UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DLP (DATA LOSS PREVENTION)

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERÍA EN COMPUTACIÓN

P R E S E N T A:

Alan Daniel Godínez Chávez
Iván Olvera Espinoza

DIRECTOR DE TESIS:
Ing. Cruz Sergio Aguilar Díaz

Ciudad Universitaria, Cd. Mx., febrero 2017

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

CONTENIDO

AGRADECIMIENTOS

Alan Daniel Godínez Chávez.

Agradecimientos a todos mis profesores, a la facultad y mis amigos que me ayudaron y enseñaron por todo el tiempo que estuvimos estudiando, Gregorio, Abraham, Iván, Oscar, Gabriel, Alex.

Iván Olvera Espinoza.

Primeramente, agradezco a la Facultad de Ingeniería por darme la oportunidad de realizar mi formación académica y profesional, así como también a cada uno de los profesores y amigos que me brindaron sus conocimientos para realizar mi formación. Agradezco también nuestro asesor de tesis el Ing. Cruz Sergio Aguilar Díaz por habernos brindado la oportunidad, tiempo y paciencia para llevar a cabo esta tesis.

DEDICATORIAS:

Alan Daniel Godínez Chávez.

A mi madre Marisela, a mi abuela Teresa, a mi esposa Vanessa, a mi hermana Lisly, a mi Hermano Iván y a todos mis amigos quienes siempre de alguna manera me ayudaron y apoyaron.

"Stay Hungry. Stay Foolish"
Steve Jobs.

Iván Olvera Espinoza.

Dedico este trabajo a los mis padres y hermanos por todo el apoyo incondicional que me brindaron para poder llegar a ser un profesional, a mi hijo Leonardo que posiblemente en estos momentos no entienda mis palabras, pero cuando sea capaz, quiero que sepas lo mucho que significas para mí, te amo.

"La confianza en uno mismo es el primer peldaño para ascender por la escalera del éxito."
Ralph Waldo Emerson

INTRODUCCIÓN

En el capítulo 1 se describe de forma general la problemática que se tiene en la actualidad sobre el robo de información, así como el por qué es importante cuidarla como uno de los activos más importantes de la compañía.

En el capítulo 2 se identificarán los requerimientos de la solución propuesta, así como sus especificaciones, se describirá para qué es necesario una herramienta DLP y su importancia dentro de las compañías pequeñas, medianas o grandes. En este capítulo se describen los objetivos que tiene el presente trabajo; se darán a conocer los alcances y limitaciones que tiene esta investigación.

En el capítulo 3 se formalizarán conceptos que ayudarán a familiarizarse con el trabajo, se tocará base con temas de redes, sistemas operativos y seguridad informática, en este capítulo se relacionará cómo una solución de DLP se integra con todos estos conceptos y áreas para lograr cumplir su objetivo, que es mantener la información a salvo. Se definirán los posibles medios por los cuales se puede robar información en medios físicos y hasta en la nube.

En el capítulo 4 se mostrará el diseño lógico para la implementación de una solución de DLP, enfocado a una empresa mediana; se hablará sobre el por qué se eligió el hardware y software que integran nuestra solución, en comparativa con las demás del mercado. Finalizando el capítulo con el alcance de la herramienta para la investigación.

En el capítulo 5 se describe el proceso de implementación de la solución, así como del proceso de configuración orientado al resguardo de la información para empresas medianas, se mostrará el resultado de las pruebas realizadas con la configuración elegida y las políticas que se pueden utilizar.

En el capítulo 6 se mostrará de manera formal la documentación y resultados obtenidos con esta investigación; se aportará un manual de usuario para aquellos que estén interesados en involucrarse con la solución y puedan realizar una configuración básica de un DLP; también se documentará un manual de operación que mostrará como ejemplo, el funcionamiento de la solución de forma productiva para una empresa.

Por último, se darán a conocer las conclusiones a las que se llegaron una vez finalizada la investigación y se ofrecerán recomendaciones para los futuros trabajos dónde el presente pueda fungir como base para su desarrollo.

Capítulo 1 ANTECEDENTES

1.1 Panorama General.

En la actualidad el mundo ha cambiado comparado con los inicios del Internet. Hace un tiempo sustraer un activo de una organización implicaba llevárselo materialmente; algunos se llevaban material de oficina, otros documentos confidenciales originales o fotocopiados. En la actualidad, los datos y la información que manejan las empresas son de los activos más valiosos y no es necesario esconderlos en el saco para robarlos. Hoy en día la información se puede enviar por correo electrónico, mensajería instantánea, subir a una página de Internet, imprimir o copiar en un dispositivo de almacenamiento masivo y de diferentes maneras inventadas o por inventar.

Actualmente conocer e implementar una buena solución de software de seguridad que pueda proteger los activos de una empresa es de vital importancia, hoy en día quién tiene acceso a la información tiene el poder. En particular, las violaciones de datos podrían no ocurrir si una empresa es consciente de su flujo de información y cuentan con la solución adecuada para protegerlo. Este trabajo de tesis explica por qué y cómo la adquisición de una solución de *Data Lost Prevention* (DLP) ayudará a una empresa a reducir la pérdida de datos, mitigar el impacto de pérdidas y ahorra dinero.

Una organización tiene el reto de mantener una reputación de fiabilidad y entorno seguro; accionistas y clientes confían en la habilidad que tiene una compañía para proteger los datos de negocio. Contar con un nivel alto de gestión debe asegurar que la empresa cumpla con sus metas y objetivos, de esta manera es necesario implementar software de seguridad con el fin de minimizar los riesgos, protegerse contra las violaciones de datos, y prevenir otros eventos que afectan la salud financiera, relaciones públicas, y la reputación de una compañía.

Los datos sensibles se están moviendo en la nube, pero muchas organizaciones carecen de controles de políticas para los datos almacenados en servicios de este tipo. Toda organización actual hace uso de estos servicios, y los empleados suelen introducir nuevos mecanismos sin el conocimiento o consentimiento del departamento de TI. Analizando los datos de uso en almacenamientos virtuales para 17 millones de usuarios; se ha encontrado que una pequeña cantidad de los documentos cargados para presentar servicios de intercambio contienen información confidencial, como información de identificación personal (PII), la información de salud protegida (PHI) o datos de tarjetas de pago.

Muchas organizaciones han invertido en herramientas de prevención de pérdida de datos para proteger su información dentro de las instalaciones, y cumplir con las leyes de privacidad de datos y cumplimiento.

Sin embargo, la mayoría de estas soluciones están diseñadas para proteger los datos en servidores de archivos o correo electrónico, y por lo tanto no se ocupan de otros factores como la nube y almacenamiento móvil. Es por ello que los administradores de TI están buscando cada vez más extender sus políticas de prevención de pérdida de datos. Ahora las compañías deben estar en busca de una solución que les permita proporcionar la capacidad de realizar un análisis bajo demanda de todos los datos almacenados en ellas.

En esta época de proliferación de información y de medios para compartirla, se requiere un cambio en la cultura de la protección de datos, tanto corporativos como personales. Hay mucha información sensible, y ya no está encerrada en manos de unos pocos individuos; además de los centros de datos y redes corporativas, la información se genera y reside ya no solo en servidores y computadoras de escritorio, sino en computadoras portátiles, teléfonos inteligentes, tabletas y servicios en nube como se ha mencionado, entre otros. Esa información debe ser asegurada. Esto, aunado a las crecientes amenazas de delincuentes, desde el exterior y en el interior de las corporaciones, convierte las estrategias de protección de información y las de prevención de pérdida de datos en fundamentales para asegurarse de que los usuarios no envían o sacan información sensible o crítica fuera de la red corporativa.

La prevención de pérdida de datos (DLP) es una estrategia para asegurarse de que los usuarios finales o alguna persona no autorizada, no envíen información sensible o crítica fuera de la red corporativa. Así una solución DLP también llamada prevención de fuga de datos, prevención de pérdida de información o prevención de extrusiones, está siendo impulsada por las amenazas internas, muchas de las cuales tienen estrictos componentes de protección de datos o de acceso.

Las soluciones DLP utilizan reglas de negocio para examinar el contenido de los archivos y etiquetar la información confidencial y crítica, para que los usuarios no puedan divulgarla. Una solución puede ser útil para identificar y etiquetar contenido bien definido (como los números de Seguro Social o de tarjetas de crédito por mencionar algunas), pero tiende a quedarse corto cuando un administrador está tratando de identificar otros datos sensibles, tales como los de propiedad intelectual.

“Hoy en día los servicios de respaldo en línea o en la nube son vistos como una forma rápida y fácil de realizar copias de seguridad de archivos personales y cada vez más empleados están utilizando estos servicios para realizar respaldos de sus datos personales o empresariales que están en los equipos de trabajo. Los servicios de respaldo de cómputo en línea como Carbonite, Mozy y Dropbox, google drive, están de moda en estos días. Estos servicios son atractivos porque resuelven los problemas de tener copias de seguridad dentro de las instalaciones corporativas, o simplemente no contar con los recursos necesarios para gestionar las copias de seguridad. Se puede pensar que estos servicios de respaldo en

línea no afectan a su negocio; pero podría no saber que los usuarios están ejecutando estos programas en sus computadoras de trabajo para respaldar sus "sistemas", incluyendo datos personales y de negocios. Y hasta que sepa con certeza que estos programas no se están utilizando en su entorno, existen numerosos riesgos de seguridad.

Los servicios de respaldo de datos en línea en sí no son el problema. Es el simple hecho de que están siendo utilizados en su red sin el consentimiento de nadie. A menudo el área de TI está al margen. Lo mismo ocurre con auditoría interna. Incluso he hablado con administradores de respaldo que han dicho que no tenían idea que sus usuarios estaban realizando copias de seguridad en su nombre. Tal vez lo peor de todo es que la gerencia suele estar ajena a los riesgos de negocio que incluyen el mal manejo de datos confidenciales de los clientes, la exposición de la propiedad intelectual, y muy posiblemente violaciones de contrato y cumplimiento"[1].

Es por esto que hemos mencionado que una solución de prevención de fuga de información es vital para una compañía hoy en día y el hecho de tener una solución de DLP no es garantía del 100% de protección de datos.

1.2 Importancia de la información.

"Desde que Francis Bacon (primer barón Verulam, vizconde de St Albans, canciller de Inglaterra y célebre filósofo) acuño la expresión "la información es poder" han pasado muchos años y hasta en este tiempo es cuando esta frase parece haber cobrado mayor sentido. La información se ha convertido en el activo más importante que posee cualquier organización, es moneda de cambio e instrumento de fuerza y presión, otorga ventaja a quien la posee, y hay toda una industria en torno a la gestión, tratamiento y por supuesto, protección de la información.

En el año 2010 se produjo, la que está considerada hasta la fecha, como la mayor filtración de información de la historia. Wikileaks publicó un total de 250.000 (cables) comunicaciones que se habían realizado entre el Departamento de Estado Estadounidense y sus embajadas repartidas por todo el mundo.

Este incidente supuso la confirmación de algo que ya se sabía; la gran dificultad de mantener la confidencialidad de la información, evitando filtraciones, pero también puso de manifiesto que ninguna organización está a salvo, incluidas aquellas que pertenecen al ámbito gubernamental o dedicadas a alguna de las múltiples ramas o ámbitos de la seguridad, que lógicamente se suponen preparadas, ya que disponen de procedimientos, herramientas y personal entrenado para manejar información considerada sensible y confidencial. Pero la seguridad 100% no existe y en última instancia, la información es manipulada por personas, y como es sabido el usuario es el eslabón más débil de la cadena.

Wikileaks es un ejemplo perfecto de cómo una fuga de información puede tener consecuencias imprevisibles y un enorme impacto mediático, tal y como ocurrió en este caso, debido a la naturaleza de la información filtrada y el ámbito al que pertenecía. El daño fue tremendo, y puso en jaque al gobierno americano que tuvo que realizar importantes esfuerzos para minimizar el impacto y las consecuencias.

Aunque el incidente de Wikileaks estableció un antes y un después, el problema de la fuga de información existe desde que los humanos manejan información. La fuga de información tiene una componente social y humana muy importante. Detrás de una buena parte de los incidentes de fuga de información se esconden motivaciones personales, o simples errores, entre otras.

La masificación del uso de las tecnologías y su integración en todos los ámbitos y estamentos de la sociedad han creado un escenario en el que, por un lado, cada vez se gestiona mayor cantidad de información y por otro, se ha convertido en un activo crítico de las organizaciones y los usuarios. Además, las tecnologías posibilitan un tratamiento de la información sin precedentes y a nivel global, de manera que es transmitida, procesada, copiada o almacenada con una rapidez y eficacia impensable hace algunos años, sumado al hecho de que es posible llevar a cabo dichas acciones, desde múltiples tipos de dispositivos, en cualquier lugar y en cualquier momento."[2]

Al crear conciencia sobre lo importante que es mantener la información dentro de la organización o compañía y cómo proteger los activos de una empresa incluidos los datos sensibles, se debe elegir el software de seguridad adecuado y la selección de una herramienta de seguridad como el software DLP, una empresa puede ayudar a prevenir violaciones de seguridad de información, Información de Identificación Personal (PII), la Propiedad Intelectual, y otros datos valiosos.
El uso y aplicación del software adecuado con el negocio adecuado puede reducir la pérdida de datos y ahorrar dinero.
Una solución de DLP, puede obtener beneficios tales como:

- Incrementar la confianza de los accionistas y clientes al proporcionar la capacidad de proteger la información de activos de la empresa.
- Mantener herramientas eficaces y eficientes para la protección contra las violaciones de datos.
- Identificar y analizar fácilmente problemas.
- Evitar el mal uso de los datos.
- Adquirir protección de información de identificación personal.
- Disminuir el costo de la pérdida de activos de la empresa.

Para esto en la actualidad se puede contar con una solución DLP que tiene como objetivo identificar, monitorizar y proteger los datos de una organización. Los datos pueden ser tratados por usuarios en sus estaciones de trabajo, pueden transmitirse o pueden ser almacenados. Esto es posible mediante agentes que controlan especialmente el acceso a datos, su copia en soportes móviles como dispositivos USB y su impresión en papel. “Por ejemplo, un software DLP podría bloquear la impresión de un documento si en él aparece información sensible; esto es logrado por un software que inspecciona los paquetes en la red en busca de patrones y determina si la comunicación está autorizada o no. Algunos protocolos de comunicación soportados son SMTP, HTTP, HTTPS, FTP y Telnet.
Por ejemplo, si un trabajador malintencionado trata de conectarse a su correo corporativo y enviarse a una cuenta externa (Hotmail, Gmail, etc.) documentación confidencial, de manera no autorizada, el software DLP podría bloquear la transmisión, loguearla y generar una alarma o encriptar el archivo para que no pudiera leerse fuera de la organización. Estos son ejemplos de lo que ésta solución puede lograr.” [3]

1.3. Propósito del proyecto.

El propósito de este proyecto de Tesis es hacer hincapié en la manera de reducir la pérdida de datos y ahorrar dinero mediante la adquisición de DLP.

Esto incluye una explicación para cada tipo de violación de datos como las amenazas internas, corrupción o supresión de datos. Adicionalmente, llevar al tema de cómo reducir las pérdidas y ahorrar dinero mediante la adquisición de DLP.

Otro punto de desarrollo es conocer los componentes que integran una solución de DLP tales como DLP red, DLP almacenamiento y DLP usuario final.
También se fundamentará por qué DLP es diferente de otro software, se dará a conocer procesos de datos que la empresa puede proteger tales como datos en uso, los datos en movimiento y datos en reposo.

Capítulo 2

ESPECIFICACIONES Y REQUERIMIENTOS DEL SISTEMA

2.1 Identificación de los Requerimientos.

Las herramientas de prevención de fuga de datos son muy eficaces para reducir el riesgo de que los datos sensibles terminen donde no deben, sin embargo, hay puntos que se deben cuidar al momento de aplicar una solución de DLP, si no se implementa adecuadamente los resultados podrían no ser positivos. Dichos puntos a cuidar son los siguientes:

Se deben establecer expectativas correctas, un error muy común en las implementaciones de DLP es no comprender de lo que es capaz la tecnología, y cómo integrarla adecuadamente en los procesos de negocio. Existen diferentes herramientas y soluciones de prevención de fuga de información, las cuales tienen diferentes capacidades, especialmente en relación con el análisis de contenido. Es importante saber que ninguna de ellas puede proteger completamente todos los datos de cada amenaza concebible. DLP se trata de la reducción del riesgo, no de la eliminación de amenazas, es importante saber qué tipo de políticas pueden ser definidas, y qué opciones para hacerlas cumplir están disponibles. Se debe contar con el flujo de trabajo adecuado para manejar las violaciones a la política y establecer una buena base de referencia desde el principio; "*saber qué datos necesitan protección, las capacidades de las herramientas instaladas para protegerlos, y el flujo de trabajo para el manejo de incidentes*".

