de certificados digitales con entidades de revocación, luego la aplicación en .NET validará que los certificados se encuentren en el cliente para que una vez comprobado, permita encriptar la unidad de datos, esto mediante la ejecución de comandos de la consola de BitLocker, esto se mostrará mas adelante.

El manejo de las entidades antes mencionadas se lo hará únicamente a través del servidor con Windows Server 2008, ya que son servicios proporcionados por Active Directory. Todo este proceso requiere de varios pasos, los cuales se detallan a continuación:

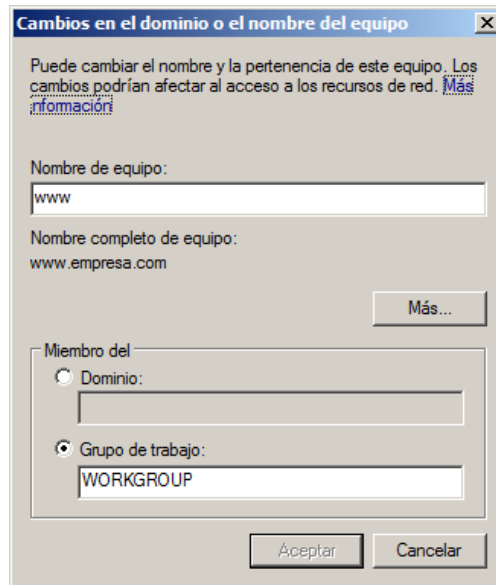
4.2.1 Instalación de Active Directory

4.2.1.1 Configuración del equipo servidor

Antes de la configuración de estos servicios, se requieren cambiar ciertos parámetros:

Cambiar el nombre del servidor.

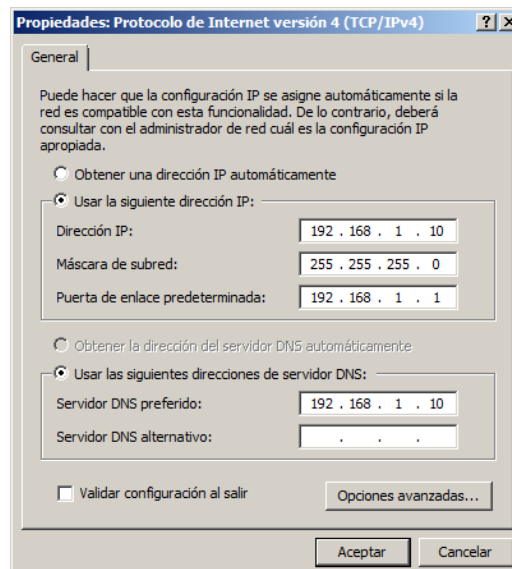
Vamos a **Inicio**, abrimos las propiedades de **Equipo**, seleccionamos **Cambiar configuración**. Aquí asignamos un nombre, en este caso se asignará el nombre **servidor(www)**.



Debemos configurar la tarjeta de red del **servidor**

Abrimos **Centro de redes y recursos compartidos**, clic en **Cambiar la configuración del adaptador**, abrimos las propiedades de la tarjeta de red, desactivamos la funcionalidad IPv6.

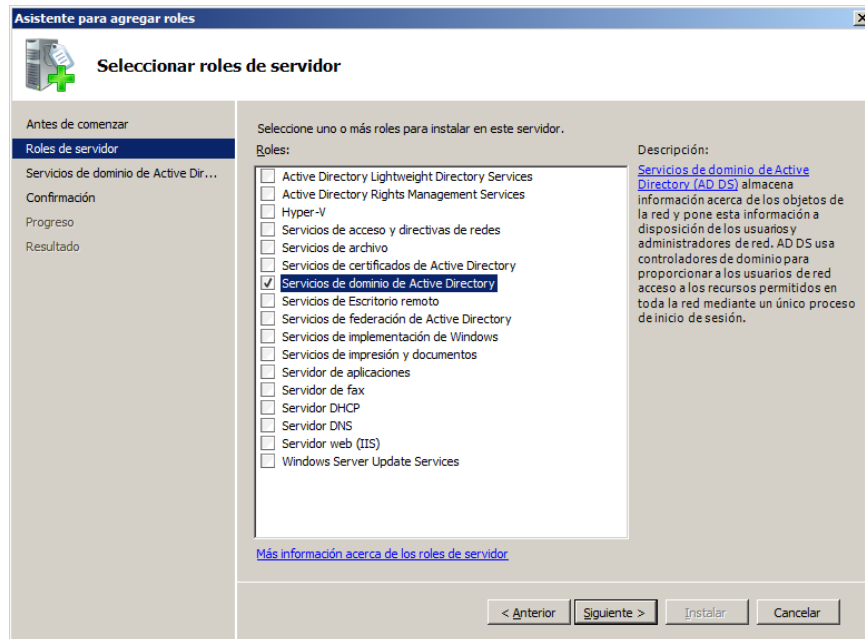
Asignamos la dirección IPv4 192.168.1.10 con máscara 255.255.255.0, puerta de enlace 192.168.1.1 y servidor DNS 192.168.1.10.



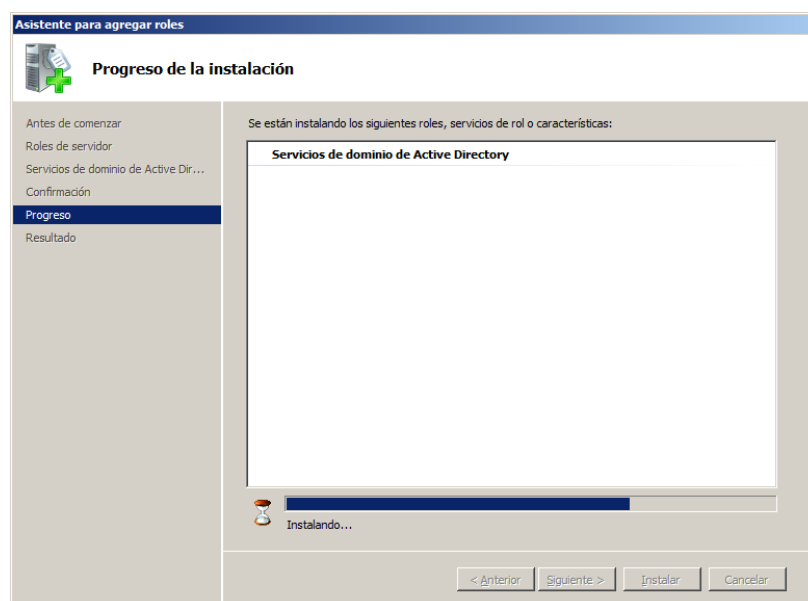
Agregamos el servicio de Active Directory

Clic en **Inicio**, abrimos **Herramientas administrativas**, luego seleccionamos **Administrador del servidor**.

Clic en **Roles**, y seleccionamos **Agregar rol**, seleccionamos **Servicio de dominio de Active Directory**.

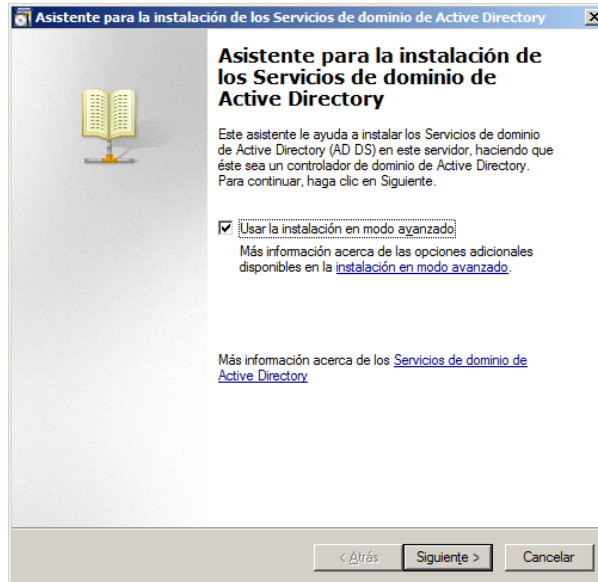


Clic en **Agregar características requeridas**, clic en **siguiete** dos veces, y luego **Instalar**.

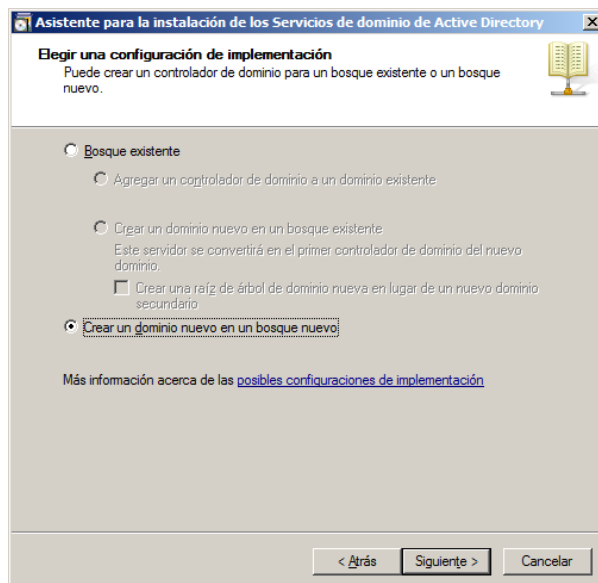


Configuramos Active Directory

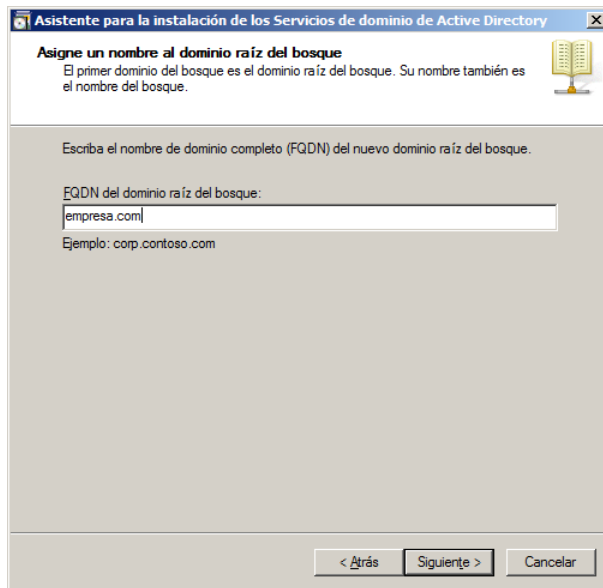
Ejecutamos el comando **dcpromo.exe** para abrir el asistente de instalación. Seleccionamos la opción de **instalación de modo avanzado**.



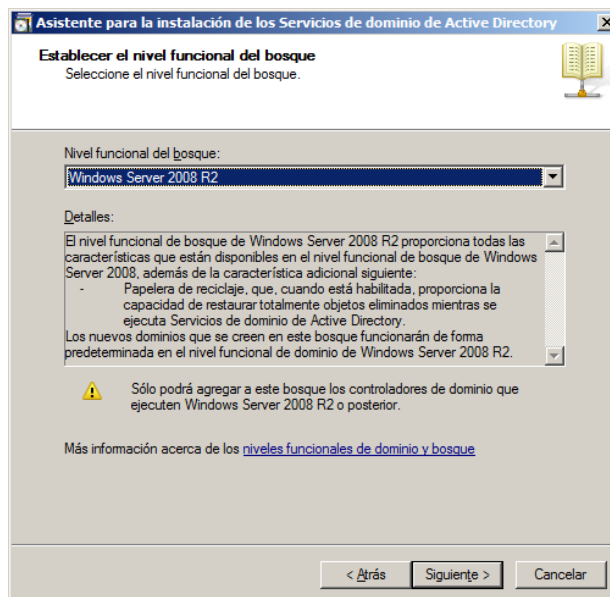
Luego seleccionamos **siguiente** dos veces, escogemos la opción **crear un dominio nuevo en un bosque nuevo** y luego siguiente.



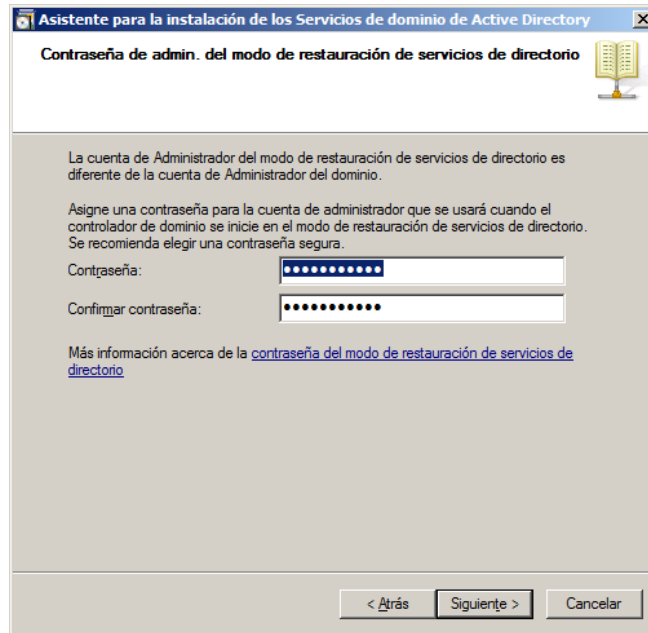
Ingresamos el nombre de dominio FQDN, se ingresó **empresa.com**, luego seleccionamos **siguiente** dos veces.



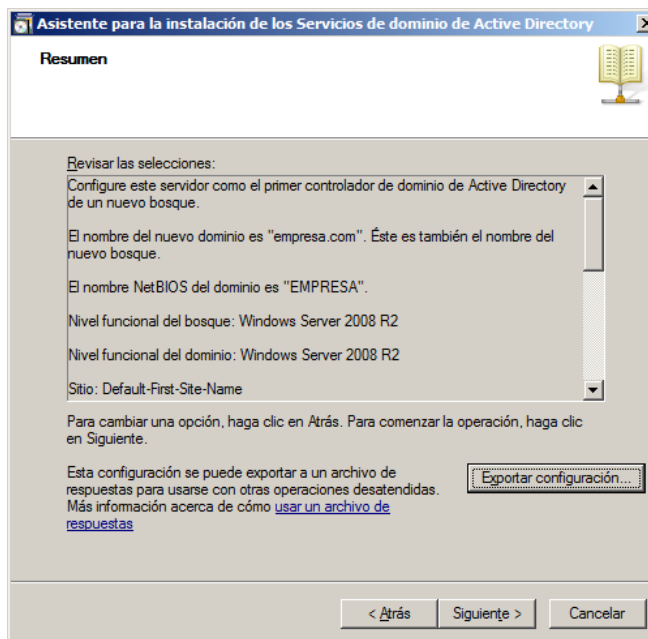
Luego procedemos a escoger en **nivel funcional de bosque**, en este caso utilizaremos Windows Server 2008 R2 ya que es compatible con Windows 7, si se requeriría compatibilidad con versiones anteriores de Windows, se tendrá que escoger la adecuada, y seleccionamos **siguiete** dos veces.



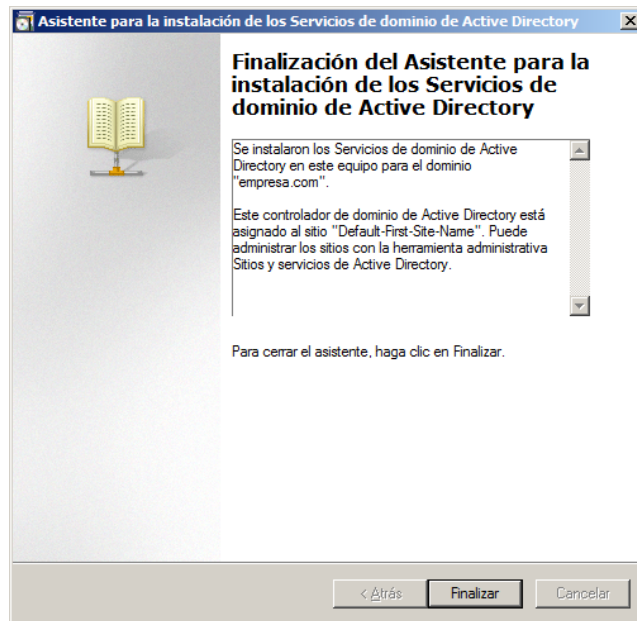
Escogemos opción **Si**, clic en **siguiete**, ingresamos la contraseña del servicio y clic en **siguiete**.



Si deseamos mantener un log de la configuración podemos seleccionar la opción **exportar configuración**, una vez hecho esto, clic en **siguiete**, e iniciará la instalación.

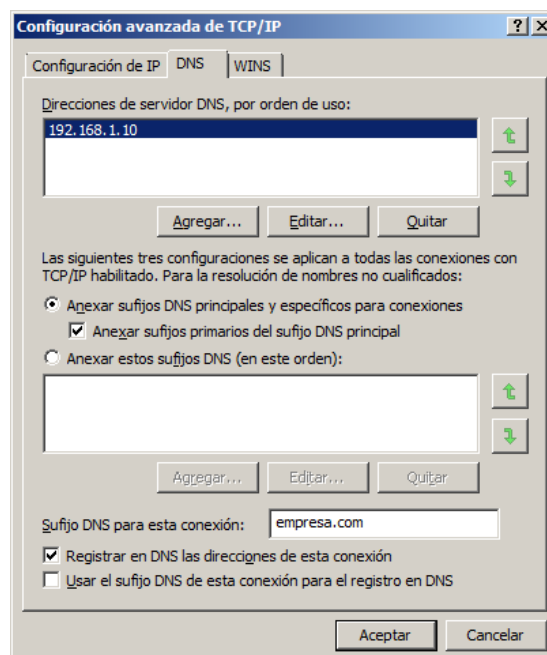


Después de la instalación, damos clic en **Finalizar**, y reiniciamos el equipo.



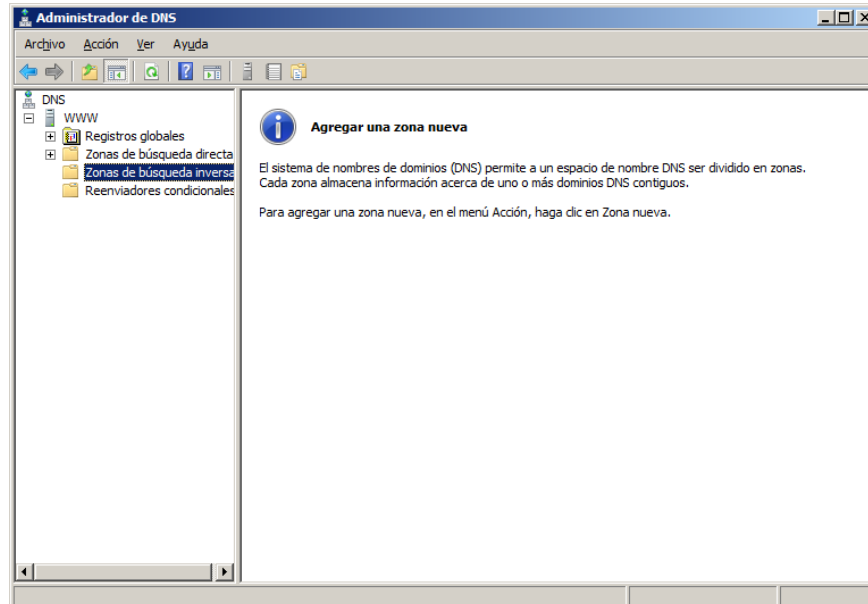
Una vez reiniciado el sistema, se puede ver el dominio asociado con la cuenta de Administrador, esto nos comprueba la creación del dominio.

Nos logueamos y accedemos nuevamente a la configuración de la tarjeta de red, comprobamos que el servidor DNS tenga la IP del propio servidor, en este caso 192.168.1.10 porque al momento de reiniciar el servidor la IP del servidor DNS se pone por default 127.0.0.1, luego hacemos clic en **opciones avanzadas** y en la pestaña **DNS** en la parte que dice **sufijo DNS para esta conexión** ingresamos el nombre del dominio que creamos (empresa.com), aceptamos y salimos.

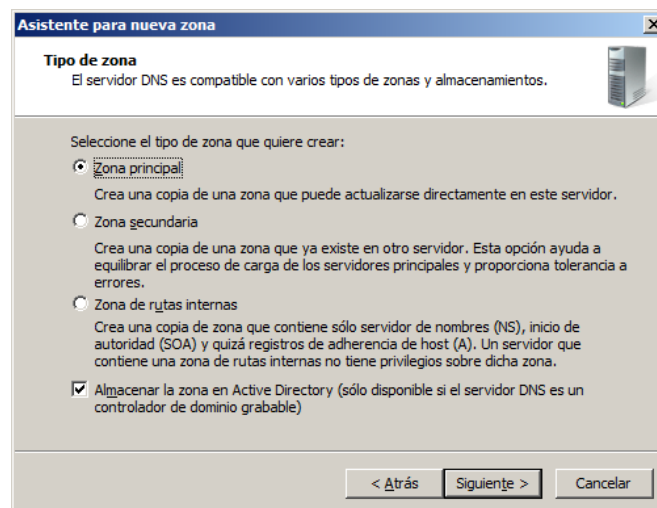


4.2.1.2 Configuración de DNS

Vamos a **Inicio** -> **Herramientas administrativas**, y seleccionamos **DNS**, en el menú de la parte izquierda, nos ubicamos en la opción **Zonas de búsqueda inversa**.

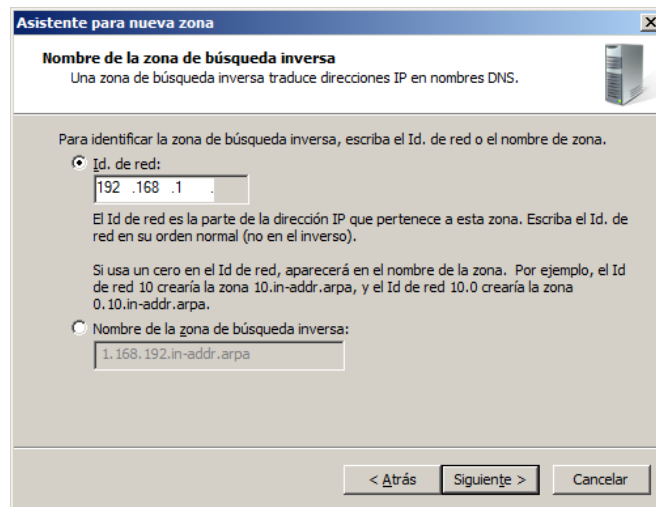


Clic derecho en **zona nueva**, clic en **siguiente**, en el tipo de zona escogemos **zona principal**, luego clic en **siguiente**.

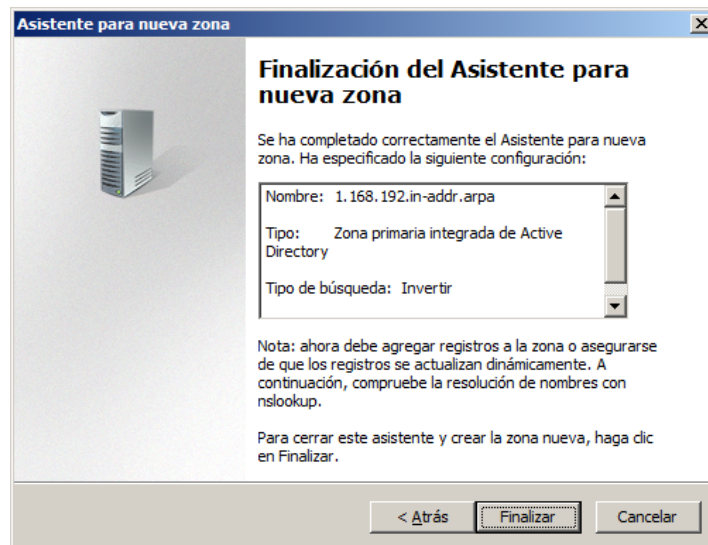


En el ámbito de replicación de zona seleccionamos la opción, **Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio**, clic en **siguiente**, en el nombre de zona escogemos **Zona de búsqueda inversa para IPv4**, clic en **siguiente**, luego ingresamos el identificador de red, que son los 3

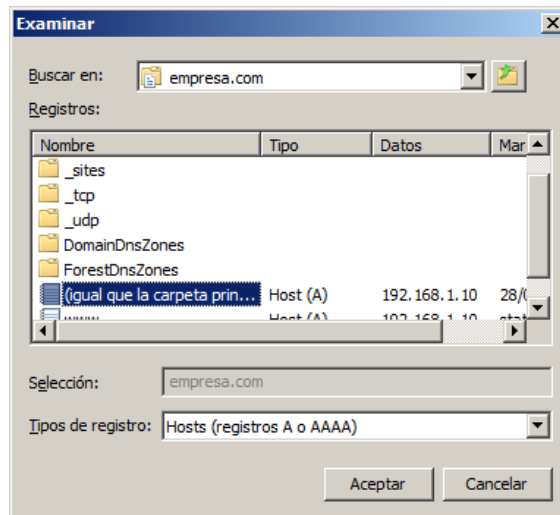
primeros octetos de la dirección IP del servidor, para nuestro caso es **192.168.1**, y clic en **siguiente**.



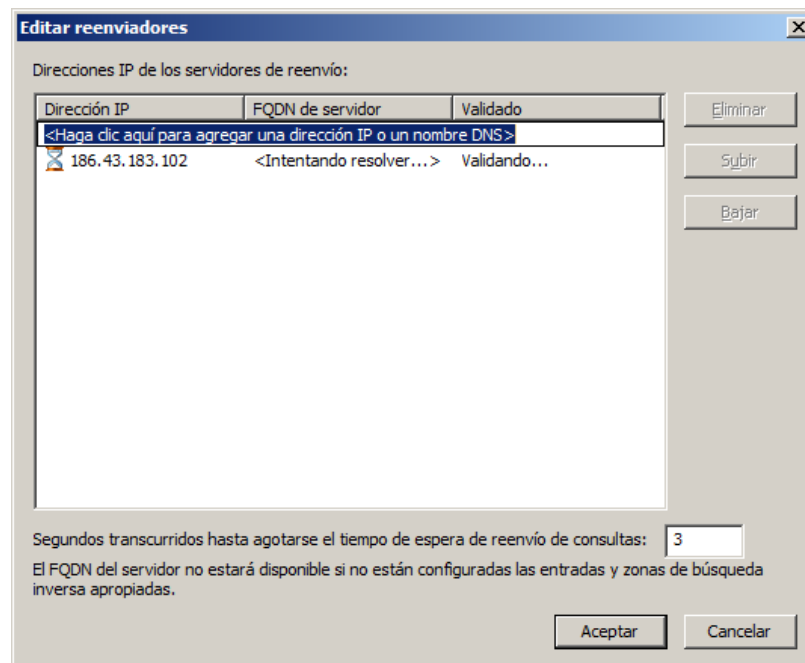
En las actualizaciones automáticas, escogemos la opción que más convenga, clic en **siguiente** y **finalizar**.



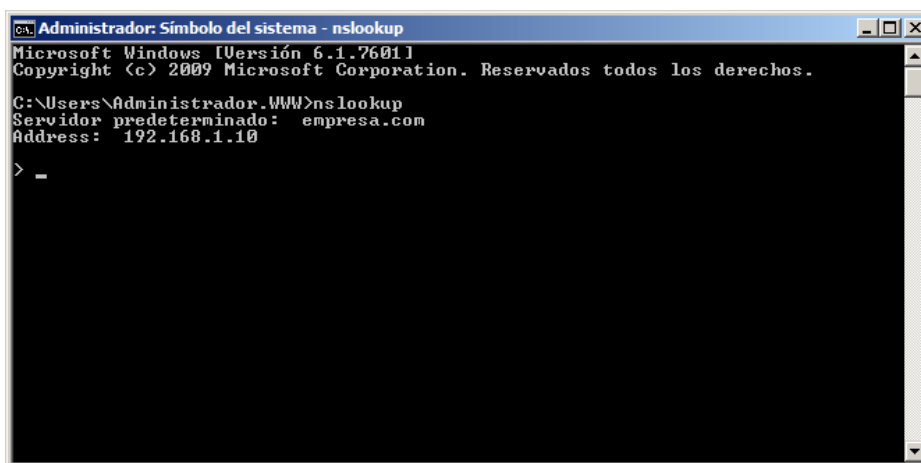
Luego seleccionamos la zona creada anteriormente y la abrimos con doble clic, dentro de esta, clic derecho y seleccionamos **nuevo puntero (PTR)**, opción examinar, doble clic es **Servidor**, doble clic en **Zona de Búsqueda directa**, doble clic en nombre de dominio, en este caso empresa.com, y escogemos la opción (**igual que la carpeta principal**), y clic en **Aceptar**.



Ahora vamos nuevamente al menú izquierdo, y clic derecho en el **servidor**, y seleccionamos propiedades y vamos a la pestaña **Reenviadores** y escogemos la opción **editar**, y ponemos la IP del dominio (186.43.183.102), actualizamos.



Para comprobar abrimos **command**, y ejecutamos el comando **nslookup** y comprobamos que en servidor predeterminado nos dé el nombre del dominio (empresa.com) y en **address** la dirección del dominio ingresada anteriormente (10.69.100.100).