Se deben tener políticas pequeñas y bien definidas; una solución de DLP no es necesariamente propensa a muchos falsos positivos, pero si se construye una mala política la organización será inundada con malos resultados, o pasará por alto importantes pérdidas. Esto es la base de la solución.

La mayoría de las veces, los falsos positivos son positivos reales, pero denotan contenido que no representa ningún riesgo en ese contexto empresarial. Utilizar la técnica de análisis de contenido correcta o añadir contexto a una política puede reducir los falsos positivos, lo que permite un uso más eficaz de las herramientas DLP.

"Las políticas de DLP están estrechamente ligadas a los usuarios, grupos y listas. Es importante asegurarse de que la herramienta de DLP se integra correctamente con la estructura de directorios de la organización, y utiliza la función que existe en la mayoría de las herramientas de DLP para enlazar a los usuarios con sus direcciones de protocolo de configuración para cliente dinámico. Algunas organizaciones

son descuidadas con sus directorios, lo cual puede hacer difícil localizar a un usuario infractor (o aplicar políticas a las personas adecuadas).
Las herramientas de DLP son una poderosa manera de proteger el contenido sensible. Aunque sean eficaces y eficientes, fracasar al evitar los obstáculos arriba mencionados puede distanciar a la empresa y llevar a resultados pobres de DLP."[4]

2.2 Objetivos.

Este trabajo de investigación tiene por objetivo desarrollar una metodología para realizar la implementación de un sistema de fuga de información en las empresas medianas, llevando un método organizado y eficaz.

Objetivos específicos:

- Comparar diversas herramientas propuestas por los fabricantes de DLP aplicados a la protección de fuga de información en las organizaciones.
- Dar a conocer el por qué se eligió la solución DLP en este trabajo.
- Analizar los resultados antes y después de aplicar las soluciones metodológicas de manejo del riesgo de fuga de información en las empresas.
- Evaluar los activos de información sensible que pueden ser protegidos mediante un sistema DLP, teniendo en cuenta los riesgos y la metodología planteada.

2.3 Alcances y Limitaciones.

Es necesario definir qué tipo de información se va trabajar (solo aquella información sensible considerada realmente importante para el negocio). Así es que la información tomada en este proyecto es aquella que tiene un valor específico para la compañía, de tal manera que se facilite la tarea de recolección y unificación al momento de vaciarla sobre un formato o formulario específico, luego proceder a configurarla en la solución que establece una protección de acceso, cifrado, contraseña, u otro control técnico que ayude a la prevención de fuga de información.

Luego de recolectada la información que se considera sensible, es requerido un esfuerzo mínimo para unificar las reglas y concluir el tiempo de configuración, ya que un documento o archivo, puede ser confidencial por un periodo de tiempo específico o determinado, esto podría ocasionar alertas innecesarias, y generar falsos positivos.

De esta manera, se procede a realizar un levantamiento previo de la información de forma adecuada y siguiendo las directrices establecidas por la propuesta metodología que se plantea en este proyecto.

Capítulo 3 FUNDAMENTOS TEÓRICOS

3.1 Antecedentes de redes

Historia y antecedentes de las redes de computación

El primer indicio de redes de comunicación fue telefónico y telegráfico. A finales de la década de 1960 y en los posteriores 70 fueron creadas las minicomputadoras. En 1976 Apple introduce el Apple I uno de las primeras computadoras personales En 1981, IBM introduce su primera PC. A mitad de la década de 1980 las PC comienzan a usar los módems para compartir archivos con otras computadoras, en un rango de velocidades que comenzó en 1200 bps y llegó a los 56 kbps (comunicación punto a punto o dial-up), cuando empezaron a ser sustituidos por sistema de mayor velocidad, especialmente ADSL.

Definición de una red de cómputo

El nombre de red de cómputos es aquel que se utiliza para hacer referencia a un tipo de conectividad que puede existir entre diversas computadoras y que tiene por objetivo el compartir los datos, accesos, dispositivos, y cualquier tipo de información que existen dentro de una computadora a otras que formen parte de la red. De este modo, el acceso a tales datos es más fácil siempre y cuando se trate de computadoras aceptadas por la red, y es también más seguro porque impide que los mismos salgan a espacios externos no aprobados por la red prediseñada.

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo NO comparte sus propios recursos con otras computadoras [5].

3.1.1 Internet

Internet es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP. Tuvo sus orígenes en 1969, cuando una agencia del Departamento de Defensa de los Estados Unidos comenzó a buscar alternativas ante una eventual guerra atómica que pudiera incomunicar a las personas [6]. Tres años más tarde se realizó la primera demostración pública del sistema ideado, gracias a que tres universidades de California y una de Utah

lograron establecer una conexión conocida como ARPANET (Advanced Research Projects Agency Network).

Servicios

El correo electrónico

El correo electrónico sirve para enviar y recibir mensajes escritos entre usuarios de una red informática.
Es uno de los servicios más antiguos y extendidos de Internet. Una de sus ventajas es que se pueden añadir archivos de todo tipo a los mensajes: documentos escritos con un procesador de textos, imágenes, etc.
Prácticamente todos los usuarios de Internet emplean el correo electrónico. Permite comunicarse con otras personas que habitan en regiones diferentes del planeta con un coste reducido.

El servicio de conversación en línea (Chat)

En el correo electrónico no hace falta que los dos interlocutores estén conectados al mismo tiempo para recibir los mensajes. Sin embargo, existen en Internet otros servicios que sí permiten la comunicación simultánea.
El más conocido de ellos es el Chat.
El Chat, cuyo significado en español es “charla”, es un servicio en el que dos o más personas pueden establecer conversaciones a través de ventanas de texto en las que van apareciendo consecutivamente las intervenciones que cada interlocutor escribe con su teclado.

Telnet

El servicio Telnet permite controlar un equipo desde un lugar distante, sin sentarnos delante de él.
Esto facilita, por ejemplo, el acceso a una computadora de un empleado desde la sede de la empresa en otra ciudad. En el ámbito científico este servicio permite acceder a base de datos o incluso instrumentos que se encuentran alejados del investigador.

Los foros de discusión

Los foros de discusión son un servicio de Internet en el que muchos usuarios acceden a los mensajes escritos por un visitante de dicho foro.

La transferencia de archivos (FTP)

El servicio FTP (File Transfer Protocol) permite transferir archivos entre equipos informáticos.
Es uno de los servicios más antiguos de Internet. En algunos casos, los archivos almacenados se protegen con una contraseña, de manera que sólo los usuarios autorizados pueden manipularlos.

SFTP

Sus siglas significan SSH File Transfer Protocol, es completamente diferente del protocolo FTP (File Transfer Protocol). SFTP fue contruído desde cero y añade la característica de FTP a SSH. Sólo usa un canal de comunicación, envía y recibe los mensajes en binario (y no en formato texto como hace FTP).

FTPS

Es una extensión de FTP mediante SSL para el cifrado de los datos, utiliza dos canales de , envía y recibe los mensajes en formato texto. FTPS normalmente es más conocido ya que usa los mismos comandos que FTP.

Videoconferencia

El servicio de videoconferencia permite mantener comunicación sonora y visual entre dos usuarios de Internet [7].

3.1.2 Intranet

Una intranet es un conjunto de servicios de Internet (por ejemplo, un servidor Web) dentro de una red local, es decir que es accesible sólo desde estaciones de trabajo de una red local o que es un conjunto de redes bien definidas invisibles (o inaccesibles) desde el exterior. Implica el uso de estándares cliente-servidor de Internet mediante protocolos TCP/IP, como por ejemplo el uso de navegadores de Internet (cliente basado en protocolo HTTP) y servidores Web (protocolo HTTP) para crear un sistema de información dentro de una organización o empresa [8].

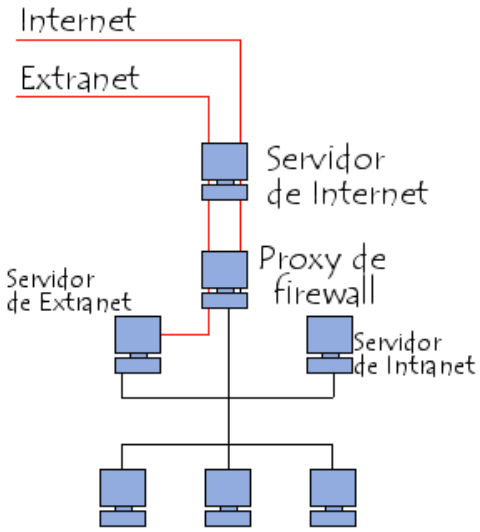


Figura 1 Red de área local.

Generalmente, la base de una intranet es una arquitectura de tres capas y comprende:

- Clientes (casi siempre personas que navegan en Internet)
- Uno o varios servidores de aplicaciones (middleware): un servidor Web que permite interpretar CGI, PHP, ASP u otras secuencias de comandos y traducirlos a consultas SQL para poder consultar una base de datos.
- Un servidor de bases de datos.

Ventajas de una Intranet

Una intranet permite construir un sistema de información a bajo coste (específicamente, el coste de una intranet puede estar perfectamente limitado a los costes de hardware, mantenimiento y actualización, con estaciones de trabajo cliente que funcionan con navegadores gratuitos, un servidor que se ejecuta bajo Linux con un servidor Web Apache y el servidor de bases de datos MySQL).

Servicios

- Acceso a la información sobre la empresa (tablero de anuncios).
- Acceso a documentos técnicos.
- Motores de búsqueda para la documentación.
- Intercambio de datos entre compañeros de trabajo.
- Nómina del personal.
- Dirección de proyectos, asistencia en la toma de decisiones, agenda, ingeniería asistida por equipo.
- Mensajería electrónica.
- Foros de discusión, listas de distribución, chat directo.
- Video conferencia.
- Portal de Internet [8].

El uso adecuado de Internet en la empresa

El uso indebido de Internet no sólo lleva a la distracción de los usuarios en tareas que no tienen que ver con el negocio de la compañía, sino que degrada la performance del vínculo de Internet, lo cual conlleva a la lentitud de accesos debido a la saturación del vínculo o, incluso, a la imposibilidad de conexión a una web o a un servicio de Internet necesario para el negocio.

El uso de antivirus o firewalls puede ayudar a evitar el ingreso de troyanos o archivos maliciosos en la red, pero no mejora nuestro propio uso de Internet. Son un complemento de nuestra seguridad.

Algunas empresas, por no tener políticas de Internet, permiten el uso de mensajería instantánea y la transferencia de archivos por este medio. Puede ocurrir fácilmente que un usuario reciba vía su mensajero un archivo que ejecutable automáticamente, y se borren todos los documentos de su disco y los de los recursos compartidos del servidor de archivos a los cuales tiene acceso.

Esto puede causar que la empresa quede sin esta información durante horas, hasta la recuperación desde un Backup, si es que existe, ya que en muchos casos no sucede así [8].

El problema no es la falta de infraestructura necesaria para administrar la seguridad, sino la ausencia de normas definidas y estrictas dentro de la firma. En ciertos casos, el mal uso de Internet por parte de los empleados de una firma puede causar algún daño no sólo a ella, sino a otros. Entonces, la empresa deberá responder civilmente -en la mayoría de los casos- por los daños que los trabajadores pudieran haber ocasionado a terceros.

Esto se traduce, desde ya, en el pago de indemnizaciones por parte de la compañía. Generación de malas prácticas laborales: la ausencia de sanciones o de controles bien definidos puede motivar a otros empleados a seguir el ejemplo de los que utilizan inadecuadamente las herramientas informáticas de la empresa.

Problemas y soluciones

Las cuestiones que más deberían preocupar a las empresas, por sus consecuencias económicas y legales son:

- Excesiva y abusiva navegación por Internet con fines extra labórales o no justificados por la tarea.
- Ocupación de memoria y demás recursos para fines personales.
- Descarga ilegal de software licenciado.
- Descarga ilegal de música.
- Tráfico de material pornográfico.
- Uso de correo electrónico para fines personales.
- Transmisión a terceros de información confidencial.
- Inutilización de sistemas o equipos informáticos.
- Para combatirlos, es conveniente seguir estos consejos:

- Identificar y priorizar los recursos informáticos de la empresa.
- Establecer condiciones de uso del correo y de navegación.
- Disponer de un plan de contingencia que contemple copias de resguardo, autenticación de usuarios, integridad de datos, confidencialidad de la información almacenada y control de acceso.
- Actualización permanente y observancia de las normas laborales.
- Educación y capacitación constante sobre la política de la empresa.

Evitar problemas al usar Internet en la empresa

Una vez convencidos de la necesidad de implementar normas de uso adecuado de Internet, el siguiente paso es cuáles, cómo y con qué gasto en recursos materiales y humanos. Esto dependerá de cada empresa y de sus necesidades:
"La inversión en seguridad para proteger determinada información tiene que estar en relación con el valor de dicha información.

Es más importante, por ejemplo, proteger los datos de una cartera de clientes que el log de navegación por Internet.

En el mismo sentido, en primer lugar, la empresa debe identificar y priorizar la protección de los recursos que considere más importantes. Una vez hecho esto, tiene que adoptar una política de uso de las herramientas informáticas. Luego, lo más importante es el cumplimiento de esa política. La capacitación constante al personal y las auditorías periódicas para determinar los grados de cumplimiento constituyen acciones indispensables para contrarrestar los problemas generados por el uso de Internet, correo electrónico y otros recursos.

Es de destacar que los fabricantes de software y de hardware para la seguridad en el uso de Internet son muchos en el mercado, y todos muy buenos.
Por eso, aunque es recomendable usar herramientas de filtro de contenidos y control de acceso, lo fundamental es la educación de los usuarios, para que comprendan el problema y colaboren con la solución [8].

Los tres modos de racionalizar el uso de Internet en la empresa

Hay tres tipos de soluciones técnicas diferentes y según el caso, pueden combinarse:

Balanceo de carga: Se utiliza un vínculo par navegación (que incluye el uso recreativo) y otro diferente para los servicios esenciales de infraestructura (VPN, VoIP, etc.). El de uso general oficia, además, de Backup para el principal, y la conmutación es transparente para los usuarios finales.

Aplicación de políticas de QoS (calidad de servicio): Se pueden dar diferentes prioridades a los servicios y/o asignar porciones determinadas del ancho de banda a uno en particular (navegación, e-mail, VPN, telefonía IP, etc.). Por ejemplo, que la navegación tenga prioridad baja, y el circuito de aprobación de ventas online tenga prioridad alta, debido a su importancia para el negocio y la facturación.

Aplicación de políticas de uso restrictivas: Sólo la gerencia o determinados perfiles del personal pueden hacer uso irrestricto de la navegación por Internet. El resto puede navegar con mayores o menores restricciones o, incluso, se puede limitar su uso a herramientas esenciales, como el correo electrónico únicamente.

Es evidente que las restricciones al uso de Internet pueden no ser del agrado de quienes deban someterse a ellas. Incluso, pueden considerarse un obstáculo para las tareas, y un perjuicio a la productividad del empleado. ¿Qué hacer? En general, siempre se puede permitir un determinado recurso para un fin, pero no para otros, o en un tipo de negocio, pero no en otros.

3.1.3 Topologías de Redes

Una red de computadoras está compuesta por equipos que están conectados entre sí mediante líneas de comunicación (cables de red, etc.) y elementos de hardware (adaptadores de red y otros equipos que garantizan que los datos viajen correctamente). La configuración física, es decir la configuración espacial de la red, se denomina topología. Los tipos de topología mas importante son:

- Topología de bus
- Topología de estrella
- Topología en anillo
- Topología de árbol
- Topología de malla

Topología de bus

La topología de bus es la manera más simple en la que se puede organizar una red. En la topología de bus, todos los equipos están conectados a la misma línea de transmisión mediante un cable. La palabra "bus" hace referencia a la línea física que une todos los equipos de la red.

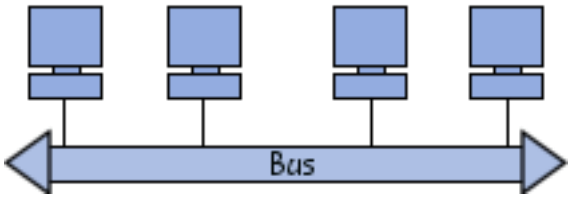


Figura 2 Topología BUS.

La ventaja de esta topología es su facilidad de implementación y funcionamiento. Sin embargo, esta topología es altamente vulnerable, ya que, si una de las conexiones es defectuosa, esto afecta a toda la red.