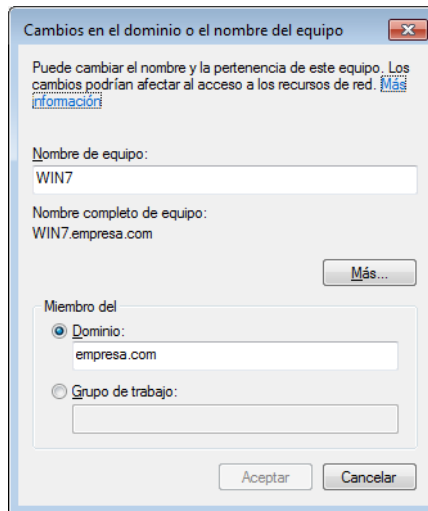
```
Administrador: Símbolo del sistema - nslookup
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\Administrador.WWW>nslookup
Servidor predeterminado: empresa.com
Address: 192.168.1.10
> _
```

4.2.1.3 Configuración del equipo cliente

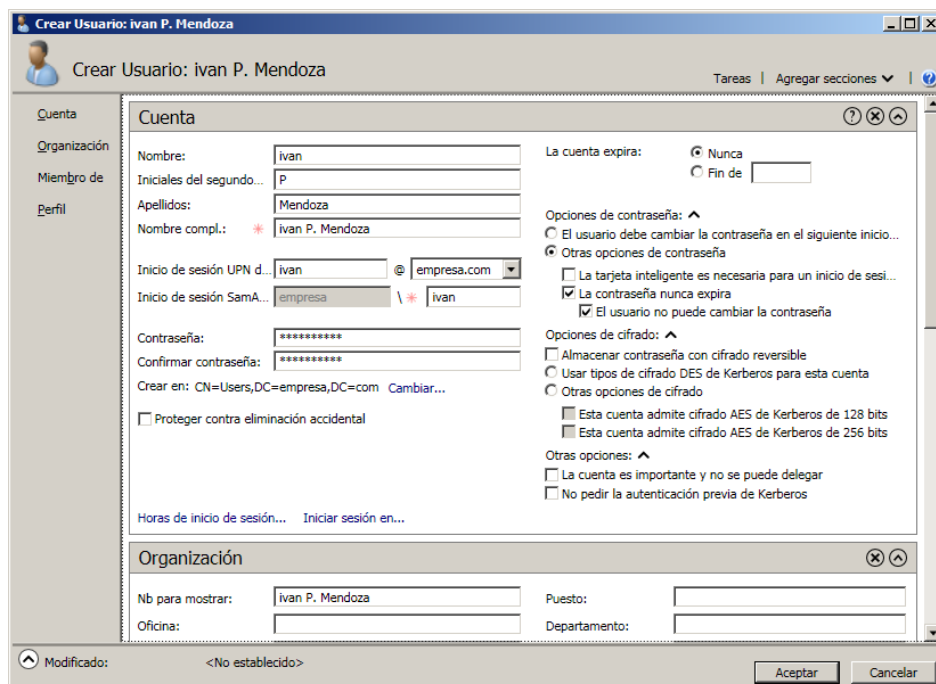
Esto se configura en el equipo cliente, es decir en el que utiliza Windows 7. Configuramos la tarjeta de red para la conexión con Active Directory, en este caso asignamos la dirección IPv4 192.168.1.100 con máscara 255.255.255.0, puerta de enlace 192.168.1.1 y servidor DNS 192.168.1.10.

Para comprobar que el servidor resuelve los nombre de dominio, abrimos el símbolo del sistema y ejecutamos el comando **nslookup**, y comprobamos que en servidor predeterminado nos dé el nombre del dominio (empresa.com) y en address la dirección del dominio ingresada en el servidor (192.168.1.10).

Para unir el equipo al dominio creado a **Inicio**, click derecho en equipo y propiedades, seleccionamos la opción **cambiar configuración** y luego click en el boton **cambiar**, escogemos la opción **dominio** e ingresamos el nombre de nuestro dominio (empresa.com), nos pedirá loguearnos con la cuenta de administrador y la contraseña, aceptamos y reiniciamos.



Volvemos a Windows Server, vamos a **Inicio -> Herramientas administrativas -> Centro de administracion de Active Directory**, en el menú en la parte izquierda, damos clic en el nombre del dominio que creamos, y en la parte derecha damos clic en la carpeta **users**, luego damos clic en usuarios del dominio y en el menú en la parte derecha escogemos y luego usuario y llenamos con los datos del usuario.



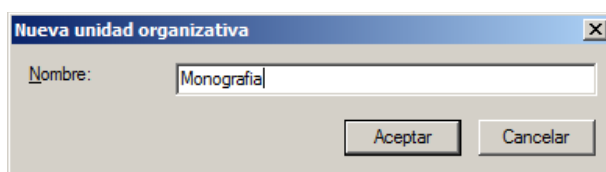
4.2.1.4 Directivas de grupo

Mediante las directivas de grupo, que son parte de las herramientas administrativas del Server 2008 podemos controlar varias tareas que queremos que se cumplan en los equipos clientes.

Para controlar que el usuario o equipo no pueda iniciar sesión mientras el servidor no esté disponible, se puede realizar la siguiente configuración:

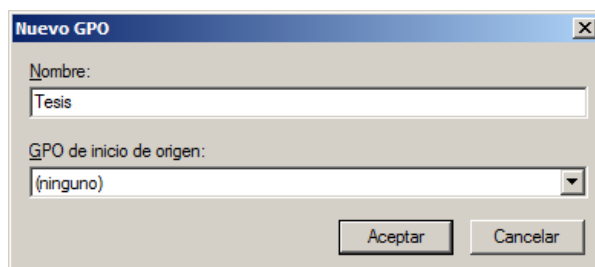
Clic en **Inicio -> Herramientas administrativas -> Administración de directivas de grupo**

Abrimos el bosque del dominio creado en nuestro caso **Bosque: empresa.com**, vamos a **Dominios -> Empresa.com**. Clic derecho en **Empresa.com**, y seleccionamos **Nueva unidad organizativa**, ingresamos un nombre (**Monografía**) y clic en **aceptar**.

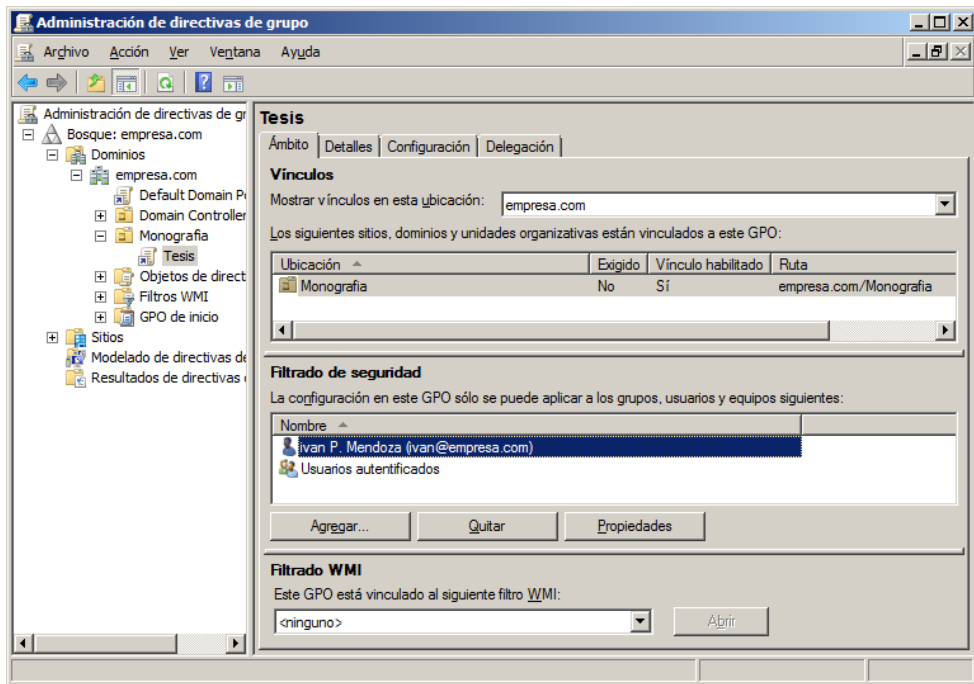


Clic derecho en la unidad organizativa creada (**Monografía**), seleccionamos **Crear un GPO en este dominio y vincularlo aquí**, ingresamos el nombre para la directiva (**Tesis**) y clic en **Aceptar**.

Seleccionamos el GPO creado (**Tesis**) y clic en **Aceptar**.

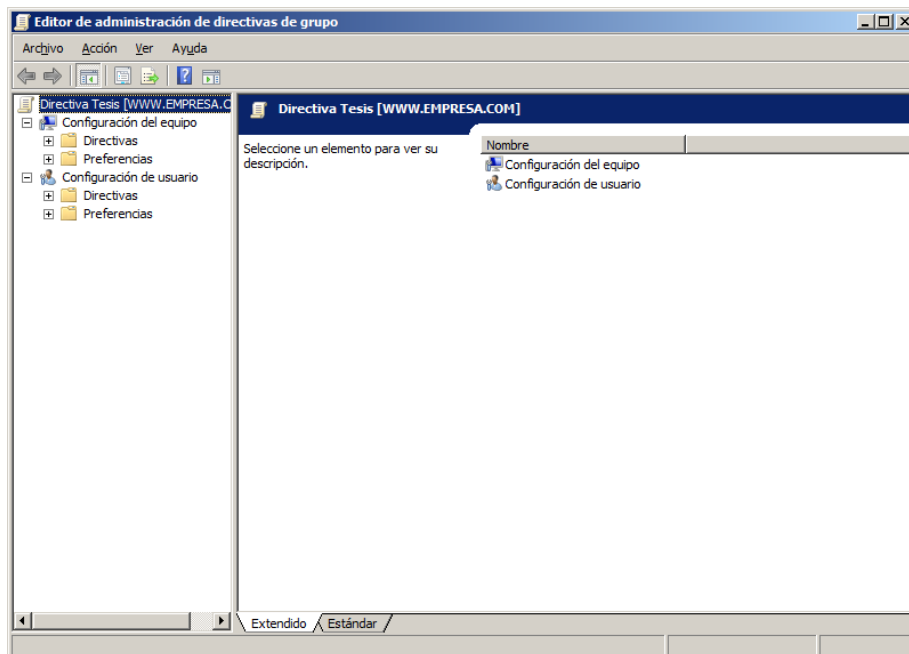


En la parte inferior de la pestaña **ámbito**, podemos vincular a este GPO con los usuarios o equipos que obtendrán las políticas que se configurarán, clic en **agregar**, ingresamos el nombre del usuario y clic en **Comprobar nombres**, deberá reconocer el usuario existente en el dominio, clic en **Aceptar** y se agregará a la lista de **filtrado de seguridad**.



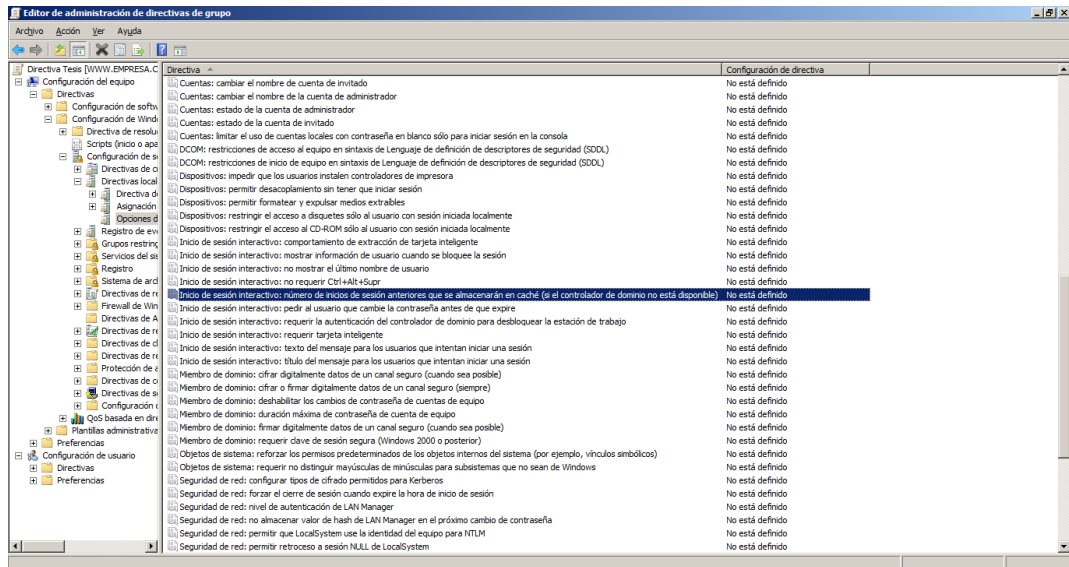
Ahora pasamos a crear las directivas para esa unidad organizativa:

Clic derecho en el GPO creado (**Tesis**) y seleccionamos la opción **Editar**, se abrirá una nueva ventana, la cual contendrá todas las directivas de grupo configurables.

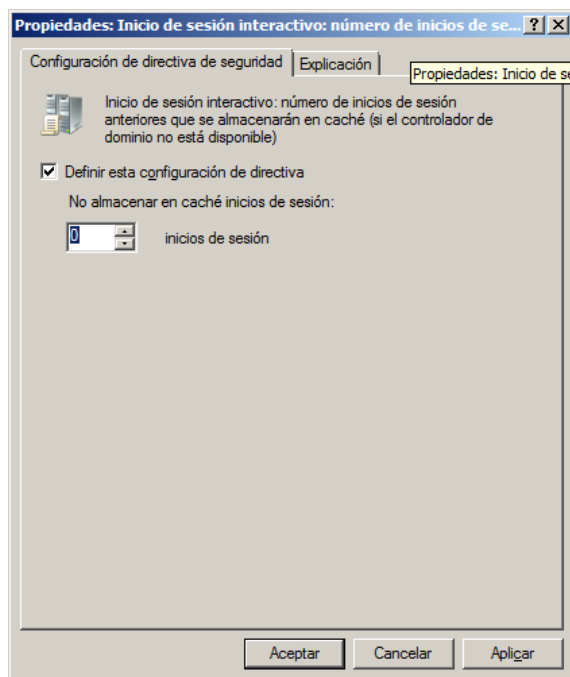


Para controlar los inicios de sesión, de manera que los usuarios no puedan loguearse cuando el servidor este apagado, ya que por defecto el equipo guarda en cache las contraseñas, y como medida de seguridad se debería desactivar, para esto:

En la nueva ventana **Editor de Administración de Directivas de Grupo**, clic en **Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad**, buscamos la directiva llamada **Inicio de sesión interactivo: Número de inicios de sesión anteriores que se almacenaran en caché (si el controlador de dominio no está disponible)**.



Clic derecho y seleccionamos propiedades, en la pestaña configuración de directiva de seguridad, seleccionamos la casilla **definir esta configuración de directiva**, e ingresamos 0 en **inicios de sesión**, y clic en **aceptar**.

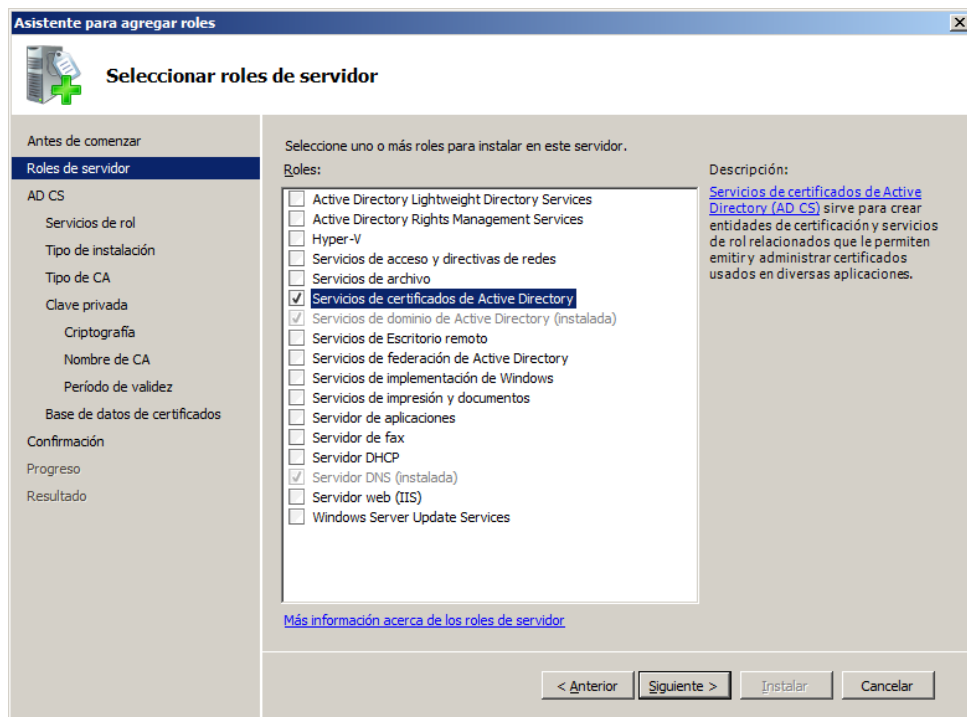


4.2.2 Creación de certificados digitales.

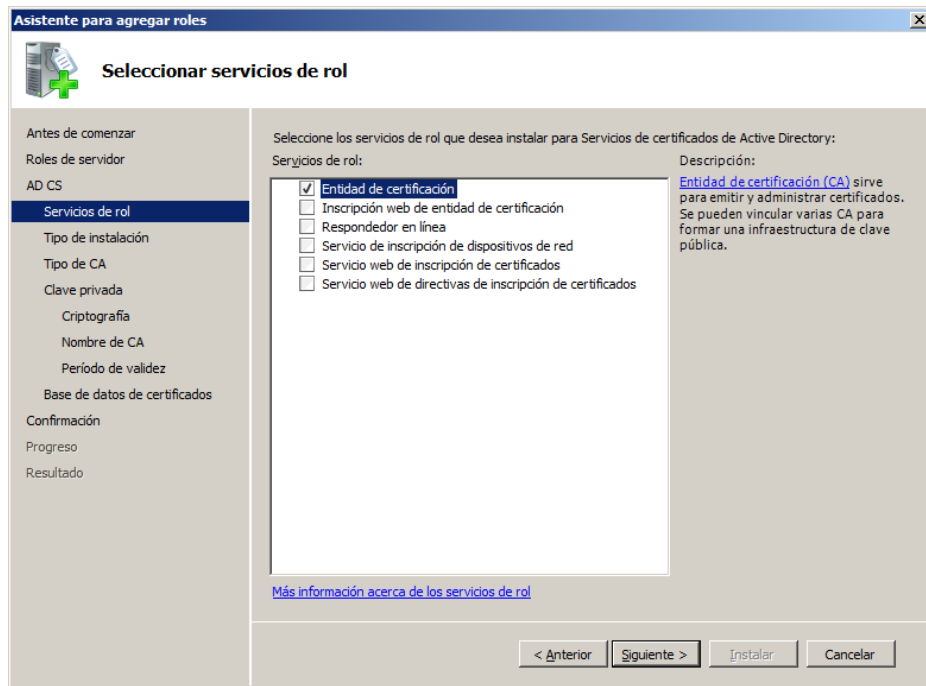
Se utilizará un certificado a nivel de máquina, lo que significa que se va a manejar un solo certificado. Para la creación de estos, debemos añadir el servicio de Administración de certificados de Active Directory. Para esto el proceso es el siguiente:

Clic en **Inicio**, abrimos **Herramientas administrativas**, luego seleccionamos **Administrador del servidor**.

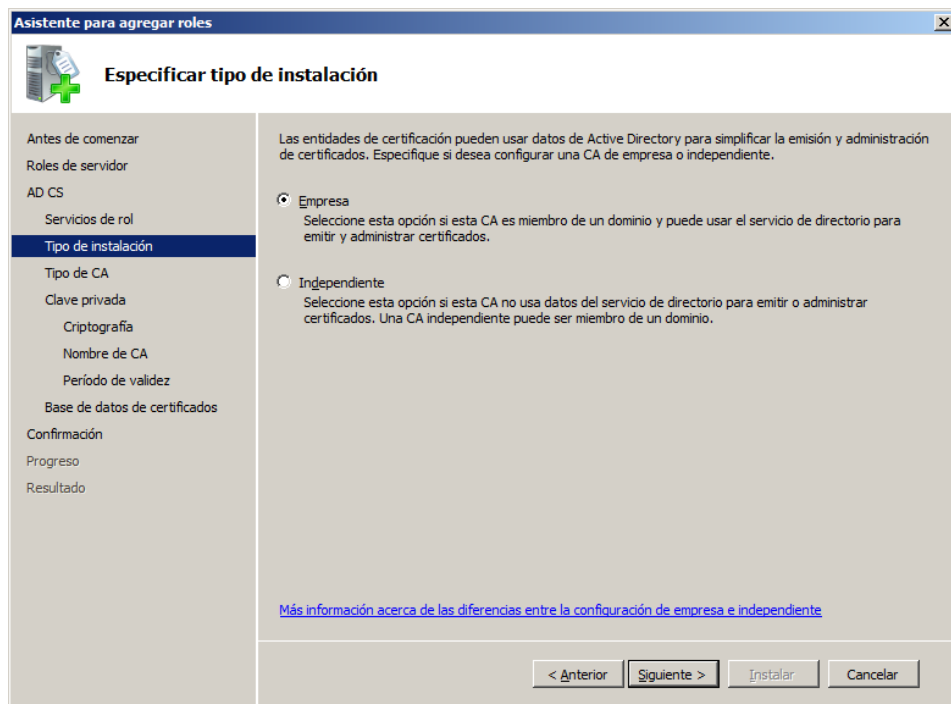
En la sección de resumen de roles, clic en **Añadir roles**, y siguiente, seleccionamos **Servicio de Certificados de Active Directory** y clic en siguiente dos veces.



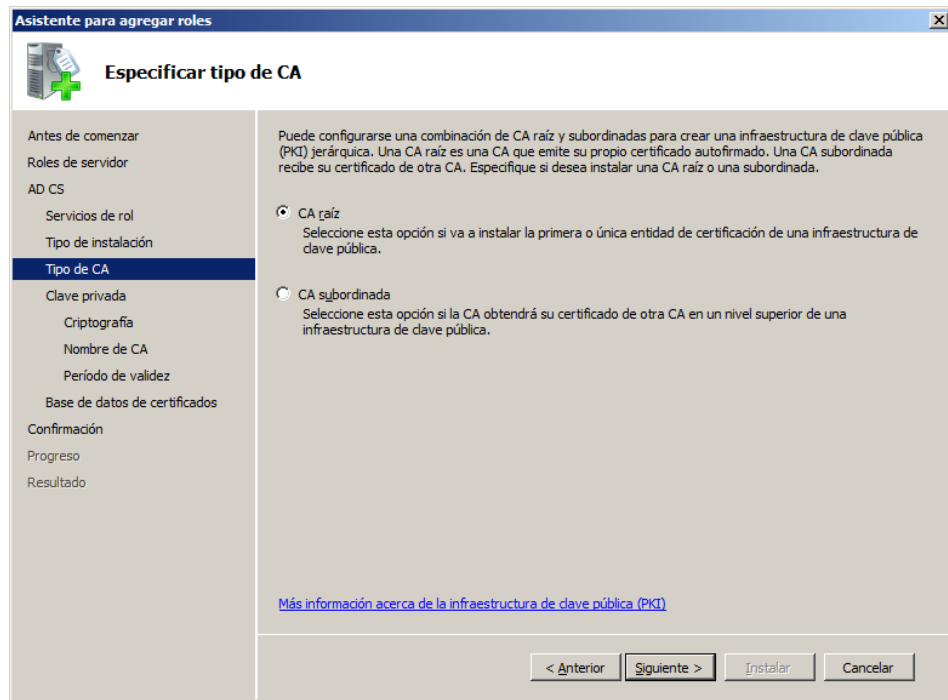
En **Servicios de rol**, seleccionamos la **Entidad de Certificación**, y damos clic en siguiente.



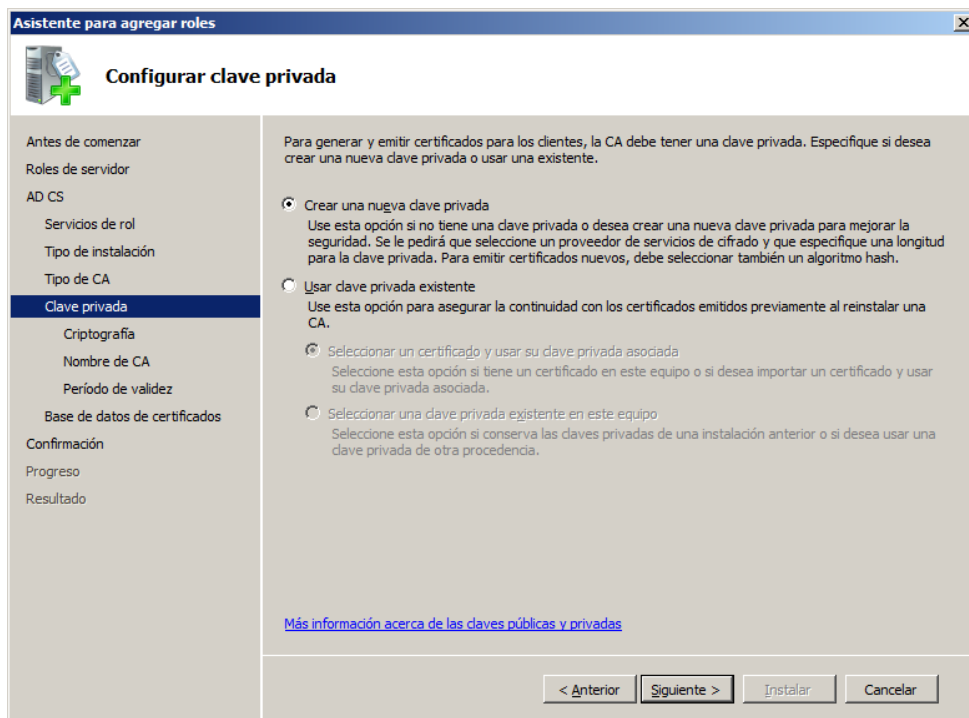
En **tipo de instalación**, seleccionamos Empresa, y clic en siguiente.



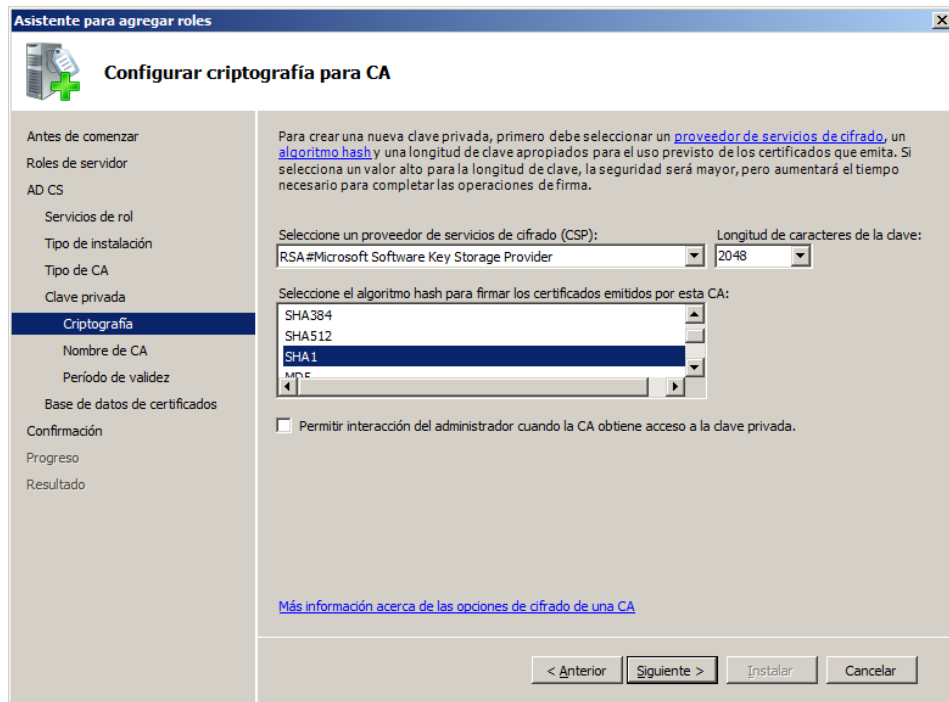
En **tipo de CA**, seleccionamos **CA Raiz**, y clic en siguiente.



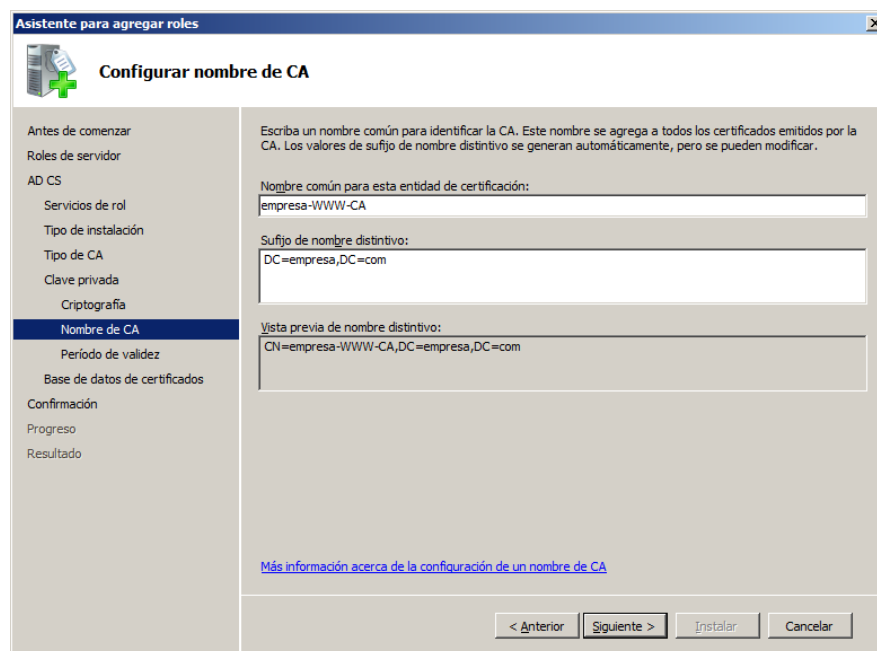
En la configuración de clave privada, seleccionamos **Crear nueva clave privada**, y clic en siguiente.



En la **configuración criptografía para CA**, seleccionamos como proveedor de servicios de cifrado (CSP) RSA, la longitud de la clave elegimos de 2048 bytes, y algoritmo hash que se utilizara para firmar los certificados emitidos es SHA1, y clic en siguiente.