Topología de estrella

En la topología de estrella, los equipos de la red están conectados a un hardware denominado concentrador. Es un equipo que contiene un cierto número de sockets a los cuales se pueden conectar los cables de los equipos. Su función es garantizar la comunicación entre esos sockets.

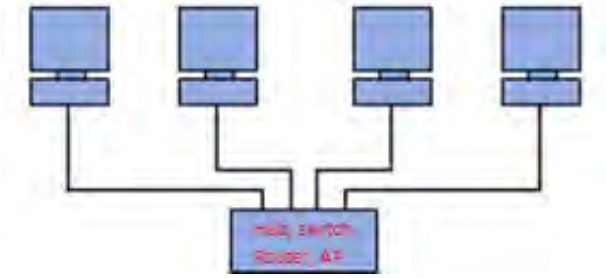


Figura 3 Topología Estrella.

A diferencia de las redes construidas con la topología de bus, las redes que usan la topología de estrella son mucho menos vulnerables, ya que se puede eliminar una de las conexiones fácilmente desconectándola del concentrador sin paralizar el resto de la red. El punto crítico en esta red es el concentrador, ya que la ausencia del mismo imposibilita la comunicación entre los equipos de la red. Sin embargo, una red con topología de estrella es más cara que una red con topología de bus, dado que se necesita hardware adicional (el concentrador).

Topologia lógica

Es la forma en que una red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La topología lógica de los enlaces punto a punto es relativamente simple,

mientras que los medios compartidos ofrecen métodos de control de acceso al medio deterministas y no deterministas [9].

Topología en anillo

En una red con topología en anillo, los equipos se comunican por turnos y se crea un bucle de equipos en el cual cada uno "tiene su turno para hablar" después del otro. En realidad, las redes con topología en anillo no están conectadas en bucles. Están conectadas a un distribuidor (denominado MAU, Unidad de acceso multi estación) que administra la comunicación entre los equipos conectados a él, lo que le da tiempo a cada uno para "hablar".

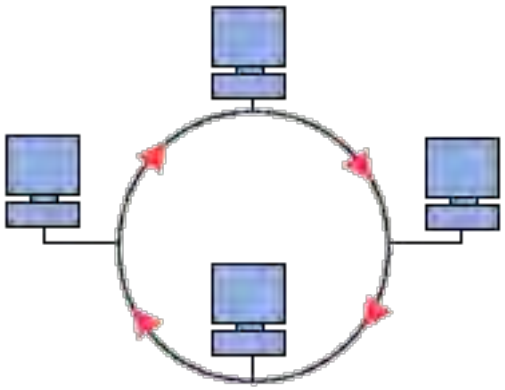


Figura 4 Topología Anillo.

Las dos topologías lógicas principales que usan esta topología física son la red en anillo y la FDDI (interfaz de datos distribuidos por fibra).

3.1.4 Tipos de Redes

Red pública: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

Red privada: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

Red de Área Personal (PAN): (Personal Area Network) es una red de computadoras usada para la comunicación entre las computadoras, Smartphone o cualquier dispositivo cerca de una persona.. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar con

una red de alto nivel y el Internet (un up link). Las redes personales del área se pueden conectar con cables con los buses de la computadora tales como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.

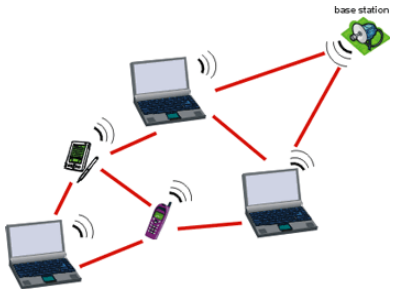


Figura 5 Red de Área Personal, PAN.

Red de área local (LAN): una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización. Nota: Para los propósitos administrativos, LANs grande se divide generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroups es un grupo de las computadoras que comparten un sistema común de recursos dentro de un LAN [10].

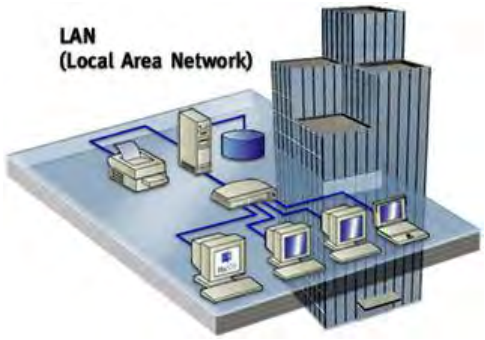


Figura 6 Red de Área Local, LAN.

Red de área local virtual (VLAN): Una Virtual LAN o comúnmente conocida como VLAN, es un grupo de computadoras, con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast, a pesar de su diversa localización física. Con esto, se pueden lógicamente agrupar computadoras para que la localización de la red ya no sea tan asociada y restringida a la localización física de cada computadora, como sucede con una LAN, otorgando además seguridad, flexibilidad y ahorro de recursos.

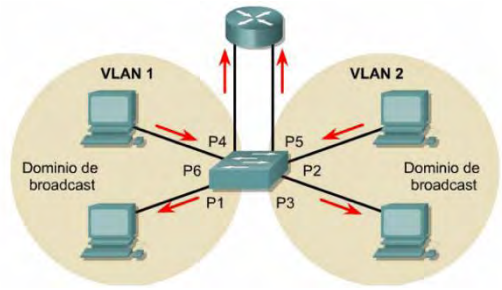


Figura 7 Red de Área Local de manera Virtual, VLAN.

Red del área del campus (CAN): Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

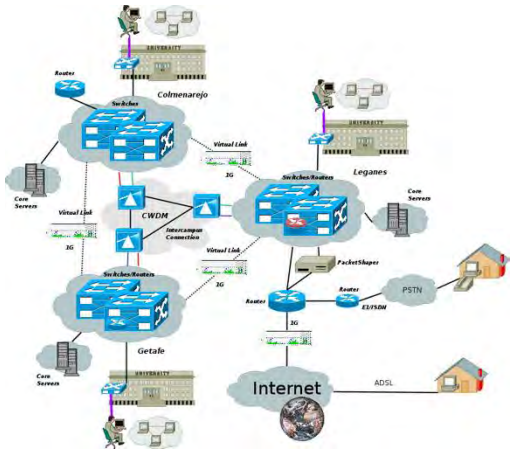


Figura 8 Red de Área Local por campus o complejo, CAN.

Red de área metropolitana (MAN): una red que conecta las redes de un área dos o más locales juntos, pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Los enrutadores (routers) múltiples, los interruptores (switch) por lo que las bases de datos estarían conectadas para crear a una MAN.

Figura 9 Red de Área Metropolitana, MAN.

Red de área amplia (WAN): es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono.

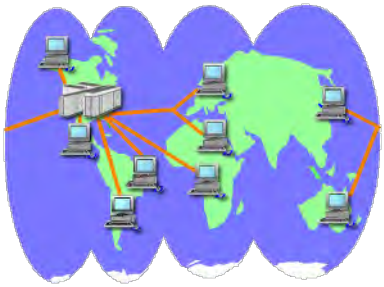


Figura 10 Red de Área Amplia, WAN.

Red de área de almacenamiento (SAN): Es una red concebida para conectar servidores, arreglos de discos y librerías de soporte. Principalmente, está basada en tecnología de fibra. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos de almacenamiento que la conforman.

Figura 11 Red de área de almacenamiento, SAN.

Red irregular: Es un sistema de cables que se conectan a través de un módem, y que da como resultado la conexión de una o más computadoras.

3.2 Sistemas operativos

Descripción del sistema operativo

Para que una computadora pueda hacer funcionar un programa informático, debe contar con la capacidad necesaria para realizar cierta cantidad de operaciones preparatorias que puedan garantizar el intercambio entre el procesador, la memoria y los recursos físicos (periféricos).

El sistema operativo se encarga de crear el vínculo entre los recursos materiales, el usuario y las aplicaciones. Cuando un programa desea acceder a un recurso material, no necesita enviar información

específica a los dispositivos periféricos; simplemente envía la información al sistema operativo, el cual la transmite a los periféricos correspondientes a través de su driver (controlador). Si no existe ningún driver, cada programa debe reconocer y tener presente la comunicación con cada tipo de periférico [11].

3.2.1 Clasificación de Sistemas Operativos

Los sistemas operativos pueden ser clasificados de la siguiente manera [12]:

- Según la administración de tareas:

  Monotarea: este tipo de sistemas operativos son capaces de manejar un programa o realizar una sola tarea a la vez. Son los más antiguos. Por ejemplo, si el usuario está escaneando, la computadora no responderá a nuevas indicaciones ni comenzará un proceso nuevo.

  Multitarea: esta característica es propia de los S.O. más avanzados y permiten ejecutar varios procesos a la vez, desde uno o varias computadoras, es decir que los pueden utilizar varios usuarios al mismo tiempo. Esto se puede realizar por medio de sesiones remotas una red o bien, a través de terminales conectadas a una computadora.

- Según la administración de usuarios:

  Monousuario: Sólo pueden responder a un usuario por vez. De esta manera, cualquier usuario tiene acceso a los datos del sistema. Existe un único usuario que puede realizar cualquier tipo de operación.

  Multiusuario: esta característica es propia de aquellos S.O. en los que varios usuarios pueden acceder a sus servicios y procesamientos al mismo tiempo. De esta manera, satisfacen las necesidades de varios usuarios que estén utilizando los mismos recursos, ya sea memoria, programas, procesador, impresoras, scanners, entre otros [13].

Lista de sistemas operativos

D.O.S.: Sus siglas corresponden a Sistema Operativo de Disco o Disk Operating System. En sus inicios, DOS ganó rápidamente una alta popularidad en el incipiente mercado de las PCs, allá por los 90. Prácticamente todo el software desarrollado para PCs se creaba para funcionar en este S.O.

Windows 3.1: Microsoft vuelve a tomar la iniciativa, y desarrolla un sistema operativo con interfaz gráfica, fácil de usar para el usuario promedio. Así nace Windows, con un sistema de ventanas con archivos identificables gráficamente a través de íconos. El mouse comienza a ser utilizado en la interacción con el sistema, agilizando y facilitando cualquier tipo de tarea. 1. Allá por 1995 en pleno auge del mercado de las PCs, y lo llama Windows 95. Con los años, Microsoft fue actualizando este sistema, lanzando Windows 98, Windows Me, Windows XP, Windows 7, Windows 8, hasta llegar al recientemente lanzado Windows 10.

OS/2: Este sistema, fabricado por IBM, intentó reemplazar a DOS como sistema operativo de las PCs. Su versión 1.0 fue lanzada con arquitectura de 16 bits en 1987, actualizada luego en su versión 2.0 a la arquitectura de 32 bits, gracias al procesador Intel 80386. No tuvo una buena recibida en el mercado, al no contar con el apoyo de gran parte de los desarrolladores de software, que se volcaron a la creación de programas para Windows.

Mac OS / Mac OS X. El Mac OS (Macintosh Operating System) es un sistema operativo creado por Apple Inc. y destinado exclusivamente a las computadoras Macintosh comercializadas por la misma compañía. Lanzado por primera vez en 1985, fue evolucionando hasta 2002, año en el que se lanza la versión 10 (conocida como Mac OS X), que cambió su arquitectura y pasó a basarse en UNIX. Es un sistema muy amigable para el usuario, se aprende a usar con bastante rapidez.

Unix: Desarrollado en 1969 por AT&T, se trata de un SO portable, multitarea y multiusuario, que corre en una variada clase de computadoras (mainframes, PCs, Workstations, supercomputadoras).

Linux, es un sistema operativo. Es una implementación de libre distribución UNIX para computadoras personales (PC), servidores y estaciones de trabajo. Es usado como sistema operativo en una amplia variedad de plataformas de hardware y computadores, incluyendo los computadores de escritorio (PCs x86 y x86-64, y Macintosh y PowerPC), servidores, supercomputadores, mainframes, y dispositivos empotrados así como teléfonos celulares.
En 1983 Richard Stallman fundó el proyecto GNU, con el fin de crear sistemas operativos parecidos a UNIX y compatibles con POSIX. Dos años más tarde creó la "Fundación del Software Libre" y escribió la GNU General Public License para posibilitar el software libre en el sistema de copyright.

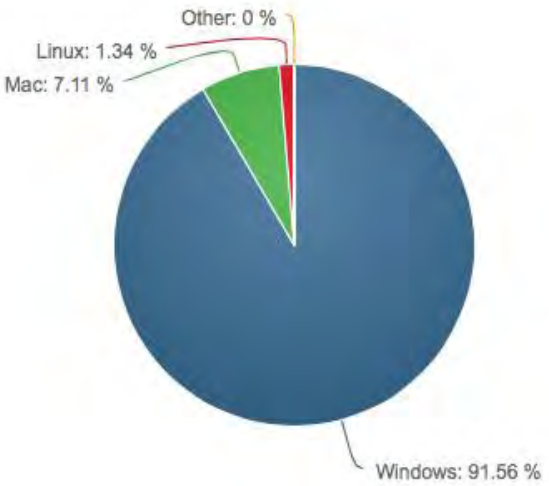


Figura 12 Sistemas operativos más usados en PC en el mundo[14].

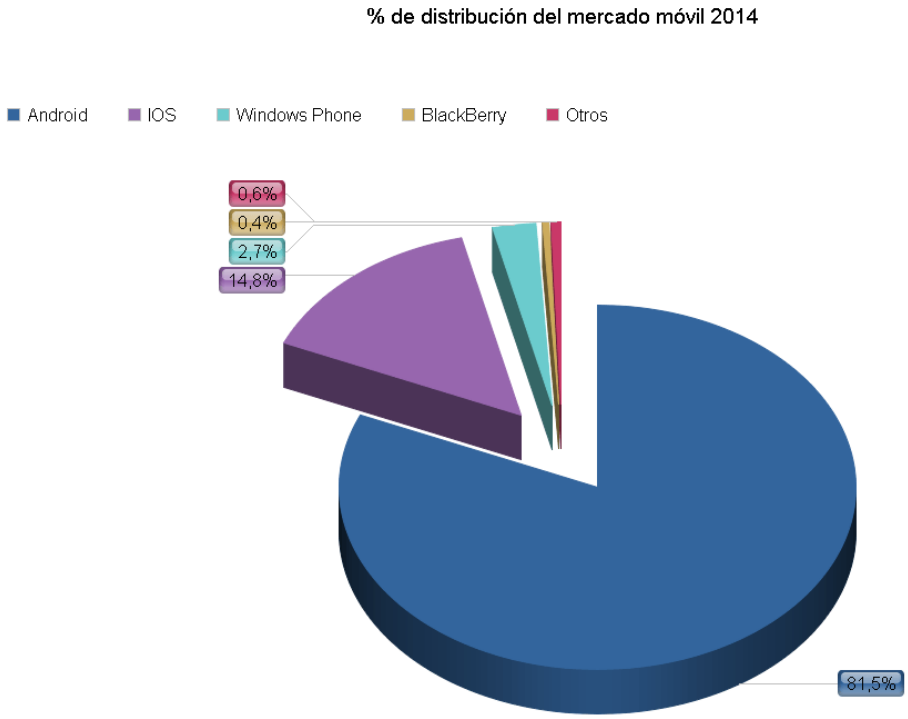


Figura 13 Sistemas operativos más usados para Smartphone en el mundo[15].

3.2.2 Sistema Operativos para Redes

El sistema operativo de red determina recursos, así como la forma de compartirlos y acceder a ellos. Para determinar el sistema operativo de red más adecuado, es necesario establecer en primer lugar la arquitectura de la red, es decir, si va a ser cliente/servidor o trabajo en grupo.

Esta decisión suele estar condicionada por el tipo de seguridad que se requiere. Después de identificar las necesidades de seguridad de la red, hay que determinar los tipos de interoperabilidad necesaria en la red [16].

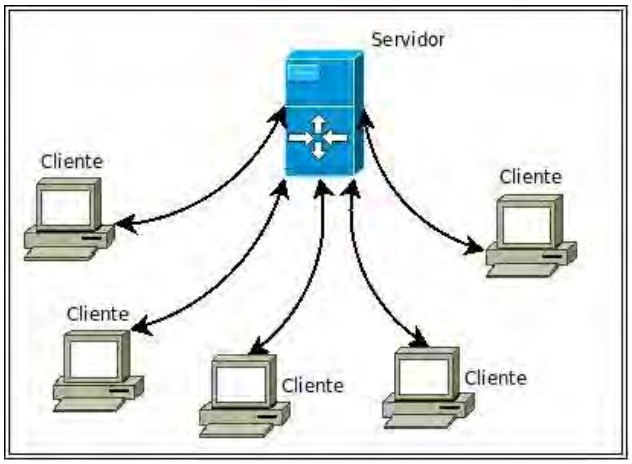


Figura 14 Modelo Cliente Servidor.