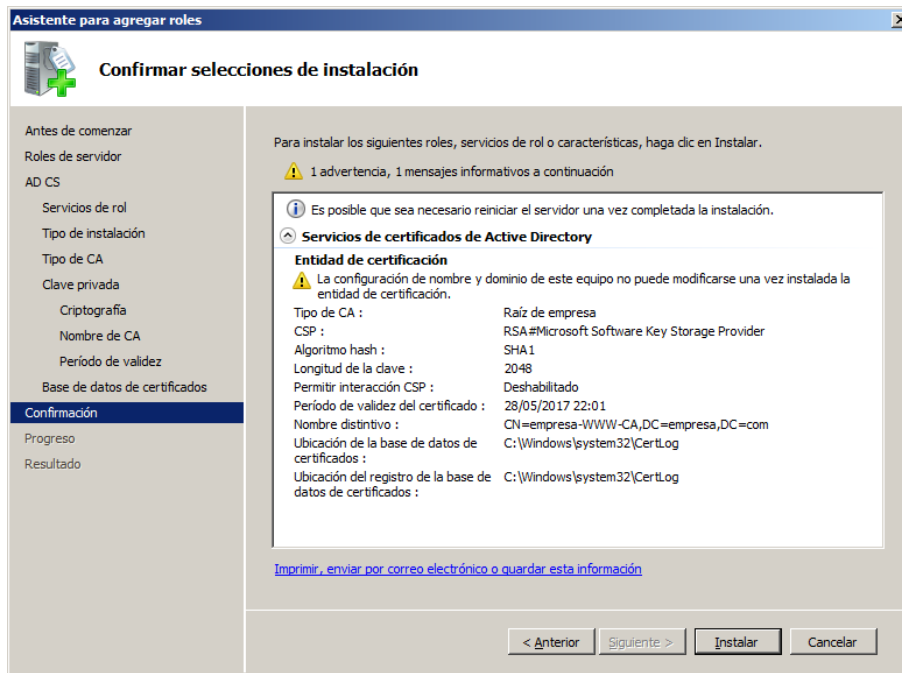


En **configurar nombre de CA**, mantendremos los valores por default ya que estamos creando la CA para el dominio antes creado y click en siguiente.



En **periodo de validez**, manejaremos una duración de 5 años.

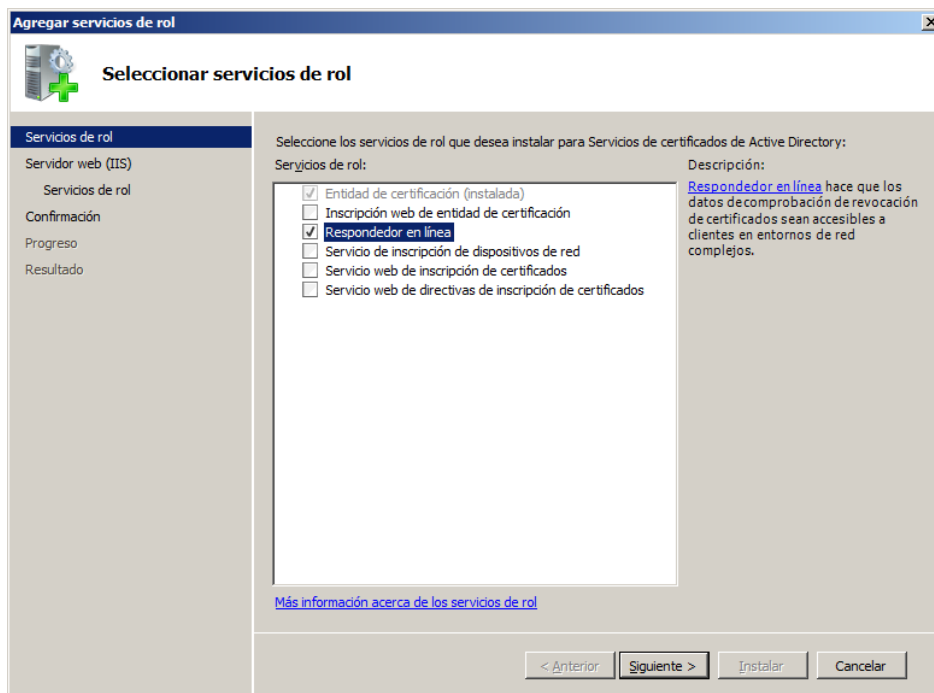
En **base de datos de certificados**, también se mantendrá o se podrá cambiar la ruta de la ubicación y registro de la base de datos de los certificados, clic en siguiente e instalar.



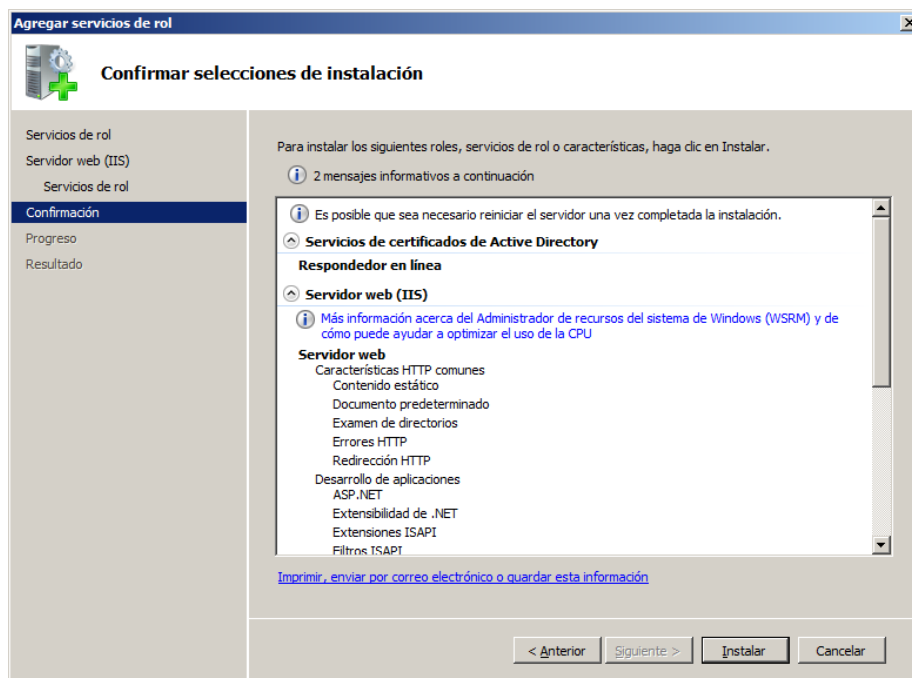
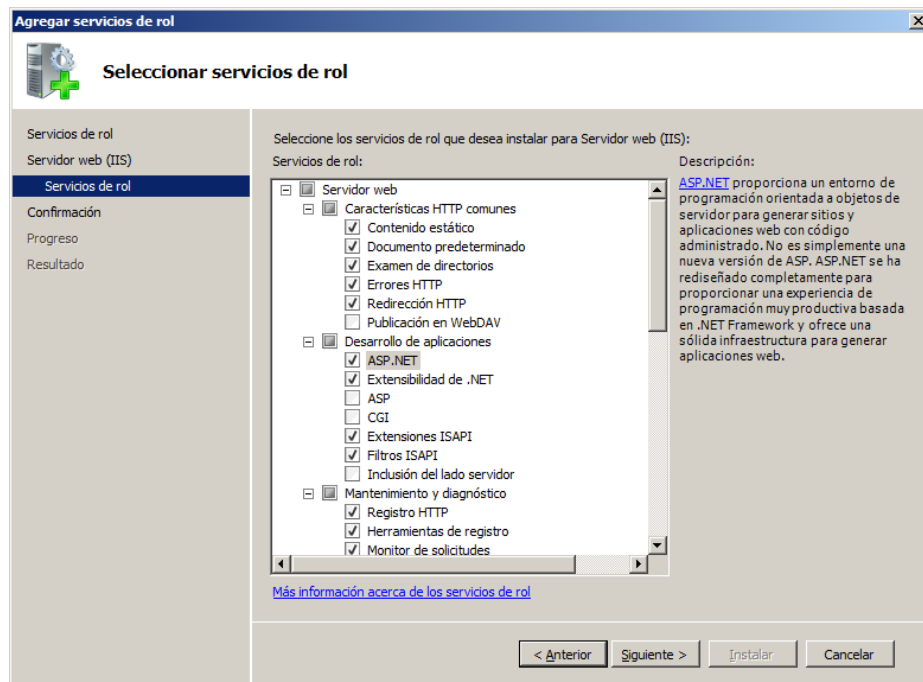
4.2.2.1 Instalación de Respondedor Online

Clic en **Inicio**, abrimos **Herramientas administrativas**, luego seleccionamos **Administrador del servidor**.

Clic en **Agregar Servicio de Rol**, y seleccionamos **Respondedor en línea**, agregamos los servicios de rol requeridos y clic en siguiente dos veces.



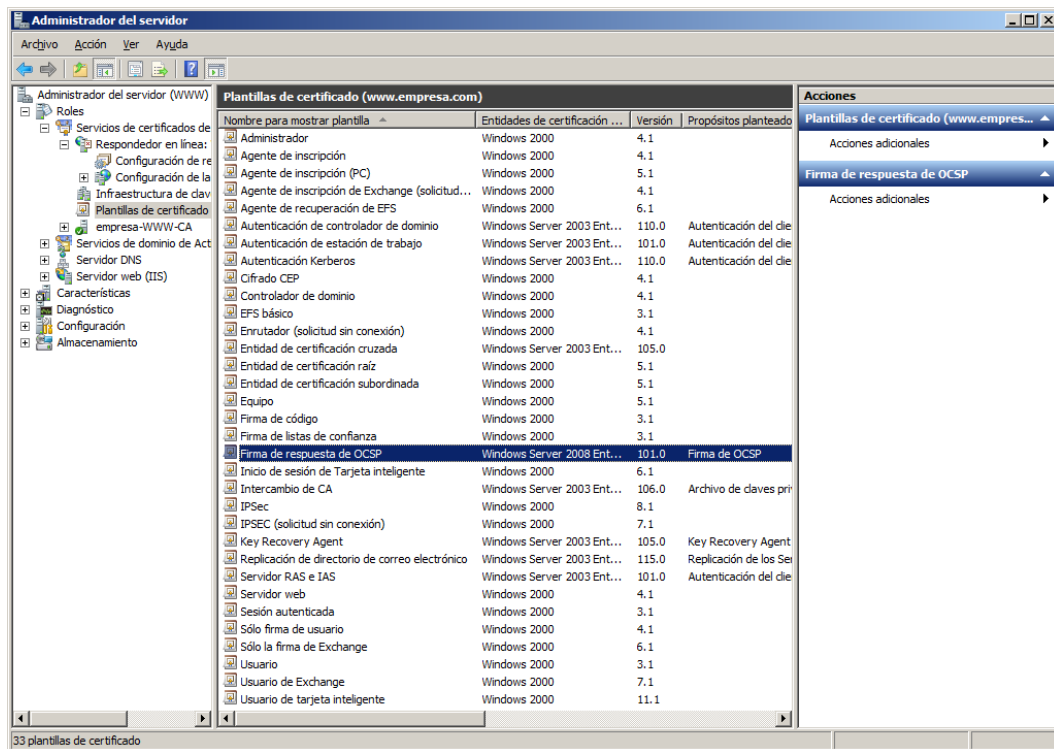
En **servicios de rol**, clic en **ASP .Net**, agregamos los servicios de rol requeridos para ASP .Net y clic en siguiente, e inicia la instalación.



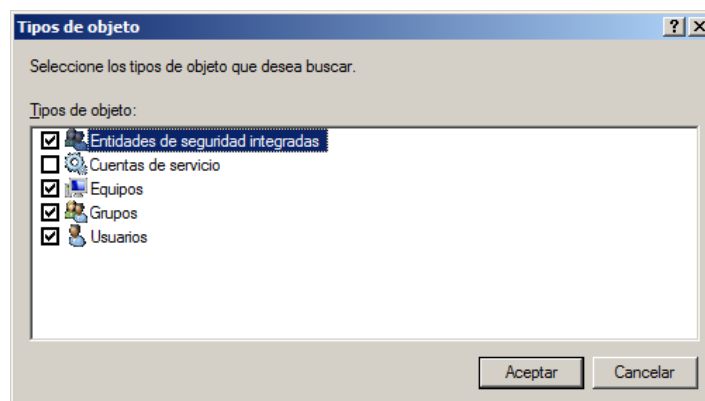
4.2.2.2 Configuración de la CA para emitir certificados

Abrimos las plantillas de certificados, se encuentran en el menú izquierdo de **Administrador de Servidor**, abrimos **Roles -> Servicios de certificados -> Respondedor en línea -> Plantillas de certificado**, buscamos la plantilla que se

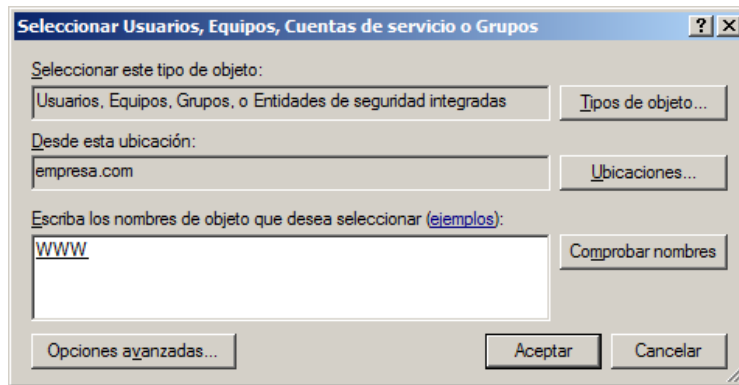
llama **firma de respuesta de OCSP**, clic derecho y seleccionamos **plantilla duplicada**.



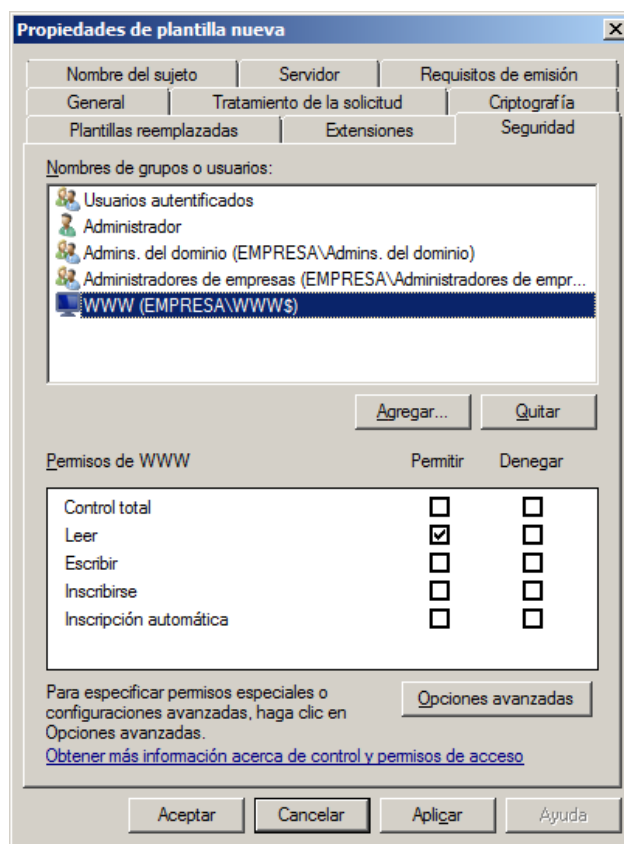
En la plantilla duplicada se presentan varias opciones, organizadas mediante pestañas, en la pestaña Seguridad, clic en agregar, clic en tipos de objetos y seleccionamos **Entidades de seguridad integradas, Equipos, Grupos y Usuarios** y clic en **Aceptar**.