Sistemas operativos de Novell

Es una de las plataformas de servicio más fiable para ofrecer acceso seguro y continuado a la red y los recursos de información, sobre todo en cuanto a servidores de archivos. El sistema operativo NetWare está formado por aplicaciones de servidor y cliente. Proporciona servicios como administración de archivos (mediante la base de datos NDS), seguridad de gran alcance y servicios de impresión transparentes al usuario. Tiene como inconveniente que no puede interoperar con otras redes de Windows NT. Ejemplo: Un cliente Microsoft Windows puede asignar una unidad lógica a cualquier volumen o directorio de un servidor de archivos de NetWare, de forma que los recursos de NetWare aparecerán como unidades lógicas

Novell.
NetWare

Figura 15 Sistemas operativos.

Sistemas operativos de Microsoft

Desde que Microsoft lanzó el primer Windows NT en 1993 como sistema operativo de red, no ha dejado de evolucionar y de ampliar funciones e interoperabilidad con otros sistemas operativos como NetWare. Windows NT combina el sistema operativo del equipo y de red en un mismo sistema y trabaja sobre un modelo de dominio. Está formado por Windows NT Server, que configura un equipo para trabajar como servidor, y Windows NT Workstation, que proporciona a un equipo las funciones de cliente. Después de Windows NT, se presentaron Windows Server 2000 y Server 2003.

Figura 16 Sistemas operativos.

Sistemas operativos de Apple

El sistema operativo de red Appletalk está completamente integrado en el sistema operativo de cada equipo que ejecuta el Mac OS. La implementación actual de AppleTalk permite posibilidades de interconexión Trabajo en Grupo de alta velocidad entre equipos Apple, así como interoperabilidad con otros equipos y sistemas operativos de red.

Figura 17 Sistemas operativos.

Solaris

El primer sistema operativo de Sun nació en 1983 y se llamó inicialmente SunOS. Estaba basado en el sistema UNIX BSD, de la Universidad de Berkeley, del cual uno de los fundadores de la compañía fue programador en sus tiempos universitarios. Más adelante incorporó funcionalidades del System V, convirtiéndose prácticamente en un sistema operativo totalmente basado en System V.

Esta versión basada en System V fue publicada en 1992 y fue la primera en llamarse Solaris.Solaris tiene una reputación de ser muy adecuado para el multiprocesamiento simétrico (SMP), soportando un gran número de CPUs[17].

Figura 18 Sistemas operativos.

GNU/Linux

Linux tiene su origen en Unix. Éste apareció en los años sesenta, desarrollado por los investigadores Dennis Ritchie y Ken Thompson, de los Laboratorios Telefónicos Bell.Es un sistema operativo de software libre (no es propiedad de ninguna persona o empresa), por ende no es necesario comprar una licencia para instalarlo y utilizarlo en un equipo informático. Es un sistema multitarea, multiusuario, compatible con UNIX, y proporciona una interfaz de comandos y una interfaz gráfica, que lo convierte en un sistema muy atractivo y con estupendas perspectivas de futuro.
Al ser software libre, el código fuente es accesible para que cualquier usuario pueda estudiarlo y modificarlo. La licencia de Linux no restringe el derecho de venta, por lo que diversas empresas de software comercial distribuyen versiones de Linux. Además de esto, este sistema cuenta con muchas distribuciones y gestores de ventanas para el entorno gráfico.

Figura 19 Sistemas operativos.

LOS SISTEMAS OPERATIVOS POR SERVICIOS

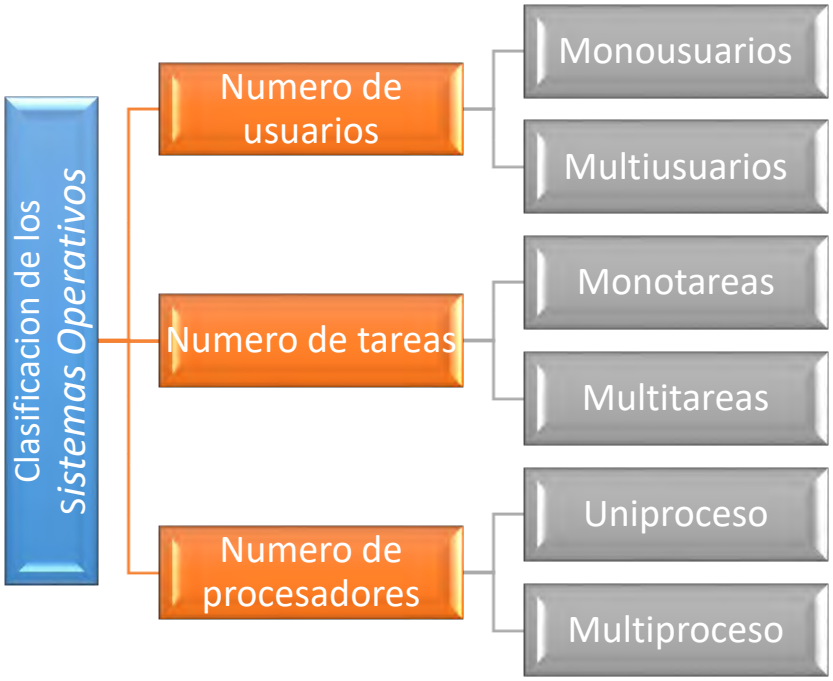


Figura 20 Clasificación de sistemas operativos por servicio.

3.3 Seguridad informática

La seguridad informática consiste en asegurar que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Si bien es cierto que todos los componentes de un sistema informático están expuestos a una amenaza, ataque o vulnerabilidad, son los datos y la información los sujetos principales de protección de las técnicas de seguridad.

La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y la disponibilidad de la información, por tanto, actualmente se considera que la seguridad de los datos y la información comprenden 3 aspectos fundamentales [18]:

- Confidencialidad
- Integridad
- Disponibilidad

Figura 21 Sistema seguro o fiable.

Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.
Un ejemplo de control de la confidencialidad sería el uso cifrado de una clave en el intercambio de mensajes.

Integridad: Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Disponibilidad: Se trata de la capacidad de un servicio, de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requieran. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite [19].

La disponibilidad se presenta en niveles:

- **Base**: Se produce paradas previstas e imprevistas.
- **Alta**: Incluyen tecnologías para disminuir el número y la duración de interrupciones imprevistas aunque siempre existe alguna interrupción imprevista.
- **Operaciones continuas:** Utilizan tecnologías para asegurar que no hay interrupciones planificadas
- **Sistemas de disponibilidad continua**: Se incluyen tecnologías para asegurarse que no habrá paradas imprevistas ni previstas.
- **Sistemas de tolerancia al desastre**: requieren de sistemas alejados entre sí para asumir el control en una interrupción provocada por un desastre.

Autenticación: Es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice. La autenticación de los sistemas informático se realiza habitualmente mediante nombre y contraseña.

No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación.

Existen 2 posibilidades:

- **No repudio en origen**: el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo el receptor recibe una prueba infalsificable del envío.
- **No repudio de destino**: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

Si la autenticidad prueba quien es el autor y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (en origen) y que el destinatario la recibió (en destino).

Seguridad perimetral

Un punto muy importante en cuestión de la seguridad es la seguridad perimetral cuya definición es más que el establecimiento de un perímetro de seguridad que proteja o bien aislé la red local interna de una externa.
El primer control de acceso que se puede aplicar en una red es la segmentación de los dominios de colisión y difusión.
El filtrado de paquetes se puede realizar a distintos niveles de la pila TCP/IP, con elementos y características diferentes por nivel. Así, a nivel de red, se encuentran los llamados router de selección que son, básicamente, equipos de red que tienen la capacidad de encaminar y filtrar paquetes.

Seguridad en la red de la PYME

En Internet, hay múltiples amenazas que pueden dañar la red de una empresa. Muchas veces se aprovecha la imprudencia de algunos empleados al usar la Web, el correo o la mensajería instantánea. La solución es establecer normas claras al respecto y hacerlas cumplir[20].

Una red corporativa puede colapsar si un ataque logra tener éxito. Por molesto que resulte, hoy a una compañía no le basta tener un antivirus y un firewall para estar a salvo de los muchos problemas que puede causarle un uso indiscriminado de Internet. Necesita algo que, sólo en parte, se soluciona técnicamente: políticas de adecuado de la Red en el entorno laboral. No todas las empresas tienen conciencia de esa necesidad de contar con una mayor seguridad. Las principales causas son:

- Descargar música o películas u otros archivos no legales.
- Abrir documentos adjuntos o hacer clic en enlaces de mensajes no solicitados.
- Visitar sitios web pornográficos o de contenido ilícito.
- Abrir programas con archivos y presentaciones con bromas enviados por familiares, amigos o compañeros de trabajo.
- Instalar programas no autorizados o complementos del navegador Web.
- Proporcionar datos personales a desconocidos por teléfono o e-mail.
- Utilizar la misma contraseña en diferentes páginas Web o compartirla con otros.

Y estas cosas peligrosas no se hacen por maldad o deslealtad, sino por desconocimiento de los problemas potenciales:
Generalmente, cuando los empleados hacen un uso irresponsable de Internet, no saben que eso puede tener consecuencias desastrosas para la empresa en la que trabajan.

3.4 Manejo de la Información

Como es sabido, la información es un arma muy poderosa, que, si cae en manos de las personas incorrectas, puede resultar en graves consecuencias para el propietario de la información.

Es por ello que es de suma importancia darle sumo cuidado a toda clase de información de las personas, pues lo que puede parecer insignificante para algunos, para otros puede ser el medio que les permita realizar algún ataque informático a cualquier individuo.
Si se toman en cuenta las siguientes medidas de protección para la información, el riesgo de que sufra un mal manejo ésta, disminuirá notablemente.

Hacer una clasificación de la información para implementar las medidas necesarias de seguridad según corresponda. Se debe seleccionar debidamente aquella que es crítica, y darle el nivel de seguridad adecuado, realizar un manejo de riesgo y evitar fugas de información

Proteger la información sensible mediante respaldo en un servidor externo o en su defecto un medio de almacenamiento externo y no en el dispositivo. Cabe señalar que en caso de que utilice un medio de almacenamiento externo, debe tener sumo cuidado con éste y resguardarlo debidamente.

Realizar los respaldos de información en por lo menos 2 medios diferentes. Dichos respaldos se deben realizar de manera periódica. Evitar eliminar la información útil hasta cerciorarse que se encuentra debidamente respaldada.

Tener extremo cuidado con la información que se lleva al Cloud, ya que esa información tendrá un alto grado de riesgo, debido a que no tendrá fronteras en la cobertura. Se debe evitar subir aquella información que sea crítica.

Una vez que se ha decidido hacer uso del Cloud, es recomendable que se lean de manera minuciosa los contratos que se tiene, para asegurarse que la información no quedará respaldada en data centers de la competencia.

Evitar dejar los documentos importantes en lugares visibles o de fácil acceso para otras personas.

Evitar en lo posible trabajar en lugares públicos como los cafés o aeropuertos, o de hacerlo tener el debido cuidado que la información que está manejando y la cual puede ver las personas a su alrededor, no sea tan descriptiva, pues muchas veces se piensa que el hacer una presentación no es importante para alguien más, sin embargo quizá con dicho documento las personas podrían enterarse para empezar de dónde trabaja, por dar un ejemplo, sin contar con otros datos que podrían descifrar las personas con ver su información.

En caso de que se recurra frecuentemente al uso de su laptop o dispositivo móvil en lugares públicos, opte por adquirir un filtro de pantalla, el cual opaca la pantalla prácticamente desde cualquier ángulo, a excepción del frontal.

Evitar traer el gafete de identificación en la calle y lugares públicos, hacer uso de él exclusivamente para las actividades que se lo demanden y guardarlo siempre que le sea posible.

Desechar la información relevante como la información bancaria, sólo si ésta ha sido destruida previamente.

3.4.1 Medios de Almacenamiento

Básicamente, una unidad de almacenamiento es un dispositivo capaz de leer y escribir información con el propósito de almacenarla permanentemente. En la actualidad contamos con muchas clases y categorías de unidades de almacenamiento, pudiendo encontrar en el mercado una amplia variedad de dispositivos internos o externos capaces de almacenar una cantidad de datos impensada en el pasado.

También llamado almacenamiento secundario, estos dispositivos pueden guardar información en su interior, como en el caso de los discos rígidos, tarjetas de memoria y pendrives, o como en el caso de las unidades de almacenamiento óptico como Blu-Ray, DVD o CD, grabándolas en un soporte en forma de disco.

Este tipo de dispositivos es la más segura y práctica forma de almacenar muchísima cantidad de información en forma sencilla y permanente, además, los datos que guardemos en ellos siempre estarán disponibles gracias a que no es necesario suministrarles energía eléctrica para que permanezcan almacenados.

Tipos de dispositivos de almacenamiento

Actualmente son tres los tipos de dispositivos que solemos usar en las tareas diarias para almacenar y transportar información:

Medios ópticos: CDs, DVDs, Blu-Ray, etc.

Figura 22 Unidades ópticas.

Medios magnéticos: Discos rígidos, cintas magnéticas, diskettes, etc.

Figura 23 Unidades Magnéticas.

Medios electrónicos: Discos SSD, pendrives, tarjetas de memoria, etc.

Figura 24 Medios electrónicos.

3.4.2 Almacenamiento Virtual (Nube).

Almacenamiento en la nube

Es un modelo de servicio en el cual los datos de un sistema de cómputo se almacenan, se administran, y se respaldan de forma remota, típicamente en servidores que están en la nube y que son administrados por un proveedor del servicio. Estos datos se ponen a disposición de los usuarios a través de una red, como lo es Internet.

Al hablar de almacenamiento en la nube, se busca mantener las ventajas principales de un sistema en la nube, como son: elasticidad en el espacio que puedes usar, y que sea un servicio por demanda, que en este caso se maneja por bloques de información, por ejemplo, puedes contratar 5GB, 10GB, 30GB o 100GB, pero no intermedios.

Típicamente se relaciona al almacenamiento en la nube como una práctica de empresas, con grandes necesidades de espacio, sin embargo, existen servicios que puedes usar como un usuario privado, algunos de ellos gratuitos (hasta cierta cantidad de datos), y que te pueden servir para respaldar tu información, tenerla accesible desde cualquier computadora.

Tipos de almacenamiento en la nube.

Existen básicamente tres tipos de servicios de almacenamiento en la nube:

Público.- Se trata de un servicio en la nube que requiere poco control administrativo y que se puede acceder en línea por cualquier persona que esté autorizada. El almacenamiento en la nube pública utiliza un mismo conjunto de hardware para hacer el almacenamiento de la información de varias personas, con medidas de seguridad y espacios virtuales para que cada usuario puede ver únicamente la información que le corresponde. Este servicio es alojado externamente, y se puede acceder mediante Internet, y es el que usualmente una persona individual puede acceder, por su bajo costo y el bajo requerimiento de mantenimiento. Entre los servicios que puedes encontrar como almacenamiento en la nube pública están:

- Dropbox, que es uno de los servicios más populares para compartir archivos en la nube.
- Google Drive, que es el servicio de almacenamiento en la nube de Google.
- Box.
- Sugar Sync.

Privado.- Almacenamiento en la nube privada funciona exactamente como el nombre sugiere. Un sistema de este tipo está diseñado específicamente para cubrir las necesidades de una persona o empresa. Este tipo de almacenamiento en la nube puede ser presentado en dos formatos: on-premise (en la misma oficina o casa) y alojado externamente. Este modelo es más usado por empresas, no tanto así las personas individuales. En este modelo la empresa tiene el control administrativo, y por lo tanto le es posible diseñar y operar el sistema de acuerdo a sus necesidades específicas.

Híbrido.- Los sistemas de almacenamiento en nubes híbridas ofrecen, como su nombre sugiere, una combinación de almacenamiento en nubes públicas y privadas, de tal forma que le es posible a los usuarios el personalizar las funciones y las aplicaciones que se adaptan mejor a sus necesidades, así como los recursos que se utilizan. Un ejemplo típico de este tipo de servicio es que se configure de tal forma que los datos más importantes se almacenen en un sistema de almacenamiento en la nube privada, mientras que los datos menos importantes se pueden almacenar en una nube pública con acceso disponible por una gran cantidad de personas a distancia.

3.4.3 Correo Electrónico

Correo electrónico, es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónica. Para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías.

Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales dependiendo del sistema que se use.

Proceso de envío de correo electrónico.