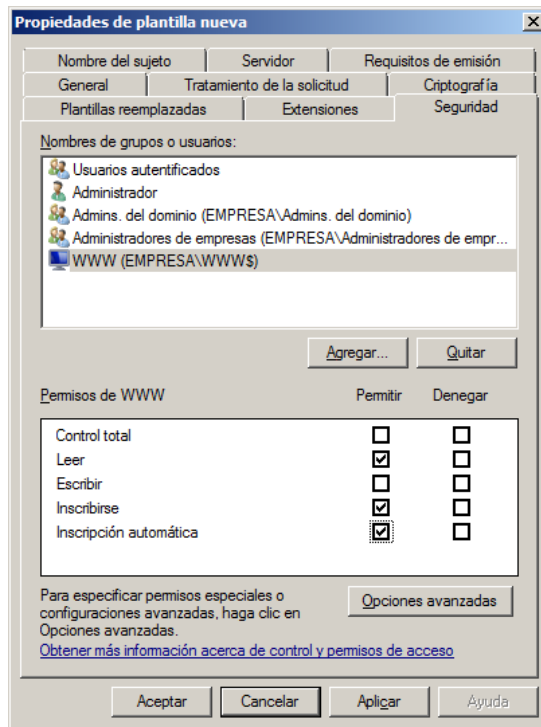
Luego en la opción de escribir los **Nombres de objetos que desea selección**, ingresamos el nombre del servidor en nuestro caso **www**, clic en comprobar nombres y nos aparece un cuadro de dialogo en el cual seleccionamos el equipo con el nombre de nuestro servidor, clic en Aceptar



Y comprobaremos que se agregó el servidor en la lista.



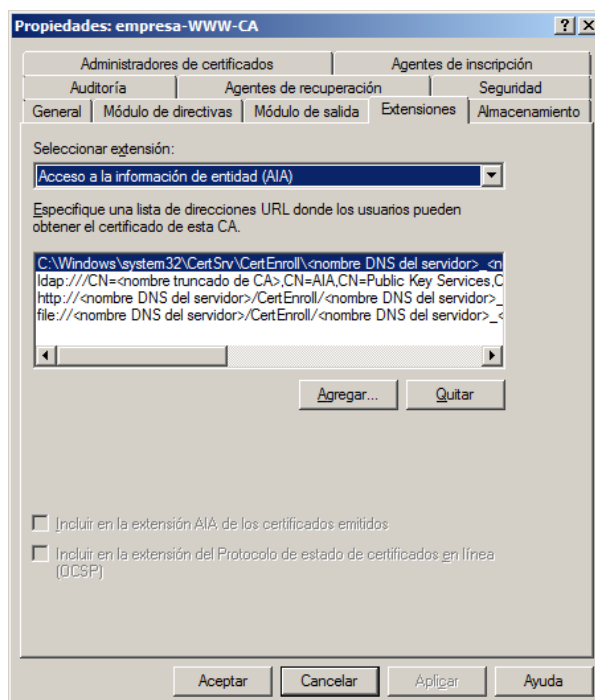
Seleccionamos el servidor que se agregó en la lista y en la parte inferior, damos los permisos de lectura, inscripción e inscripción automática, clic en Aceptar.



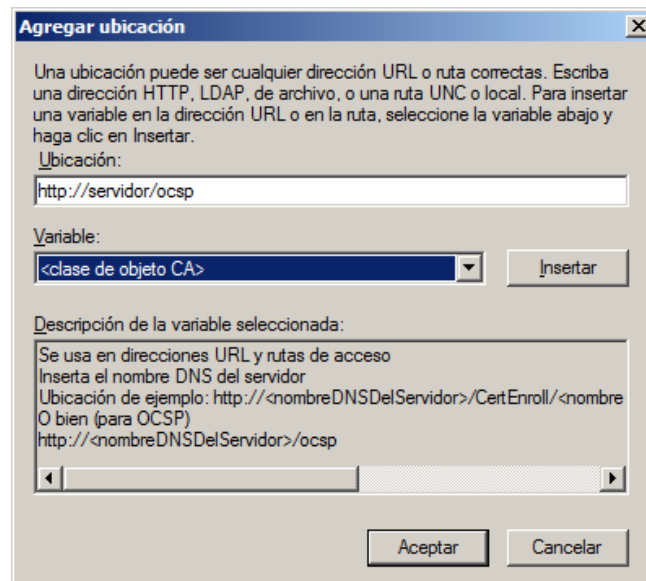
4.2.2.3 Configurar CA para soporte de respondedor en línea

Clic en Inicio -> Herramientas Administrativas -> Entidad de Certificación, seleccionamos el nombre de la CA creada, y en el menú Acción, clic en propiedades.

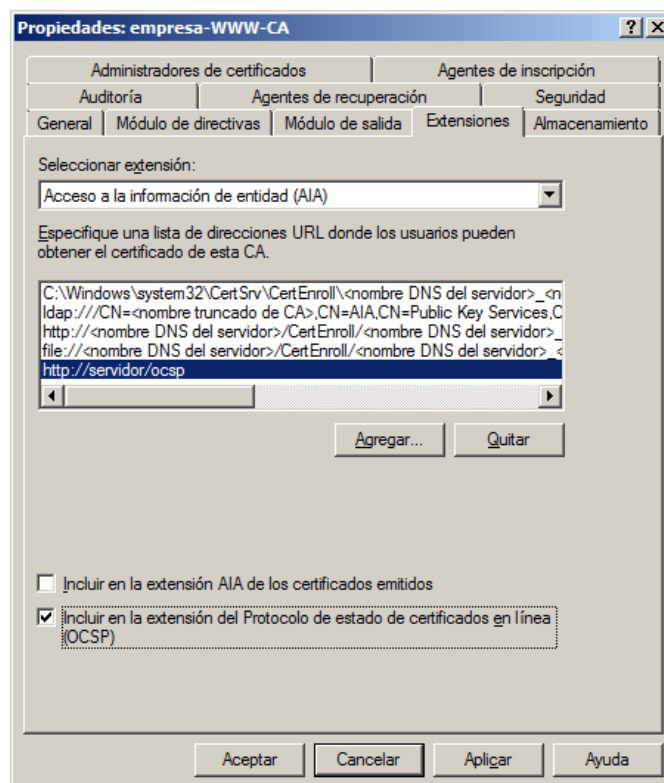
Vamos a la pestaña extensión, y en Seleccionar extensión, elegimos Acceso a la Información de Entidad (AIA).



Clic en **agregar**, en ubicación ingresamos la dirección del servidor DNS, de modo que quedaría http://servidor/ocsp, y clic en aceptar.

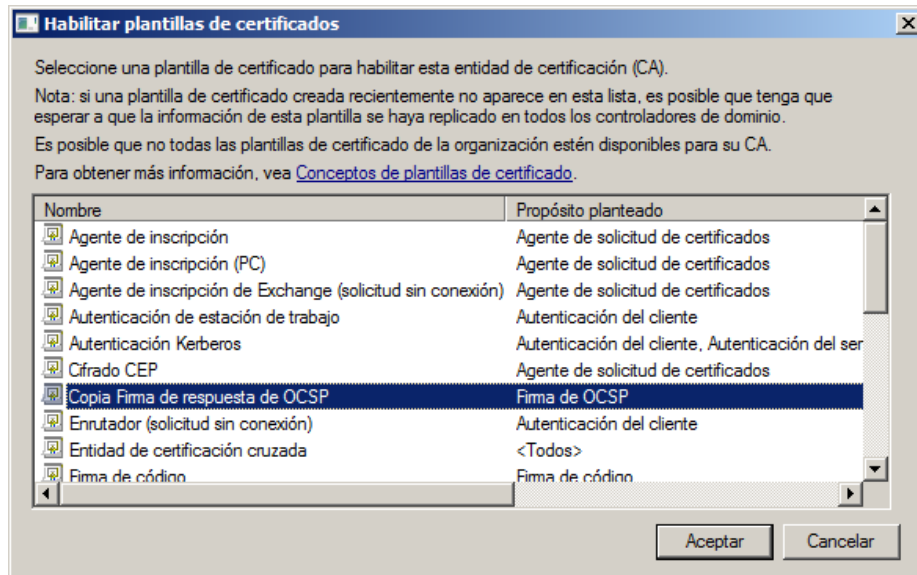


Luego seleccionamos la ubicación agregada, y seleccionamos la opción **Incluir en la extensión del protocolo de estado de certificados en línea (OCSP)**, clic en **aceptar** y luego clic en si para **reiniciar el Servicio de certificados de Active Directory**.

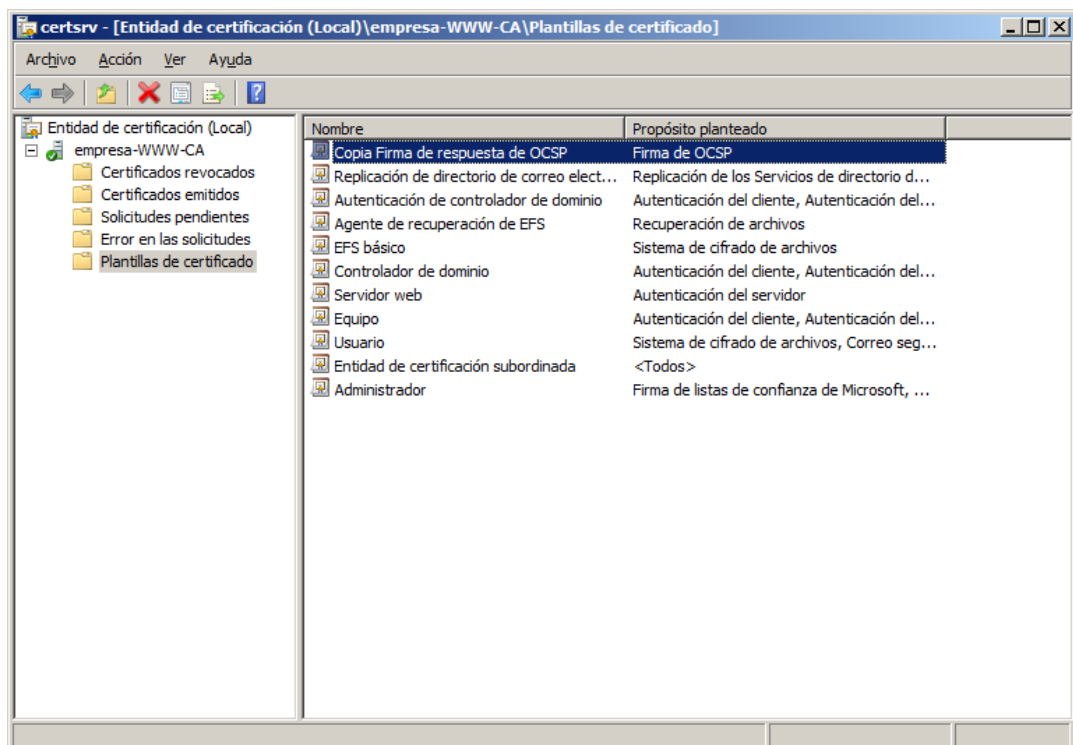


En la ventana de la Entidad de Certificación, clic derecho en Plantillas de certificado, seleccionamos nuevo y clic en Certificado que se va a emitir.

En el cuadro de dialogo Habilitar plantillas de certificados, seleccionamos el duplicado de la firma OCSP, que se creó anteriormente y clic en Aceptar.



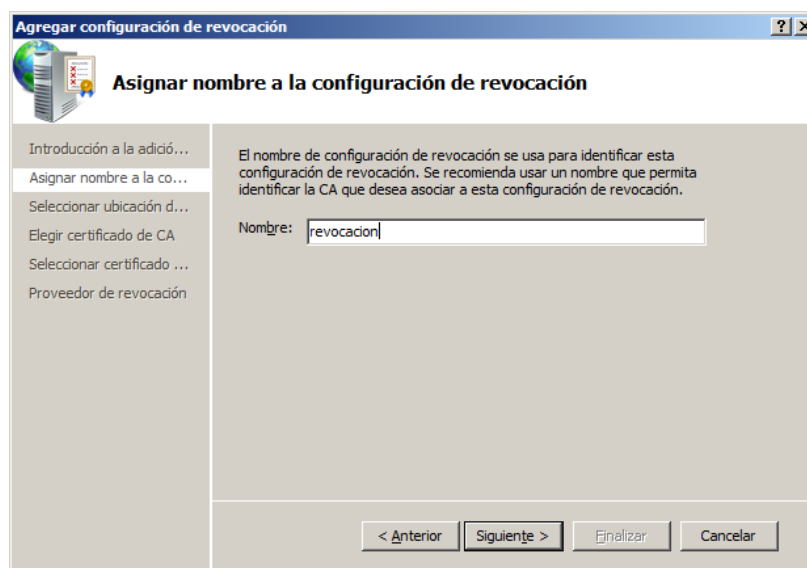
Aparecerá en la lista de Plantillas de certificado.



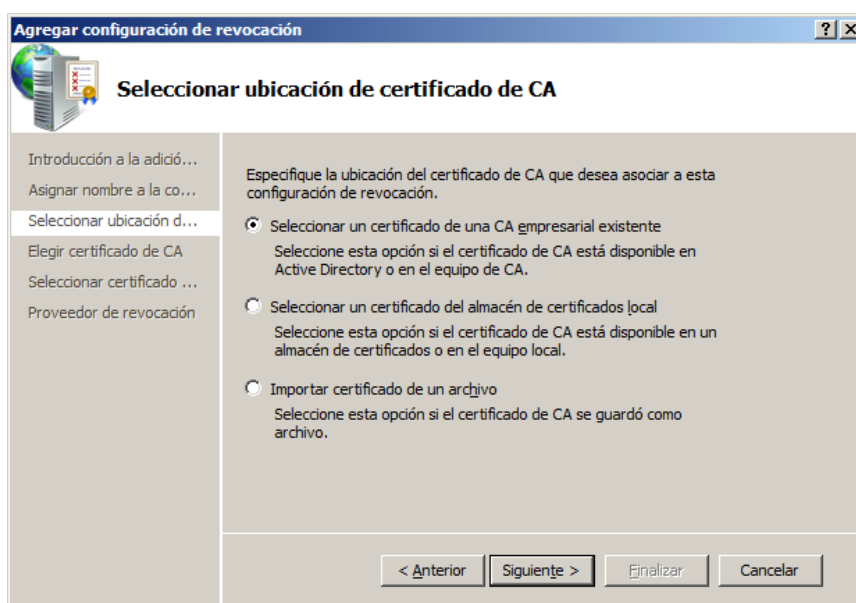
4.2.2.4 Configuración de Revocación

Clic en **Inicio** -> **Herramientas administrativas** -> **Administrador del respondedor Online**, seleccionamos **Configuración de revocación** y en el menú **Acción**, clic en **Agregar configuración de revocación**, clic en **Siguiente**.