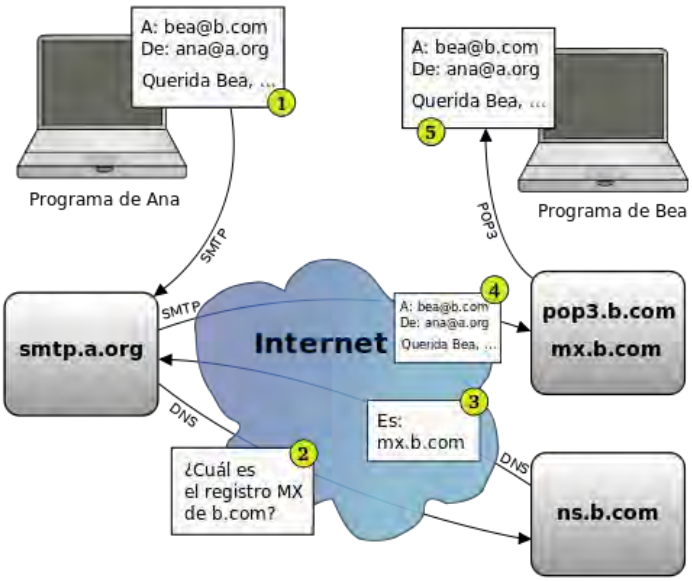


Figura 25 Proceso de envío electrónico.

3.5 Servidores

Un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse a una computadora física en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.
Un servidor sirve información a las computadoras que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.
Los servidores web, servidores de correo y servidores de bases de datos son a lo que tiene acceso la mayoría de la gente al usar Internet.

Tipos de Servidores

Servidores de Aplicaciones (Application Servers): Designados a veces como un tipo de middleware (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.

Servidores de Audio/Video (Audio/Video Servers): Los servidores de Audio/Video añaden capacidades multimedia a los sitios web permitiéndoles mostrar contenido multimedia en forma de flujo continuo (streaming) desde el servidor.

Servidores de Chat (Chat Servers): Los servidores de chat permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo discusiones en tiempo real.

Servidores de Fax (Fax Servers): Un servidor de fax es una solución ideal para organizaciones que tratan de reducir el uso del teléfono pero necesitan enviar documentos por fax.

Servidores Groupware (Groupware Servers): Un servidor groupware es un software diseñado para permitir colaborar a los usuarios, sin importar la localización, vía Internet o vía Intranet corporativo y trabajar juntos en una atmósfera virtual.

Servidores IRC (IRC Servers): Otra opción para usuarios que buscan la discusión en tiempo real, Internet Relay Chat consiste en varias redes de servidores separadas que permiten que los usuarios conecten el uno al otro vía una red IRC.

Servidores de Listas (List Servers): Los servidores de listas ofrecen una manera mejor de manejar listas de correo electrónico, bien sean discusiones interactivas abiertas al público o listas unidireccionales de anuncios, boletines de noticias o publicidad.
Servidores de Correo (Mail Servers): Casi tan ubicuos y cruciales como los servidores web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.

Servidores de Noticias (News Servers): Los servidores de noticias actúan como fuente de distribución y entrega para los millares de grupos de noticias públicos actualmente accesibles a través de la red de noticias USENET.

Servidores Proxy (Proxy Servers): Los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

Servidores Telnet (Telnet Servers): Un servidor telnet permite a los usuarios entrar en una computadora huésped y realizar tareas como si estuviera trabajando directamente en esa computadora.

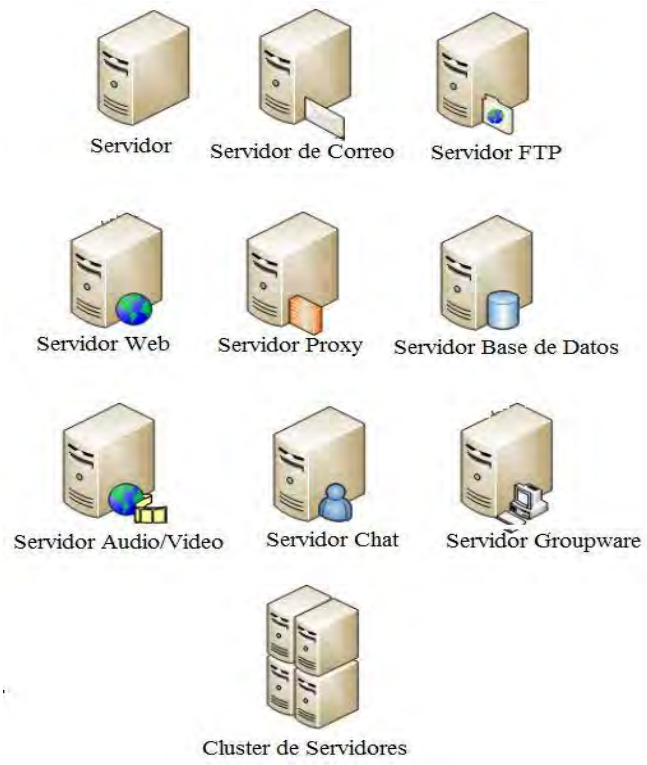


Figura 26 Tipos de Servidores de Internet.

3.6 Políticas de seguridad

En el ámbito de la seguridad de la información, una política es un documento que describe los requisitos o reglas específicas que deben cumplirse en una organización. Presenta una declaración formal, breve y de alto nivel, que abarca las creencias generales de la organización, metas, objetivos y procedimientos aceptables para un área determinada. Entre otras características:

- Requiere cumplimiento (obligatorio).
- El incumplimiento deriva en una acción disciplinaria.
- Se enfoca en los resultados deseados y no en los medios de ejecución.
- Deben ser concisas y fáciles de entender.
- Deben mantener un balance entre la protección y la productividad.

Las políticas de seguridad de la información proveen un marco para que las mejores prácticas puedan ser seguidas por los empleados, permiten minimizar riesgos y responder a eventos indeseados e inesperados. También ayudan al personal de la organización a asegurar sus activos, definir la postura de la organización hacia la protección de la información frente a accesos no autorizados, modificación, divulgación o destrucción. De manera específica, las políticas permiten:

- Proteger activos (personas, información, infraestructura y sistemas).
- Definir reglas para la conducta esperada del personal y usuarios.

- Definir roles y responsabilidades del personal.
- Definir y autorizar sanciones en caso de una violación.
- Mitigar riesgos.
- Ayudar en el cumplimiento de leyes, regulaciones y contratos.
- Crear conciencia entre el personal sobre la importancia y protección de los activos, principalmente de la información [21].

Capítulo 4

DISEÑO LÓGICO DE LA IMPLEMENTACIÓN (DLP).

Es este capítulo se describe el diseño lógico que se llevó a cabo durante la implementación de la solución de Symantec DLP.

4.1 Justificación de las herramientas

Para el diseño del proyecto y de acuerdo con los requerimientos establecidos en el capítulo 2, así como las herramientas investigadas en los antecedentes teóricos. Se decidió diseñar e implementar con la

herramienta Data Loss Prevention (DLP) la cual es una solución unificada para detectar, supervisar y proteger la información confidencial donde quiera que se almacene o utilice. La solución ofrece una cobertura integral de la información confidencial en el punto final de la red y los sistemas de almacenamiento, tanto si los usuarios están o no conectados a la red corporativa.

4.2 Análisis y Diseño de Servidor de Seguridad Perimetral

Para la implementación del Servidor perimetral se analizó el siguiente diagrama de red con la finalidad de identificar el lugar óptimo para la implementación de la solución de Symantec DLP.

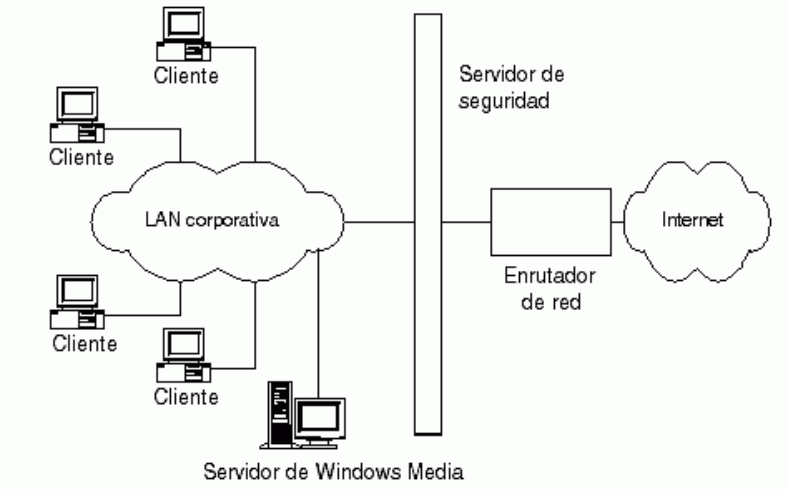


Figura 27 Diagrama general de red

Al realizar el análisis se identificó que los módulos necesarios serían los siguientes:

Endpoint Discover de Symantec Data Loss Prevention.

Está herramienta realiza un análisis en busca de datos confidenciales almacenados en los puntos finales, incluidos equipos portátiles, equipos de escritorio y estaciones de trabajo en oficinas remotas, con el objetivo de realizar un inventario, asegurar o reubicar esos datos.

Endpoint Prevent de Symantec Data Loss Prevention.

Permite proteger la información y evitar que los archivos confidenciales se descarguen en los discos locales, se copien a dispositivos USB o a otro tipo de soportes extraíbles, así como se transfieran por la red, se graben en CD o DVD, o bien se copien a una unidad, o se impriman o envíen por fax de forma electrónica.

Para el uso de estas dos herramientas se debe realizar la implementación en un Servidor y por ello se recomienda un software de Licencia y que tenga soporte todo el tiempo. Por ello se descarta el uso de GNU Linux y se sugiere Windows 2008r2 para dicha implementación.

4.2.1 Elección de Hardware y Software

Un servidor de detección permitirá validar las solicitudes realizadas en la red corporativa desde cualquier punto para la extracción de información, el cual se podrá instalar y configurar bajo plataforma Windows o Microsoft Windows Server 2008 R2, Enterprise Edition (64-bit). A continuación, se mencionan algunas características técnicas de Microsoft Windows Server 2008 R2, Enterprise Edition (64-bit).
Los requerimientos mínimos para llevar a cabo esta implementación son los siguientes:

Requerido para	Enforce Server - Oracle Server	Endpoint server
Procesador.	2 x 3.0 GHz CPU quad core.	2 x 3.0 GHz CPU dual core.
Memoria.	8 GB de RAM, si está Oracle en el mismo servidor 16 GB RAM.	8 GB RAM.
Disco duro.	500 GB RAID 1+0, RAID 5. 1 TB RAID 1+0, RAID 5, si Oracle está en el mismo servidor.	200 GB SCSI Para Network Discover 150 MB extra para mantener los incremental scans indexes.
NIC.	1 GB/100 Mb, para comunicarse a los detection servers.	1 GB/100 Mb, para comunicarse al Enforce Server.

Figura 28 Requerimientos de hardware para el Servidor Windows 2008 R2.

Procesador Core I3 o superior, 4 GB en RAM, 500 GB Disco Duro, tarjeta de red 10/100/1000 MBps.

Figura 29 Características Técnicas de los Servidores Endforce y EndPoint.

El software que se requiere para llevar a cabo la implementación depende del número de empleados que tiene la compañía.

Módulo de Symantec DLP	Componente de Symantec DLP	Tipo de Licenciamiento
Endpoint.	Endpoint Prevent.	Licenciamiento por total de equipos cliente con Agente Instalado.
Endpoint.	Endpoint Discover	Licenciamiento por total de equipos cliente con Agente Instalado.

4.2.2 Software DLP.

200 licencias de Symantec endpoint protect

200 licenciad de Symantec endpoint disocver

4.3 Diseño y Alcances de la implementación DLP

Especificación a nivel más detallado la arquitectura para implantar la solución Symantec DLP.

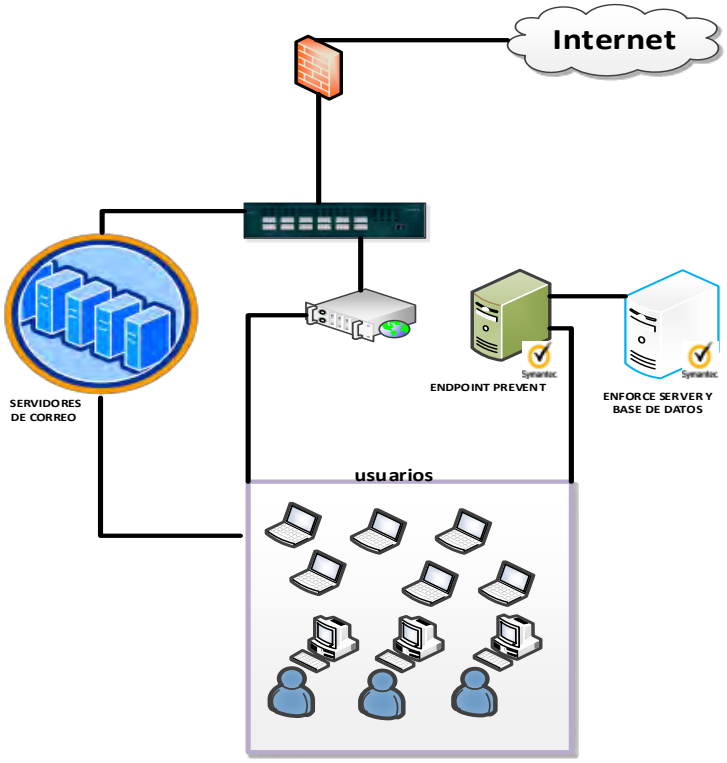


Figura 30 Esquema del Diseño de un Agente DLP.

En esta etapa solo se tienen contemplados los módulos de Endpoint Discover y Protect de Symantec Data Loss prevention.

Capítulo 5

IMPLEMENTACIÓN DE DLP.

5.1 Instalación de los módulos de DLP.

Este capítulo contempla la instalación y puesta a punto de la solución de Symantec DLP (Implementación de la base de Datos Oracle, Enforce Server, Endpoint Server, instalación de agentes y las políticas).

Para la implementación del Servidor perimetral se realizará los siguientes procedimientos generales.

1. Instalación y Configuración del Servidor (Windows Server 2008 R2).
2. Instalación y Configuración de la herramienta EndForce.
3. Instalación y Configuración de la herramienta EndPoint.
4. Instalación y Configuración del Agente.
5. Pruebas de Funcionalidad del sistema.

Son requeridos servidores para la instalación de los componentes de Symantec DLP, los cuales los deberán ser entregados por la compañía con el sistema operativo instalado y activado, nombres de equipo definidos, configuración de red definitiva, conexiones físicas realizadas y acceso remoto habilitado.

5.2 Configuración del Agente

Es necesario que la compañía proporcione acceso a una herramienta de distribución de software o directorio activo para distribución de agentes. Opcionalmente esta instalación puede ser manual; Además debe proporcionar el listado de equipos a los que se les instalará el agente de Symantec DLP.

Nota: Los equipos a los cuales se instalará el agente de Endpoint deben cumplir con los requerimientos y disponibilidad para la instalación definidos (ver capítulo 4.2).

5.2.1 Creación de paquetes de instalación.

Symantec DLP 12.5 ofrece una característica adicional en la creación de paquetes de instalación de agentes de Endpoint, para lo cual se describe el siguiente procedimiento.

Iniciar sesión a través de la consola de administración de DLP con privilegios de Administrador.

Ir al menú System>Agents>Agent Packaging.

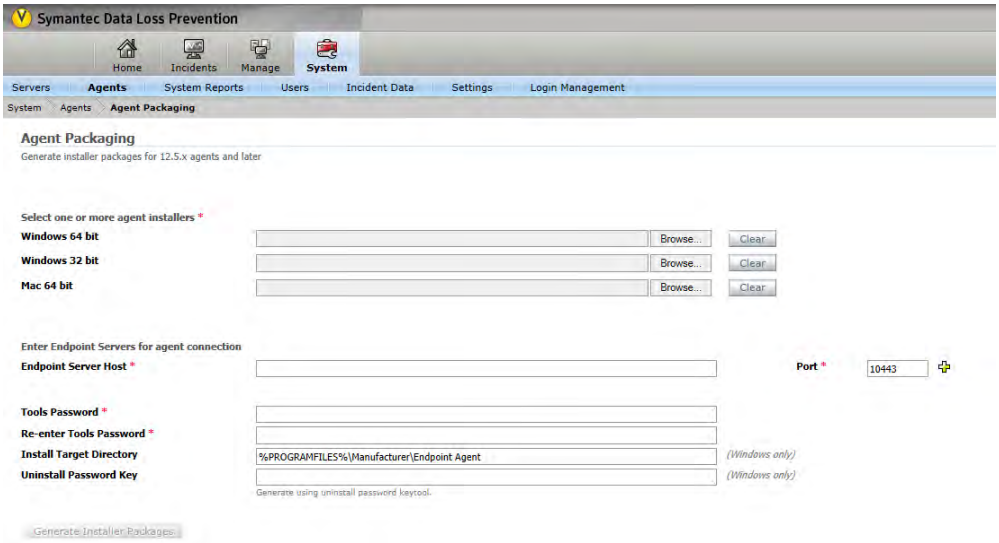
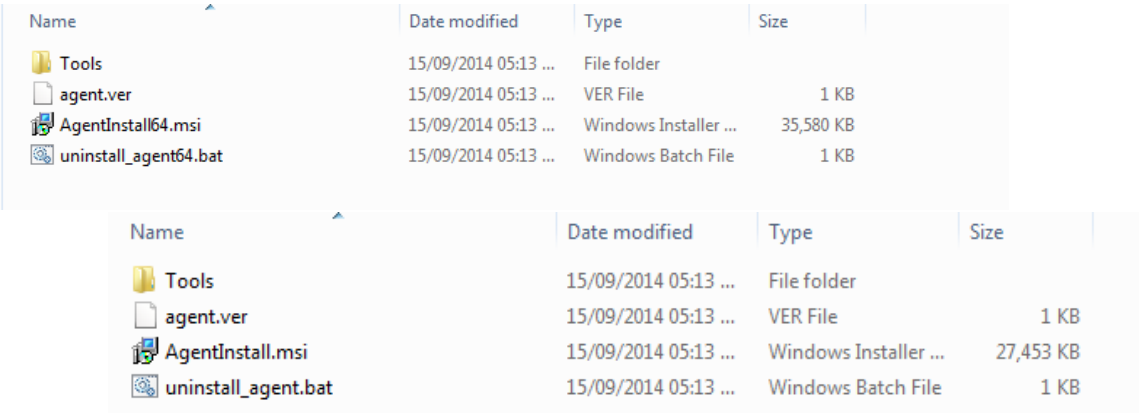


Figura 31 Generación de paquete del agente DLP.

Una vez mostrada la ventana es necesario especificar los archivos “msi” de instalación de 32 y 64 bits que previamente fueron descargados del portal de software de Symantec. Dar clic en examinar en la arquitectura especifica e ir a la carpeta donde se encuentra el instalador del agente de Symantec DLP y seleccionar el archivo AgentInstall64.msi/AgentInstall.msi.



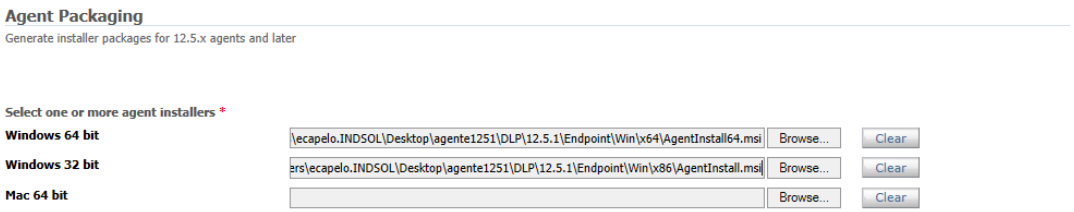


Figura 32 Generación de paquete del agente DLP.

En la sección Enter Endpoint Servers for agent connection introducir las configuraciones del servidor que administrará a los agentes de Endpoint.

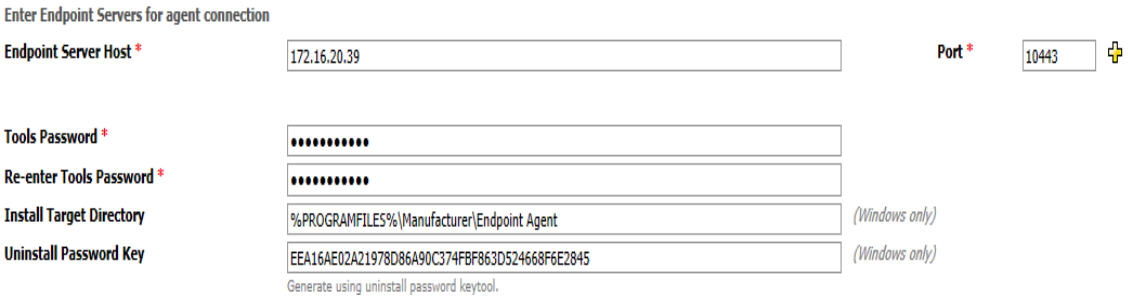


Figura 33 Generación de paquete del agente DLP.

Dónde:

Endpoint Server Host: Se especifica la dirección IP o nombre del servidor de Endpoint.

Port: Se especifica el puerto de comunicación entre el agente de Endpoint y Endpoint Server, por default “10443”.

Tolos Password: Password de acceso a las herramientas de soporte una vez que el agente este instalado en el equipo cliente.

Install Target Directory: Ruta de instalación del agente de Endpoit.

• UNINSTALLPASSWORDKEY: Es el password de desinstalación del agente de DLP generado por UninstallPwdKeyGenerator.exe, pero para lograr desinstalar el agente, es necesario especificar el valor real y no el binario generado por la herramienta.

• Estos ajustes se realizarán para x86 y x64 de los agentes de DLP.

Para generar los paquetes de instalación con las configuraciones antes especificadas es necesario dar clic sobre el botón “Generate Install Packages”. La herramienta generará los archivos y al concluir será mostrada la opción de descarga a través del navegador web y seleccionar la ruta de almacenamiento.

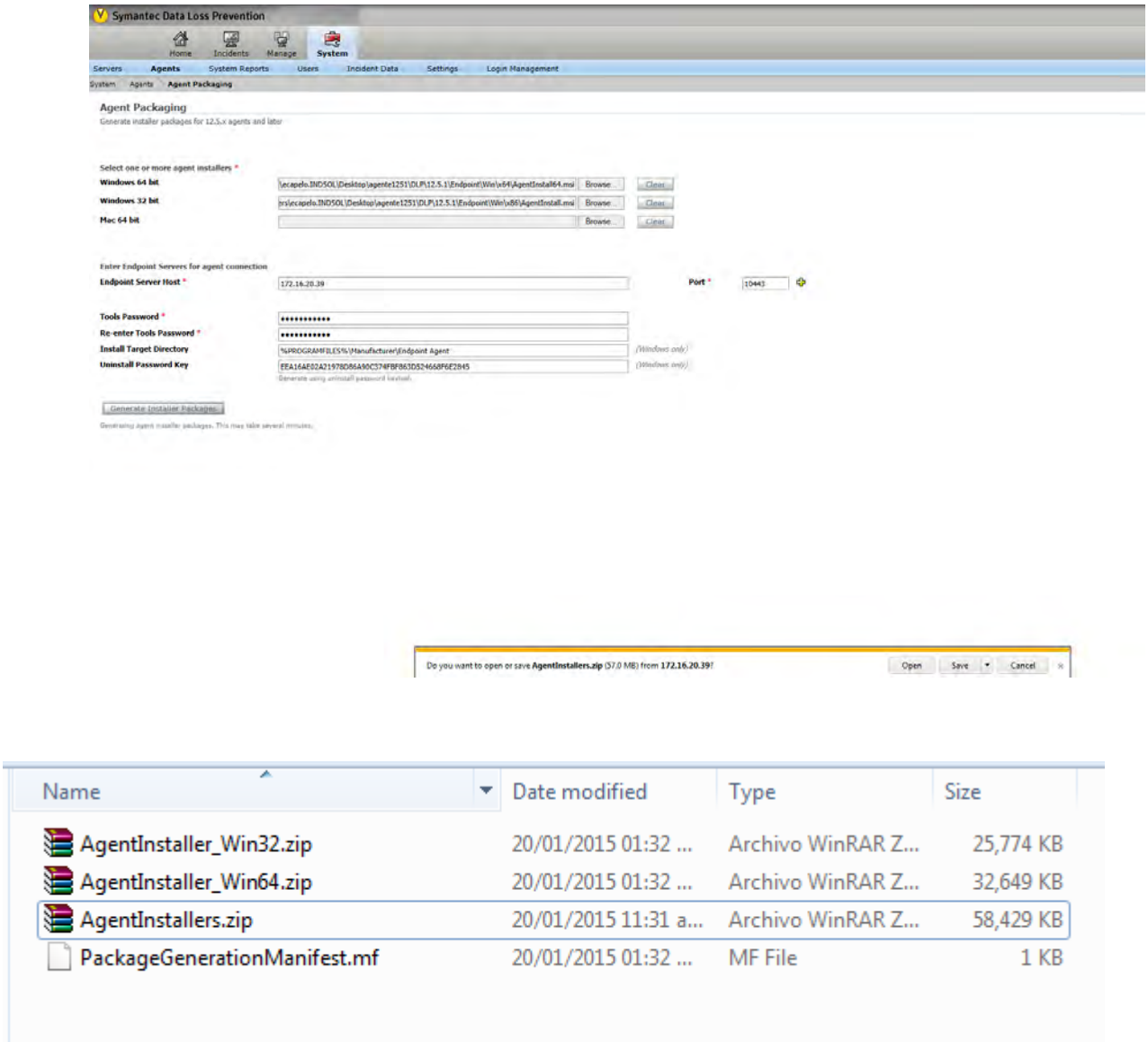


Figura 34 Generación de paquete del agente DLP.

5.2.2 Instalación del Agente DLP:

Para la instalación de los agentes en los clientes con sistema operativo Windows soportado, es necesario ejecutar el archivo install_agent64.bat / install_agent.bat dependiendo de la arquitectura de equipo cliente.

Para clientes con sistema operativo Windows 7 o Windows 8, es necesario ejecutar el archivo con privilegios de administrador.

Ejecutar el archivo install_agent64.bat / install_agent.bat con privilegios de Administrador

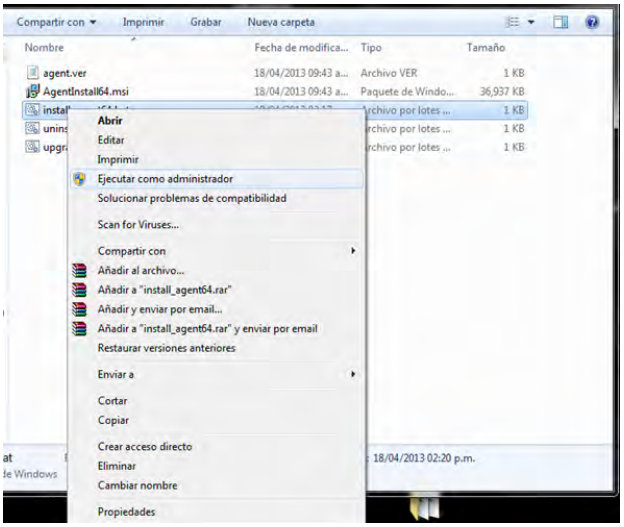


Figura 35 Instalación del agente DLP.

Una pantalla cmd de desinstalación será mostrada, en la cual se muestra la configuración especificada en el archivo bat, esta acción puede tardar aproximadamente 5 minutos.

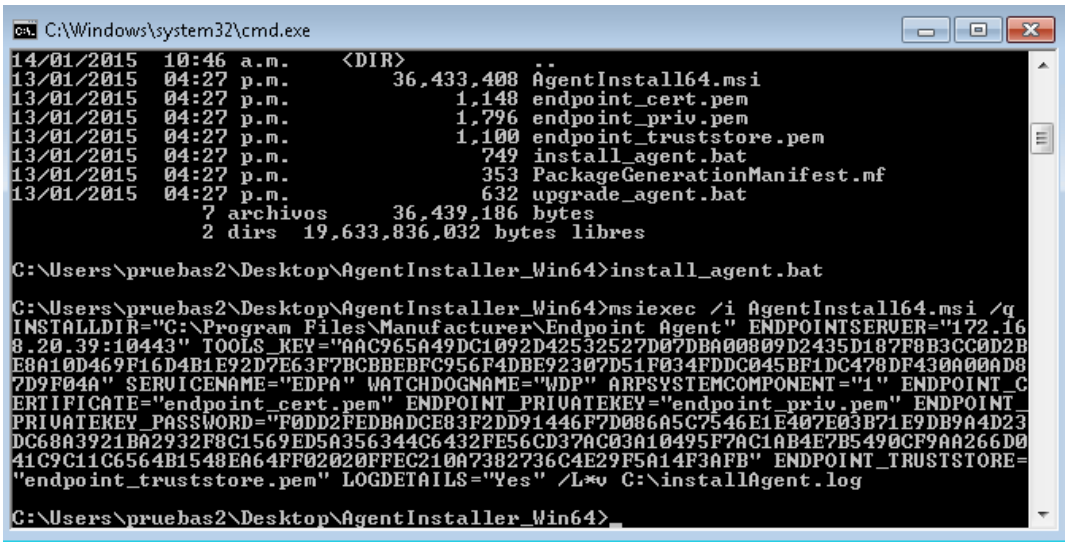


Figura 36 Instalación del agente DLP.

Al finalizar la instalación, la ventana de cmd se cerrará automáticamente y solo es necesario verificar que los servicios, en este caso EDPA y WDP estén de forma automática e iniciados. Así como los procesos edpa y wdp.

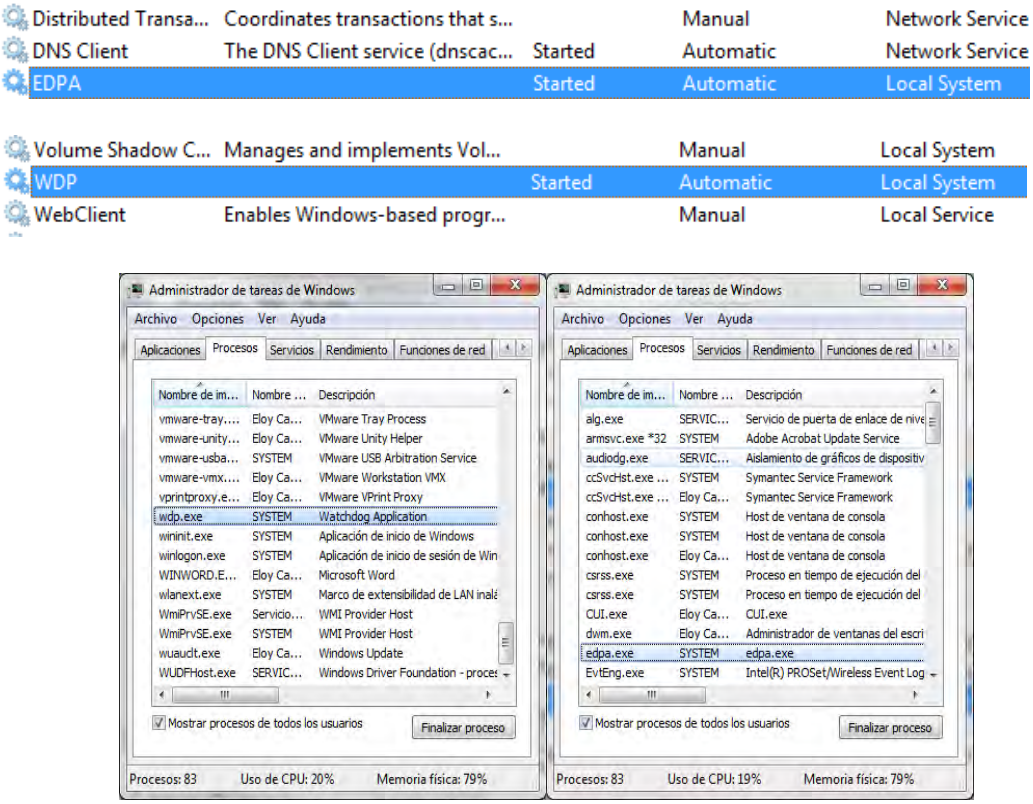


Figura 37 Instalación del agente DLP.

5.2.3 Desinstalación del Agente de DLP.

Para la desinstalación es necesario tener accedo al archivo uninstall_agent64.bat/ uninstall_agent.bat, por medio del cual podemos sacar la siguiente línea:

msiexec /uninstall {9967A8CA-E48C-4AE9-99C8-6A48AF57669A}

Comando que podemos especificar en un Ejecutar y de esta manera ver la interfaz de la desinstalación del agente, en la cual debemos especificar el password original para la desinstalación

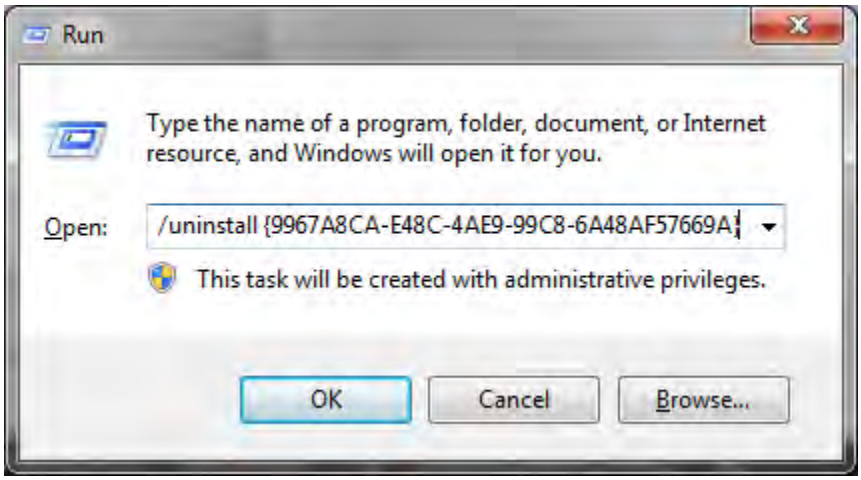


Figura 38 Desinstalación del agente DLP.