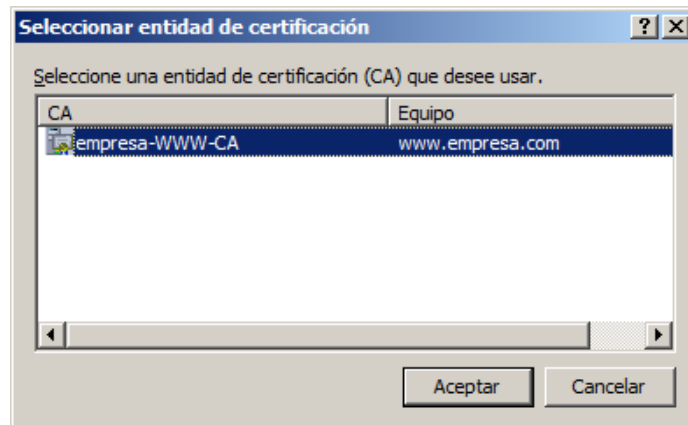
En **Nombre** ingresamos el nombre para nuestra configuración de revocación, en nuestro caso se puso **Revocación**, clic en **Siguiente**.



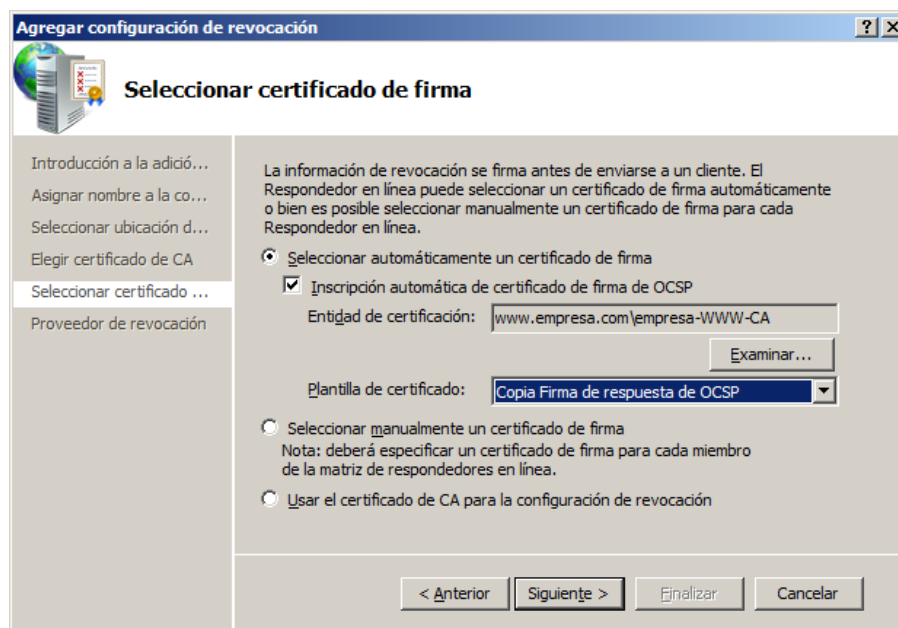
En **Seleccionar ubicación de certificado de CA**, escogemos la opción **Seleccionar un certificado de una CA empresarial existente**, clic en **Siguiente**.



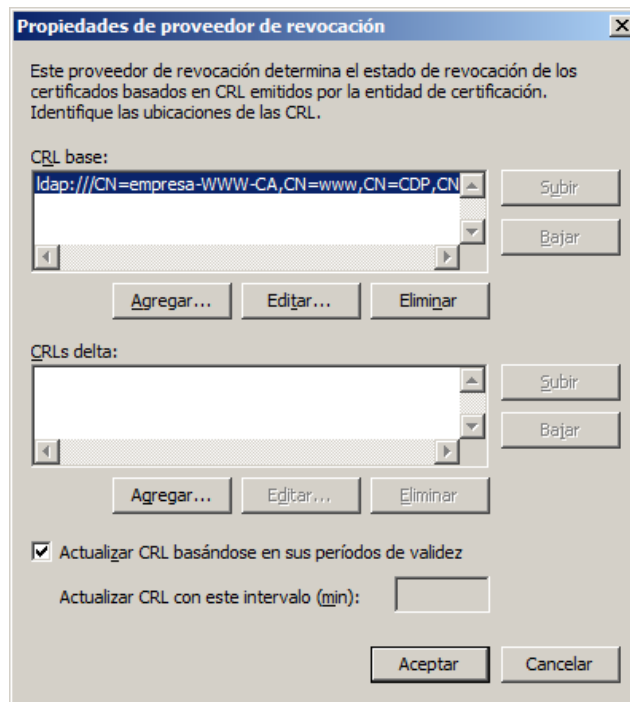
En **Elegir certificado de CA**, escogemos **Buscar certificados de CA publicados en Active Directory** y clic en **Examinar**, en la lista deberá aparecer la autoridad de certificación de la empresa, la seleccionamos y clic en **Aceptar**, luego de esto se mostrara como un link la autoridad de certificación con el cual se comprueba que se seleccionó la CA de la empresa, clic en **siguiente**.



En **seleccionar certificado de firma** escogemos la opción **Seleccionar automáticamente un certificado de firma** y seleccionamos la casilla **Inscripción automática de certificados de firma OCSP**, clic en **Examinar**, seleccionamos la autoridad de certificación que emite certificados de firma de OCSP y clic en **Aceptar**; nos aseguramos que en plantilla de certificado, aparezca seleccionada la plantilla de firma que se creó anteriormente, clic en **Siguiente**.



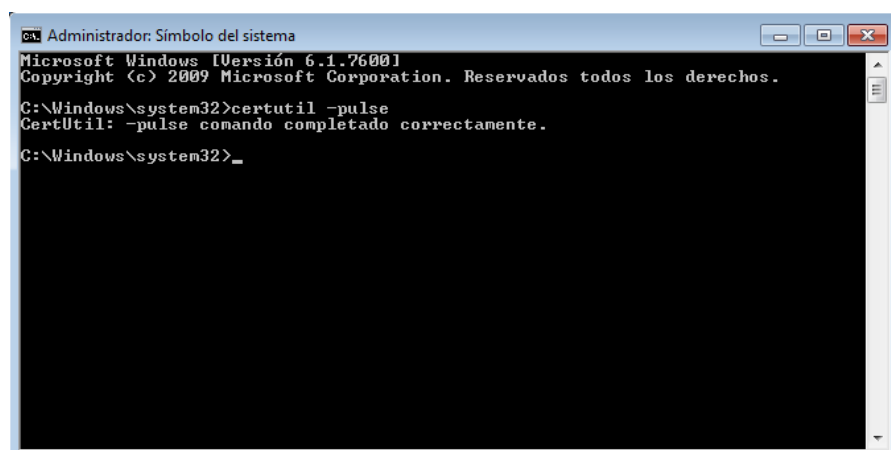
En **Proveedor de Revocación**, damos clic en **Proveedor** y comprobamos que todos los lugares en la CRL base sean válidos, clic en **Aceptar** y clic en **Finalizar**.



4.2.2.5 Verificación de la configuración

Nos loguemos en el equipo cliente, y abrimos símbolo del sistema ejecutándolo como administrador, y ejecutamos el siguiente comando:

```
>certutil -pulse
```



En el equipo cliente, abrimos Administrar certificados de cifrado de archivos, clic en siguiente.

Seleccionamos la opción **crear un nuevo certificado**, clic en **siguiente**.

Seleccionamos la opción **Un certificado emitido por la entidad de certificación de dominio (servidor)**, clic en siguiente.

Luego se presenta la opción de hacer una copia de seguridad del certificado y de la clave, escogemos la opción que más nos convenga, clic en **siguiente**.

Seleccionamos la unidad o carpeta, que vamos a asociar con el certificado, clic en **siguiente**.

Si deseamos revocar el certificado, podemos seleccionar el certificado que ahora se encontrará en el servidor, en la consola de la CA (**Entidad de certificación**), clic derecho en el certificado, seleccionamos **Todas las tareas** y clic en **revocar certificado**, aquí ingresamos el motivo por el que se revocará y clic en sí. Para comprobar la revocación, este se encontrará en el directorio **Certificados revocados**.

Abrimos la entidad de certificación, y en el directorio, se encontrarán los certificados emitidos por el servidor y creados por los clientes.

4.2.3 Aplicación de BitLocker

Para utilizar BitLocker, se ejecutarán comandos de la consola (MSDOS) de Windows 7 del equipo cliente.

BitLocker puede ser manejado a través de varios comandos para que realice tareas específicas, como bloquear, desbloquear, activar la encriptación bitlocker y desactivarlo entre otras, así mismo estos comandos poseen parámetros para especificar la forma en la que va a encriptar o desencriptar la unidad de datos.

4.2.3.1 Comandos BitLocker

Básicamente los comandos que se utilizarán son 4, que servirán primeramente para activar la encriptación BitLocker, una vez hecho estos, el siguiente comando permitirá bloquear la unidad, eliminando el acceso a los datos, el siguiente debe desbloquear la unidad permitiendo acceder a los datos nuevamente, y por último un comando que desactive y elimine por completo la encriptación si el caso lo requiera.

4.2.3.2 Funcionamiento de comandos

Para gestionar las tareas de encriptación BitLocker maneja el comando:

>manage-bde

Para activar la encriptación de una unidad, se utiliza el comando:

>manage-bde -on E: -pw

Donde `-on` es el parámetro que le indica a BitLocker que debe activar la encriptación, mas no bloquearla, el siguiente parámetro especifica la unidad en la que se va a aplicar la encriptación, en este caso una partición de disco denominada E:, y el tercero, `-pw`, especifica el método de bloqueo, en este caso con contraseña.

Una vez ingresado este comando, BitLocker pide una contraseña y la repetición de la misma, ya que se especificó que el bloqueo sea mediante contraseña.

Después de estos BitLocker procederá a encriptar la unidad, partición de disco en este caso, esto puede tardar varios minutos, dependiendo de las capacidades del equipo.

Una vez activada la encriptación, la unidad no se bloquea, para esto se requiere el siguiente comando:

>manage-bde -lock E:

El parámetro `-lock` lo que hará será simplemente bloquear la unidad especificada (E:), impidiendo el acceso a los datos.

Para desbloquear la unidad es necesario el comando:

>manage-bde -unlock E: -pw

El parámetro `-unlock` indica que se desbloquee la unidad especificada (E:), el siguiente parámetro `-pw`, indica el método de desbloqueo, como la activación de BitLocker se lo hizo mediante contraseña, así también se deberá desbloquear.

Una vez ingresado esto, BitLocker solicitará la contraseña de desbloqueo, y una vez ingresada se podrá acceder a la información de la unidad; pero esto es temporal ya

que no elimina la encriptación, sino que permite acceder a la información hasta que se vuelva a activar el bloqueo indicado anteriormente.

Si se desea eliminar por completo la encriptación se utiliza el comando:

>manage-bde –off E:

El parámetro –off indica que se elimine la encriptación de la unidad especificada (E:). Para esto se requiere que la unidad este desbloqueada, mediante el parámetro –unlock como se indicó anteriormente.

El problema que surge al ejecutar esto es que la seguridad añadida de tipo contraseña, permanece almacenada por BitLocker, así que al activar nuevamente bitlocker, este no pide una contraseña, sino que se mantiene la anterior. Para solucionar esto se puede utilizar el parámetro –protectors, el cual permite gestionar la seguridad que hayamos añadido, utilizándolo conjuntamente con el parámetro –delete podemos eliminar las seguridades, y así poder crear una nueva contraseña para la unidad con el comando correspondiente. El comando quedaría de esta forma, indicando la unidad en la que se aplicarán los cambios.

>manage-bde -protectors –delete E:

De la misma forma, si se quisiera añadir una contraseña se especificaría:

>manage-bde -protectors -add E: -pw

Donde –protectors permite manejar las seguridades, el parámetro -add indica que se anade una seguridad a la unidad especificada (E:), y –pw indica que la seguridad es de tipo contraseña.

4.2.4 Funcionamiento aplicación Visual Basic .NET

La aplicación presenta en primera instancia un cuadro de diálogo en donde se le pide al usuario que ingrese los parámetros para acceder al dominio, una vez validado esto le permitirá acceder a la parte de ciframiento, donde podrá activar o desactivar BitLocker para el posterior ciframiento de las unidades de datos. Todo este proceso se lo detalla en el anexo 1 de este documento.

4.3 Ventajas

- Si se utiliza el sistema en el equipo que ocupa un directivo, se elimina la necesidad de implantar políticas que impidan la salida de estos equipos.
- Protege la información crítica de la empresa, en el caso de que el equipo sea sustraído.
- Verificación de los usuarios registrados en Active Directory que se encuentra en el servidor para acceder a la información.
- Autenticación de los usuarios mediante la utilización de certificados digitales emitidos por la Entidad Certificadora de Active Directory.
- Seguridad de la información mediante la utilización de la herramienta Bitlocker del sistema para que sea “basura” ante personas desconocidas o extrañas que pretendan manipular dicha información.
- Mantener segura la información confidencial de las empresas utilizando nuestra herramienta mediante métodos de encriptación de la información.

CAPÍTULO 5. ANÁLISIS ECONÓMICO PARA LA IMPLEMENTACIÓN

Montar esta infraestructura depende necesariamente de las versiones de sistemas operativos indicadas anteriormente, ya que otras versiones no proporcionarían las funcionalidades requeridas para el funcionamiento y control del sistema.

Para el desarrollo de la aplicación se utilizaron versiones de prueba descargadas directamente del sitio web de Microsoft, pero para aplicarlo a una empresa, se requerirá adquirir licencias del producto:

Costos		
Producto	Precio	Detalles
Windows Server 2008 R2 Enterprise	\$ 3.919,00	Incluye 25 licencias de acceso de cliente
Windows 7 Enterprise	\$ 320,00	Incluye versiones de 32 y 64 bits El uso de BitLocker
Visual Studio 2010 Professional	\$ 500,00	
Total	\$ 4.739,00	

Fuente: (Microsoft Store)

Alternativas como CryptoForge o BestCrypt pueden requerir la implementación de herramientas adicionales para controlarlos mediante Active Directory y certificados digitales.

TrueCrypt, CryptoStudio o AESCrypt pueden resultar satisfactorias si es que se busca una alternativa más económica, ya que son de licencia gratuita, como se había visto antes, al utilizar esto se depende bastante de las actualizaciones que se publiquen en su sitio, y no se puede recurrir a un soporte técnico como cuando se adquiere licencias como es el caso de BitLocker incluido en Windows Server 2008.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- El Directorio Activo permite gestionar una amplia gama de aspectos, posee varias herramientas como gestión de usuarios mediante certificados, y controlar como se ejecutan las aplicaciones, esto realmente facilita la interoperabilidad entre estas herramientas.
- El cifrado de BitLocker no funciona para la encriptación de directorios o carpetas, únicamente se limita a unidades fijas como particiones de disco, y también para unidades extraíbles.
- El Directorio Activo permite crear unidades organizativas a las cuales se los puede añadir usuarios, equipos o recursos que necesiten estar dentro de las mismas.
- Crear Directivas de Grupo (GPO) facilita al Administrador a crear seguridades tanto para la empresa como para los usuarios que mantengan acceso al dominio, a su vez los usuarios mantendrán restricciones que su Administrador dispuso correctas hacerlas.
- Es impresionante ver el trabajo que ahorra Directorio Activo ya que cuando la pequeña empresa a la que se la implemento el servicio va creciendo en número de usuarios, equipos y recursos, sus problemas también crecerían como por ejemplo sus carpetas compartidas en desorden, pérdidas del control de acceso de usuarios, permisos a equipos que se conectan a la red, etc.; esto se facilita con el servicio de AD porque permite recolectar y organizar la información de los usuarios y recursos de la red.
- La administración de Active Directory puede realizarse desde cualquier servidor de dominio de toda la red.
- Cuando queremos aplicar una nueva GPO se debe revisar que el usuario no este registrado en ningún otro grupo ya que las políticas solo aplican a los usuarios que estén libres.