Al ejecutar la línea, será mostrada una ventana de confirmación donde se pregunta si se está seguro de desinstalar el producto, para completar la acción, se presiona el botón Sí,

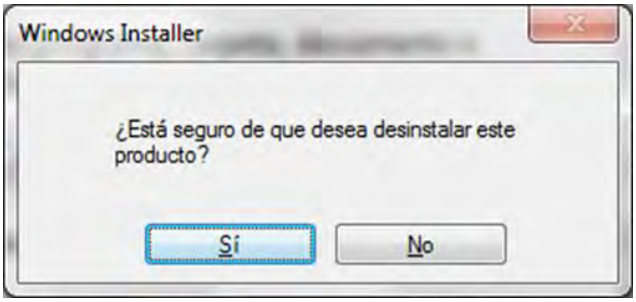


Figura 39 Desinstalación del agente DLP.

El proceso de desinstalación comenzará

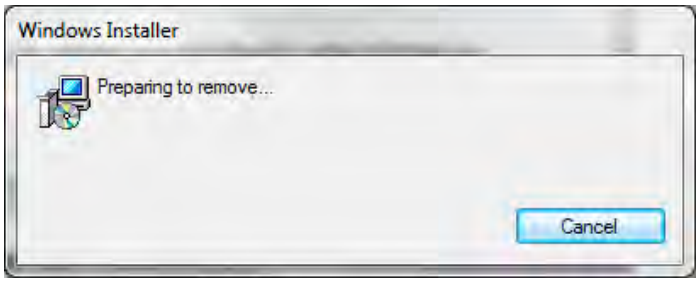


Figura 40 Desinstalación del agente DLP.

Durante el proceso de desinstalación se indicará que ingresemos el password de desinstalación el cual es: **********

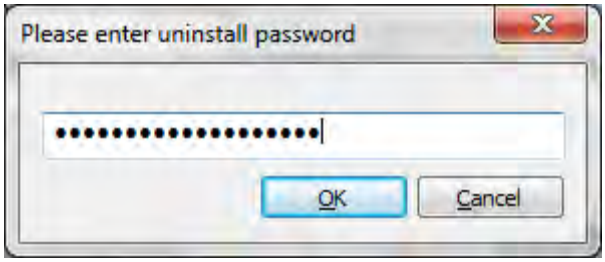


Figura 41 Desinstalación del agente DLP.

El proceso de desinstalación continuará

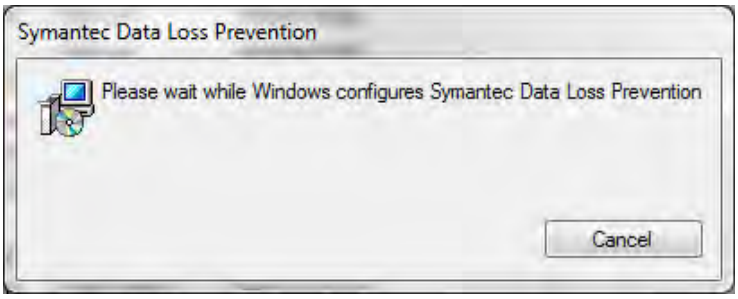


Figura 42 Desinstalación del agente DLP.

Al finalizar, es conveniente verificar que la ruta de instalación y servicios se hayan eliminado.

5.3 Pruebas de Funcionalidad.

El objetivo de realizar estas pruebas es garantizar el correcto funcionamiento y detección de incidentes por medio de los agentes instalados de Endpoint Prevent.

El esquema de la prueba es el siguiente:

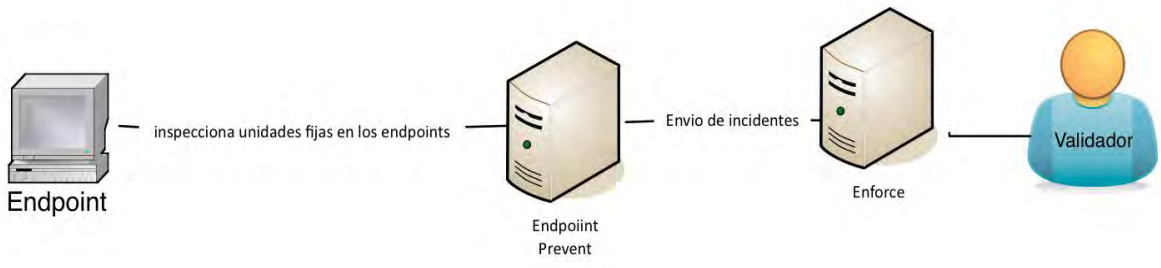


Figura 43 Esquema de pruebas

Prueba 1.

Detección en HTTPS

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes en el protocolo Web HTTPS
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave o expresiones regulares.
	2. Escribir un mensaje que contenga información confidencial y enviarlo desde un correo electrónico WEB que utilice cifrado HTTPS.
	3. Verificar el correcto envío del correo electrónico.
	4. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent.
	1. Symantec DLP detecta y reporta el incidente.
Resultados esperados	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 2

Detección en unidades extraíbles con Endpoint Prevent.

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes por parte de Endpoint Prevent en medios extraíbles al copiar o guardar información confidencial.
Pasos a seguir	1. Crear una política de prueba que detecte una expresión regular de RFCs ó Números de Tarjeta de Crédito.
	2. Crear y copiar un archivo a un dispositivo extraíble que contenga información confidencial de RFC´s ó Números de tarjeta de Crédito.
	3. Verificar que el archivo se transfirió correctamente.
	4. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint.
Resultados esperados	1. Symantec DLP detecta y reporta el incidente.
	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 3.

Prueba de detección de impresión con Endpoint Prevent.

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes por parte de Endpoint Prevent en la impresión de documentos.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave o expresiones regulares.
	2. Crear un archivo de texto (Por ejemplo, utilizando Microsoft Word ó PDF) y en él escribir las palabras configuradas en la política de prueba
	3. Mandar a impresión el documento.
	4. Verificar la correcta impresión del archivo.
	5. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent.
Resultados esperados	1. Symantec DLP detecta y reporta el incidente.
	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 4.

Prueba de detección de portapapeles con Endpoint Prevent.

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes por parte de Endpoint Prevent al copiar información de un archivo.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave ó expresiones regulares.
	2. Crear un archivo de texto (Por ejemplo, utilizando Microsoft Word) y en él escribir las palabras configuradas en la política de prueba.
	3. Cortar o copiar la totalidad o una parte del archivo
	4. Verificar el correcto copiado o cortado del archivo pegándolo en un archivo diferente.
	5. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent.
Resultados esperados	1. Symantec DLP detecta y reporta el incidente.
	2. Las palabras copiadas o cortadas configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 5.

Prueba de detección en Offline con Endpoint Prevent.

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes cuando el equipo es desconectado de la red corporativa por parte de Endpoint Prevent
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave ó expresiones regulares.
	2. Crear un archivo de texto (Word, PDF) y en él escribir información que sea detectada por la política de prueba.
	3. Desconectar el equipo con el agente de Endpoint de la red corporativa.
	4. Guardar el archivo de texto en una unidad extraíble USB.
	5. Verificar el correcto almacenamiento del archivo.
	6. Conectar el equipo con el agente de Endpoint a la red corporativa.
	7. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent.
Resultados esperados	1. Symantec DLP detecta y reporta el incidente.
	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 6

Prueba de detección de archivos comprimidos.

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes en archivos comprimidos.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave.
	2. Crear un archivo de texto (Microsoft Word, PDF) y en él escribir las palabras configuradas en la política de prueba.
	3. Comprimir el archivo utilizando el formato zip o rar.
	4. Adjuntar el archivo utilizando una cuenta de correo público que utilice http ó https (por ejemplo, Yahoo).
	5. Verificar el correcto envío del correo electrónico.
	6. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent.
Resultados esperados	1. Symantec DLP detecta y reporta el incidente.
	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 7

Prueba de bloqueo con Endpoint Prevent.

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la funcionalidad de bloqueo de fuga de información confidencial en Endpoint Prevent.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave ó expresiones regulares.
	2. Anadir una regla de bloqueo de fuga de información confidencial.
	3. Enviar un correo electrónico que en él cuerpo del mensaje escribir las palabras ó expresiones configuradas en la política de prueba.
	4. Verificar que aparezca la ventana de bloqueo y que el archivo no se envió.
	6. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent.
	1. Symantec DLP detecta y reporta el incidente
Resultados esperados	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 8

Prueba de Notificación para Endpoint.

Descripción de la prueba	Esta prueba tiene la finalidad de mostrar en la pantalla del usuario una Advertencia al intentar enviar información confidencial.
Pasos a seguir	1. Crear una política de prueba que detecte un listado de palabras clave o una expresión regular.
	2. Crear y añadir una regla de respuesta de notificación para Endpoint.
	3. Enviar un correo electrónico que contenga información que sea detectada por la política de prueba.
	4. Verificar que la ventana de advertencia de fuga de información aparezca en pantalla al intentar enviar el correo electrónico.
	6. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent
	1. Symantec DLP detecta y reporta el incidente.
Resultados esperados	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

Prueba 9

Prueba de detección de información confidencial en mensajería instantánea soportada (Messenger, Yahoo Messenger, AIM)

Descripción de la prueba	Esta prueba tiene la finalidad de comprobar la correcta captura de incidentes al detectar envío de información confidencial en mensajería instantánea.
Pasos a seguir	1. Crear una política de prueba que detecte información confidencial (listado de palabras ó expresión regular)
	2. Enviar un archivo que contenga información confidencial, utilizando una aplicación de mensajería instantánea soportada.
	3. Verificar el correcto envío del archivo.
	4. Verificar la correcta detección de los incidentes a través del reporte Incidents all de Endpoint Prevent
Resultados esperados	1. Symantec DLP detecta y reporta el incidente.
	2. Todas las palabras configuradas en la política de prueba aparecen identificadas en el detalle del incidente.
	3. La detección del incidente se realiza con prontitud en la consola.
Resultados obtenidos	

5.4 Implementación de Políticas.

Esta etapa se contempla la configuración de políticas de detección y prevención que serán aplicadas en la consola de Administración de Symantec DLP.

Se deberá haber cubierto todos los puntos de los capítulos (5.1, 5.2, 5.3) de la Implementación de Symantec DLP; Además se deberá proporcionar el diseño lógico de las políticas a implementar en la solución de Symantec DLP.

Se implementan políticas para detectar y evitar pérdida de datos. Una política integra mecanismos de detección y respuesta. Si se viola una o más reglas de una política, el sistema genera un evento el cual es nombrado como un incidente que puede informar y sobre el cual puede podemos tomar acciones.

Las políticas que se implementan se basan en los objetivos de seguridad de la información. Las acciones que toma en respuesta a la violación de las políticas se basan en los requisitos de cumplimiento definidos. Actualmente la compañía tiene 3 bases de datos en las cuales se encuentran almacenada la información más importante para el giro del negocio.

Base de datos 1

En esta base de datos se encuentra almacenados la siguiente información de todos los empleados, nombre del empleado, tarjetas de nómina, tarjetas de crédito.

Base de datos 2.

En esta base de datos se encuentran los siguientes campos de todos los empleados.

Nombre del empleado, edad, Dirección, teléfono, CURP.

Base de datos 3

En esta base de datos se encuentran almacenada la siguiente información de todos los clientes.

Nombre del cliente, edad, Dirección, teléfono, CURP, RFC.

Cabe mencionar que la información solo puede ser manipulada o generada solo por su área, la base de datos 1 pertenece a Nomina, base de datos 2 pertenece a Recursos Humanos y la base de datos 3 pertenece a Ventas, el resto de la compañía por ningún motivo puede hacer uso de la información antes mencionada, el uso de indebido de la información será consignada por el representante de área.

Para realizar la detección de información sensible

RFC

[a-zA-Z][aeiouAEIOU][a-zA-Z]{2}\d{2}((0[13578]|1[02])(0[1-9]|[12]\d|3[0-1])|(0[469]|11)(0[1-9]|[1-2]\d|30)|02(0[1-9]|1\d|2[1-9]))(\w{3})?

CURP

(?i)([a-z][aeiou][a-z]{2}\d{2}((0[13578]|1[02])(0[1-9]|[12]\d|3[0-1])|(0[469]|11)(0[1-9]|[1-2]\d|30)|02(0[1-9]|1\d|2[1-9]))[hm][a-z]{2}[^aeiou\d]{3}\d{2})

Tarjetas de crédito

^((67\d{2})|(4\d{3})|(5[1-5]\d{2})|(6011))(-?\s?\d{4}){3}|(3[4,7])\d{2}-?\s?\d{6}-?\s?\d{5}$

5.5 Ajustes y Mantenimiento.

La revisión de los servidores de DLP es necesaria para la comprobación del buen funcionamiento de la solución, así como el arreglo de fallas básicas. La Revisión de salud de los servidores se realiza desde la plataforma Enforce DLP (Consola DLP), los pasos a seguir son los siguientes:

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 44 Revisión de la salud de los servidores DLP.

Una vez que ingresamos a la consola de DLP, ir a System > Overview.

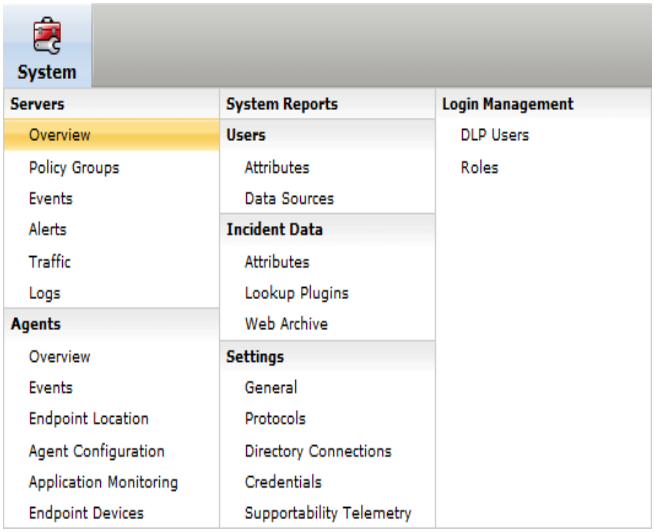


Figura 45 Revisión de la salud de los servidores DLP.

La siguiente ventana muestra los servidores instalados que son parte de la solución de Symantec DLP (Servidor Enforce y Servidores de Detección) y el estado general de los mismos. Se debe revisar que todos ellos muestren el estado “Running”, como en la imagen siguiente.

Servers

Status	Server	Version	Channels
Running	Enforce Server	12.0.1.01064	N/A
Running	Endpoint Discover	12.0.1.01064	Endpoint
Running	Endpoint Prevent	12.0.1.01064	Endpoint
Running	Network Discover	12.0.1.01064	Network Discover
Running	Network Monitor 1	12.0.1.01064	Network Monitor

Figura 46 Revisión de la salud de los servidores DLP.

Revisión de la salud de los servicios en el Servidor Enforce.

Servicio	Descripción
Vontu Manager	Provee los servicios de administración y reportes centralizados para Symantec Data Loss Prevention.
Vontu Monitor Controller	Controla los servidores de detección.
Vontu Notifier	Provee notificaciones de base de datos.
Vontu Incident Persister	Escribe los incidentes a la Base de Datos.
Vontu Update	Instala las actualizaciones del sistema. Sólo se usa cuando se están haciendo actualizaciones.

Figura 47 Revisión de la salud de los servidores DLP.

Ingresar mediante Escritorio Remoto al Servidor Enforce.

Figura 48 Revisión de la salud de servidor Enforce.

Presionar el botón Start y escribir en el campo de búsqueda: services.msc. Posteriormente hacer clic sobre el programa que aparece (services.msc).

Figura 49 Revisión de la salud de servidor Enforce.