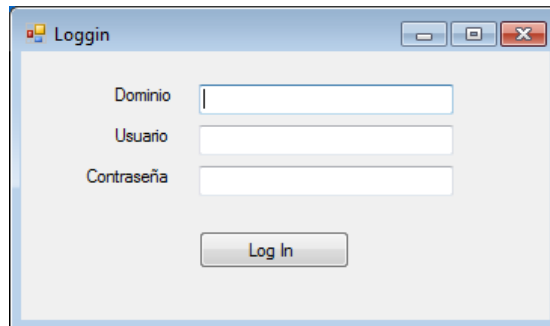
Recomendaciones

- Para aumentar la seguridad serviría de mucha ayuda que el equipo cliente maneje un módulo TPM compatible, ya que como se analizó en la sección 2.5.2, esto brinda una seguridad extra a las contraseñas de encriptación.
- Con respecto a las licencias de software, la seguridad es muy delicada y crítica, y utilizar un software no licenciado conlleva a depender de las actualizaciones que estos publiquen, o arriesgarse a la discontinuación de estos.
- Utilizar alternativas de software libre disminuirá el presupuesto necesario para la implementación, pero poner en marcha estas herramientas en conjunción con el Directorio Activo puede requerir de componentes adicionales, que pueden necesitar otros estudios.
- Antes de implementar una nueva regla para una unidad organizativa se la debe hacer en un entorno separado y controlado antes de realizar el ajuste en los usuarios.
- Para realizar algún cambio y probar que este funcione bien se recomienda hacer en un entorno de máquinas virtuales.
- Controlar que el servidor se administre solo desde el servidor y no desde un escritorio remoto para evitar vulnerabilidades en el sistema.
- Es una buena práctica, el renombrar la cuenta Administrador y deshabilitar la cuenta invitado, tanto en el servidor como en los equipos clientes.
- Revisar cada cierto tiempo las alertas de inicios de sesión fallidos ya que pueda que algún intruso esté intentando ingresar a nuestro sistema y ocasionar algún daño.

ANEXOS.

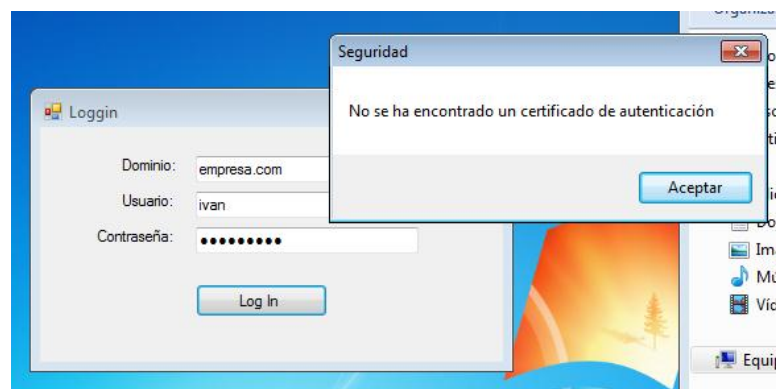
Anexo 1. Manual de Usuario

La aplicación presenta esta pantalla de inicio:



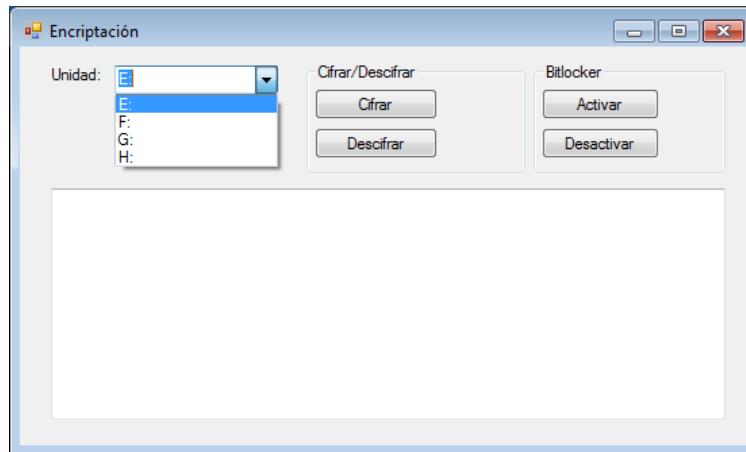
The screenshot shows a window titled 'Loggin' with three text input fields labeled 'Dominio', 'Usuario', and 'Contraseña'. Below the fields is a 'Log In' button. The window has standard Windows-style window controls (minimize, maximize, close) in the top right corner.

En donde el usuario debe ingresar el nombre del **dominio**, por ejemplo empresa.com, después en el cuadro de dialogo de **usuario** debe ingresar el nombre de usuario que está registrado en el dominio, y finalmente la **contraseña** de acceso, que puede ser personal o proporcionada por el administrador del Directorio Activo, luego de esto presiona el botón **Log In**.



Una vez presionado, el sistema realiza dos comprobaciones, la primera comprueba que el usuario exista en el dominio y la segunda que el usuario posea un certificado emitido, en este caso, por la CA del servidor de dominio, si encuentra algún problema con estos factores no se puede continuar.

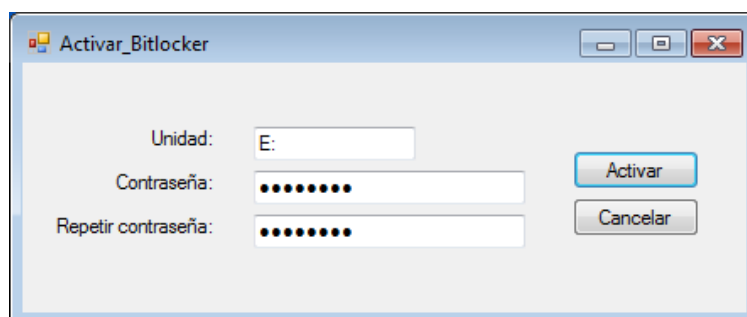
Si los datos son correctos se muestra el cuadro de diálogo para la encriptación de datos:



En unidad se presenta una lista desplegable en donde aparecen las unidades de disco del sistema operativo. A esto le sigue una sección llamada Cifrar/Descifrar y BitLocker.

- La primera sección sirve para bloquear y desbloquear la unidad para acceder a los datos, esto funciona únicamente si la unidad seleccionada ya ha sido cifrada.
- La segunda sección sirve para activar la encriptación de BitLocker, para desactivarla se requiere que la unidad haya sido descifrada antes.

Por ejemplo se ha elegido la unidad E:, luego presionamos el botón para **activar** bitlocker, esto abrirá un cuadro de diálogo donde el usuario deberá ingresar una contraseña para encriptar los datos:



El sistema validará que la contraseña cumpla con la longitud mínima establecida de 8 caracteres, y activará BitLocker en la unidad, esto puede tardar un tiempo muy variable, ya que depende de las capacidades del equipo, y de la cantidad de datos que se van a encriptar.

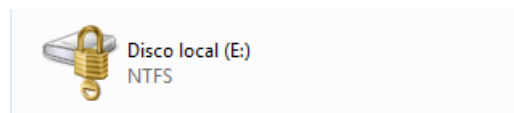
Una vez realizada la encriptación la unidad cambiará de icono, para indicar que ya está activado BitLocker, así:



Entonces ahora se puede **cifrar** la unidad:

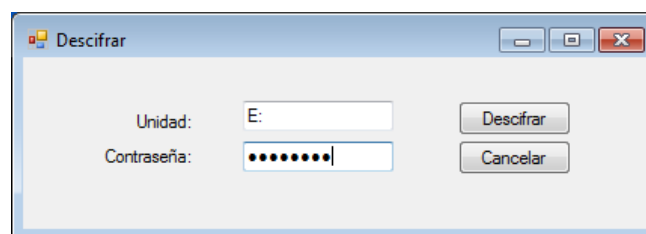


Y se mostrará de la siguiente manera:

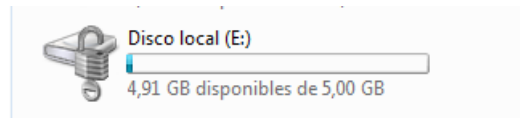


De esta manera ya no se puede acceder a los datos.

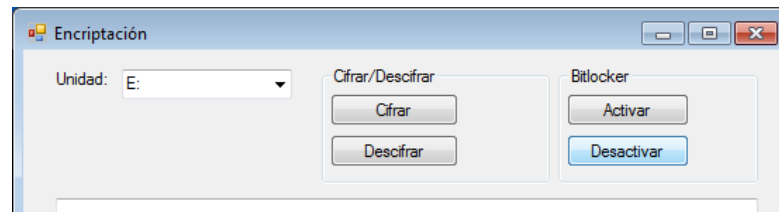
Para volver a acceder, se selecciona la opción **Descifrar**. Entonces se mostrará un cuadro de diálogo que le pedirá al usuario ingresar la contraseña de encriptación:



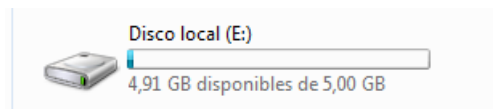
Una vez ingresada la contraseña correcta, se descifrarán los datos, permitiendo acceder a ellos:



Si se desea eliminar por completo el ciframiento de BitLocker se selecciona el botón **Desactivar**.



De esta manera no se podrá bloquear la unidad, el icono vuelve al estado inicial:



Anexo 2. Código fuente

Función utilizada para comprobar que el usuario existe en el dominio.

```
Public Function IsAuthenticated(ByVal Domain As String, ByVal username As
String, ByVal pwd As String) As Boolean
    Dim Success As Boolean = False
    Dim Entry As New System.DirectoryServices.DirectoryEntry("LDAP://" &
Domain, username, pwd)
    Dim Searcher As New System.DirectoryServices.DirectorySearcher(Entry)
    Searcher.SearchScope = DirectoryServices.SearchScope.OneLevel
    Try
        Dim Results As System.DirectoryServices.SearchResult =
Searcher.FindOne
        Success = Not (Results Is Nothing)
    Catch
        Success = False
    End Try

    If Success = False Then
        MessageBox.Show("Usuario incorrecto")
        Return False
    Else
        MessageBox.Show("Usuario correcto")
        Return True
    End If

End Function
```

Función para verificar que el certificado fue emitido por la CA del dominio.

```
Public Function VerificarCertificado() As Boolean

    Dim certificado As Boolean = False
    objstore = (New X509Store(StoreName.Root, StoreLocation.LocalMachine))
    objstore.Open(OpenFlags.ReadOnly)

    For Each Me.objcert In objstore.Certificates
        If objcert.Issuer = "CN=empresa-WWW-CA, DC=empresa, DC=com" Then
            Return True
        End If
    Next
    Return False
End Function
```

Función para cifrar, en realidad ejecuta comandos de BitLocker en el Shell de Windows para llamar a las funciones de encriptación y desencriptación, básicamente esta es la manera en la que se ejecutan las funcionalidades del sistema entero.

```
Public Sub cifrar(ByVal unidad As String)
    Dim comando As String

    comando = "manage-bde -lock " & unidad

    Dim strArgumentos As String = "-lock " & unidad
    Dim strExe As String = "manage-bde"

    Dim startInfo As ProcessStartInfo = New ProcessStartInfo(strExe,
strArgumentos)

    startInfo.UseShellExecute = False

    startInfo.ErrorDialog = False

    startInfo.CreateNoWindow = True

    startInfo.RedirectStandardOutput = True

    Try
        Dim p As Diagnostics.Process =
System.Diagnostics.Process.Start(startInfo)

        Dim sr As System.IO.StreamReader = p.StandardOutput
        Dim cadenaSalida As String = sr.ReadToEnd()
        sr.Close()

        txtLog.Text = cadenaSalida
    Catch ex As Exception
        txtLog.Text = (ex.Message)
    End Try
End Sub
```

BIBLIOGRAFÍA

- Aprea, Jean-Françoise. Active Directory con Windows Server 2003. España: Ediciones ENI, 2005.
- Areitio Bertolín, Javier. Seguridad de la Información. Madrid: Paraninfo, 2008.
- González Gallego, Rafael Enrique. Diccionario de Computación y Electrónica. México D.F., 2004.
- Muñoz Muñoz, Ramiro. «Un proyecto español de firma electrónica.» Firma Digital y Administraciones Públicas. Madrid: Instituto Nacional de Administración Pública, 2003. 146.

FUENTES DE INTERNET

Características Cryptoforge

cryptoforge.com. www.CryptoForge.com. 2012. Mayo de 2012. <<http://www.cryptoforge.com.ar>>.

Características CryptoStudio

CryptoStudio. Crypto Studio. 2005. Mayo de 2012. <<http://cryptostudio.sourceforge.net/index.html>>.

Características BestCrypt

Jetio. Jetico. 2012. 15 de Mayo de 2012. <<http://www.jetico.com/encryption-bestcrypt-volume-encryption/>>.

Información sobre BitLocker

Microsoft. Biblioteca Technet. 2012. Mayo de 2012. <<http://technet.microsoft.com/es-es/library/dd835565%28v=ws.10%29.aspx>>.

Información sobre licencias Microsoft

Microsoft Store. Microsoft Store. 2012. Mayo de 2012. <http://www.microsoftstore.com/store/msstore/en_US/pd/productID.216652500>.

Cifrado de BitLocker

MSDN. MSDN. 2012. Mayo de 2012. <http://msdn.microsoft.com/es-es/library/cc766200%28v=ws.10%29.aspx#BKMK_Form>.

Información Active Directory

Rodríguez, Daniel Omar. Seguridad Informática. Enero de 2008. Mayo de 2012. <<http://danielomarrodriguez.blogspot.com/2008/01/active-directory.html>>.

Encriptación

Tepper, Patrick Mac Kay. MSDN. 2012. Mayo de 2012. <<http://msdn.microsoft.com/es-es/library/bb972216.aspx#XSLTsection128121120120>>.

Encriptación (ilustraciones)

TextosCientificos. TextosCientificos.com. Noviembre de 2006. Mayo de 2012. <<http://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion>>.

Características TrueCrypt

TrueCrypt. True Crypt. 2012. Mayo de 2012. <<http://www.truecrypt.org/>>.

Active Directory Technet

Technet. Technet. Abril de 2007. Mayo 2012. <<http://social.technet.microsoft.com/wiki/contents/articles/active-directory-domain-services-ad-ds-overview.aspx>>