Buscar cada uno de los servicios siguientes: Vontu Manager, Vontu Monitor Controller, Vontu Notifier, Vontu Incident Persister, Vontu Update. El estado de cada uno de estos servicios debe reportarse como "Started" bajo la columna "Status" para garantizar que la solución funcione. En la imagen siguiente se muestran los servicios tal y como deben aparecer en el servidor Enforce de la Suprema Corte de Justicia de la Nación.

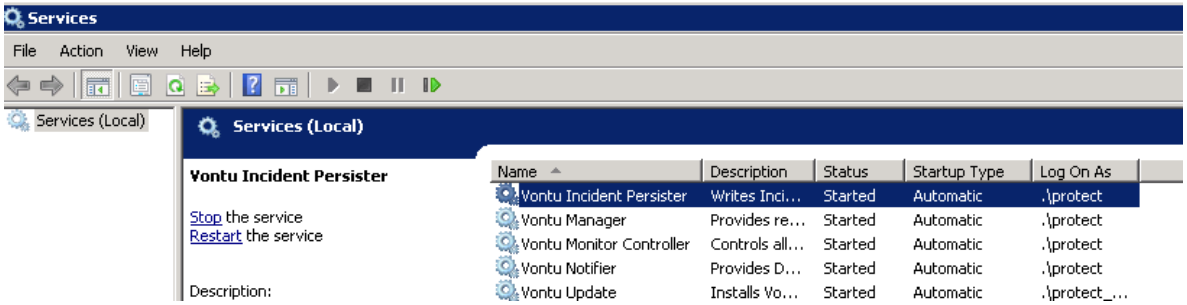


Figura 50 Revisión de la salud de servidor Enforce.

Servicios DLP de los Servidores de Detección.

Servicio	Descripción
Vontu Monitor	Exclusivo en los servidores de detección.
Vontu Update	Instala las actualizaciones del sistema. Sólo se usa cuando se están haciendo actualizaciones.

Ingresar mediante Escritorio Remoto al Servidor de Detección por revisar.

Figura 51 Revisión de la salud de servidor Detección.

Presionar el botón Start y escribir en el campo de búsqueda: services.msc. Posteriormente hacer clic sobre el programa que aparece (services.msc)

Figura 52 Revisión de la salud de servidor Detección.

Buscar cada uno de los servicios siguientes: Vontu Monitor y Vontu Update. El estado de cada uno de estos servicios debe reportarse como “Started” bajo la columna “Status” para garantizar que la solución funcione. En la imagen siguiente se muestran los servicios tal y cómo deben aparecer en un servidor de Detección de la Suprema Corte de Justicia de la Nación.

Resolución de Problemas básicos.

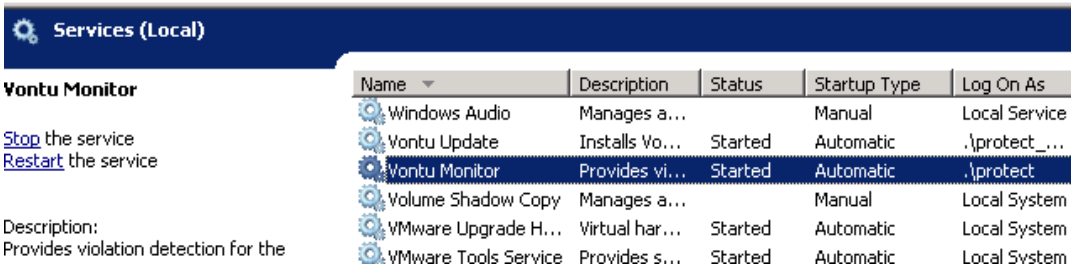


Figura 53 Revisión de la salud de servidor Detección.

Apagar los servicios de Symantec Data Loss Prevention en Windows.

En el sistema que tiene la base de datos, ir a Start > All Programs > Administrative Tools > Services

Detener todos los servicios de Symantec DLP, en el siguiente orden:

Vontu Update

Vontu Incident Persister
Vontu Manager
Vontu Monitor (en servidores de detección)
Vontu Notifier

Para finalizar, detener el Servicio OracleService PROTECT

Reiniciar los servicios de Symantec Data Loss Prevention en Windows.

En la computadora que tiene la Base de Datos, ir a Start > All Programs > Administrative Tools > Services. Del menú de servicios, iniciar todos los servicios de Oracle:

OracleServicePROTECT
OracleDBConsoleprotect
Iniciar el servicio VontuNotifier.

Posteriormente, iniciar los demás servicios en el siguiente orden:

Vontu Manager
Vontu Monitor (en servidores de detección)
Vontu Incident Persister
Vontu Update
Monitor Controller

No. Actividad	Problema	Solución
1	Uno o más servicios no están iniciados.	Se deberá dar clic derecho sobre el servicio en cuestión y seleccionar “Start”. Se espera a que el servicio inicie.
2	Los servicios no responden al reinicio manual.	Se intenta iniciar los servicios a través de la Consola Enforce (Ver apartado “Revisión de la salud de los servidores desde la plataforma Enforce DLP (Consola DLP)”).
3	Los servicios no responden a las soluciones anteriores.	Se reinicia el servidor por completo.

Capítulo 6

DOCUMENTACIÓN Y RESULTADOS.

En este capítulo se describen las configuraciones que se llevaron a cabo durante el proceso de implementación de Symantec DLP.

6.1 Documentación de instalación sistema Symantec DLP.

A continuación, se muestra paso a paso como se lleva a cabo la instalación y la configuración de la solución de Symantec DLP, comenzaremos con la instalación de la base de datos y la consola de administración (Enforce server).

Instalación de Oracle 11g, Paso 1:

- Detener los servicios de Oracle> **Distributed Transaction Coordinator service**

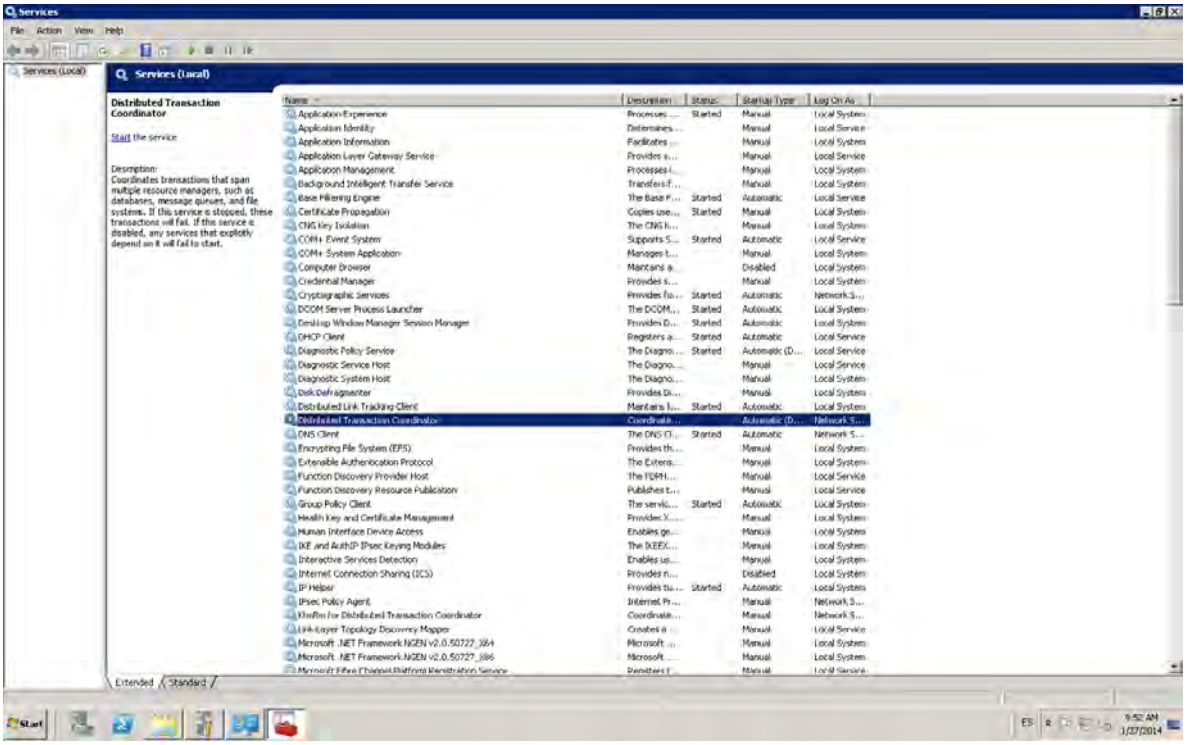


Figura 54 Configuración de Oracle.

Instalación de Oracle 11g, Paso 2:

Se descomprimen los archivos para instalar la base de datos

- Oracle_11.2.0.3.0_Server_Win64_1of2
- Oracle_11.2.0.3.0_Server_Win64_2of2

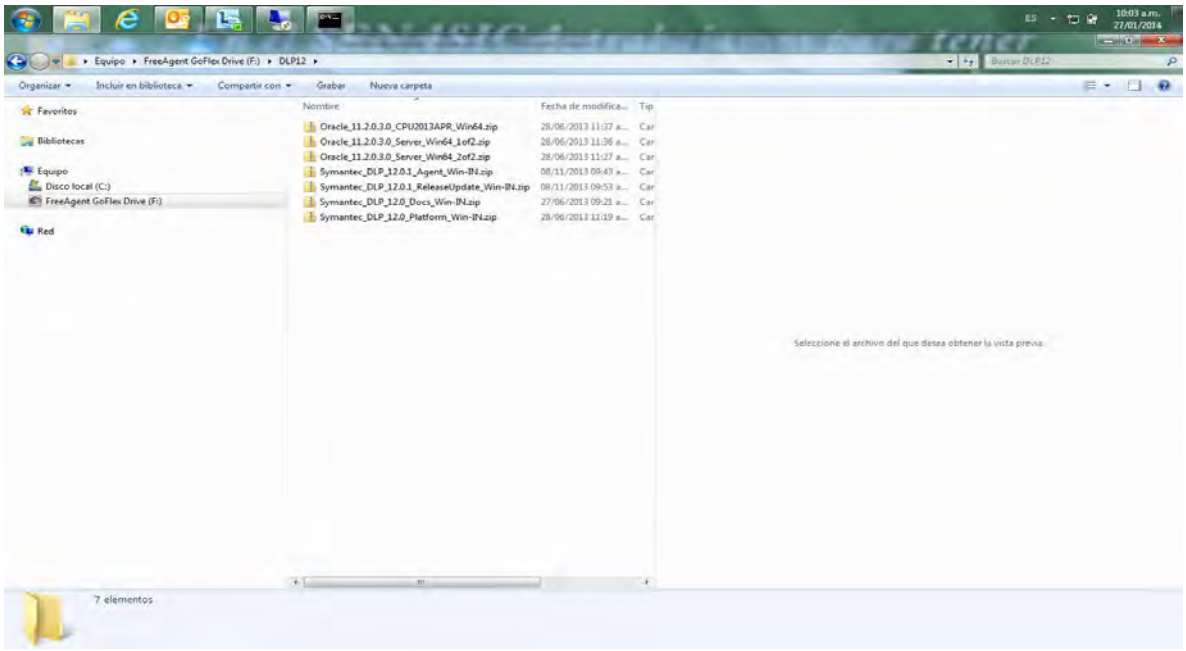


Figura 55 Configuración de Oracle.

Instalación de Oracle 11g, Paso 3:

Se ejecuta el archivo (setup) instalador de Oracle.

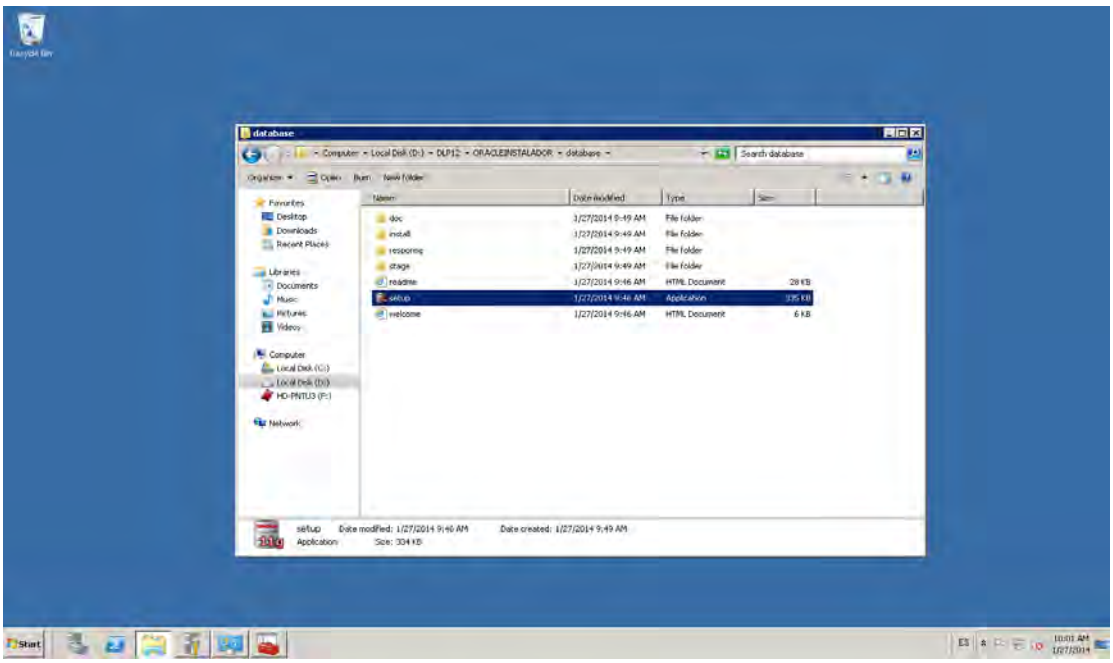


Figura 56 Configuración de Oracle.

Aparecerá en pantalla el asistente de instalación de Oracle 11g.

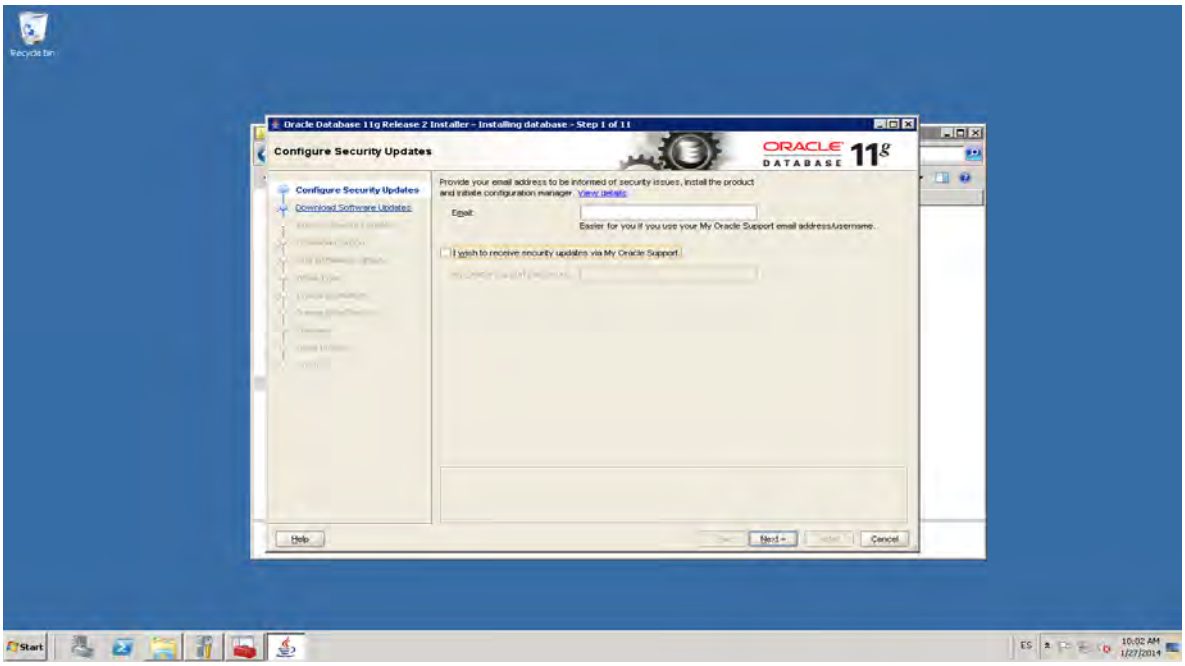


Figura 57 Configuración de Oracle.

Instalación de Oracle 11g, Paso 5:

***Nota**: Si no se desea recibir actualizaciones realiza la siguiente acción; En la notificación indica que no se proporcionado ninguna dirección de correo electrónico para recibir información. De clic en "Si" para continuar.*

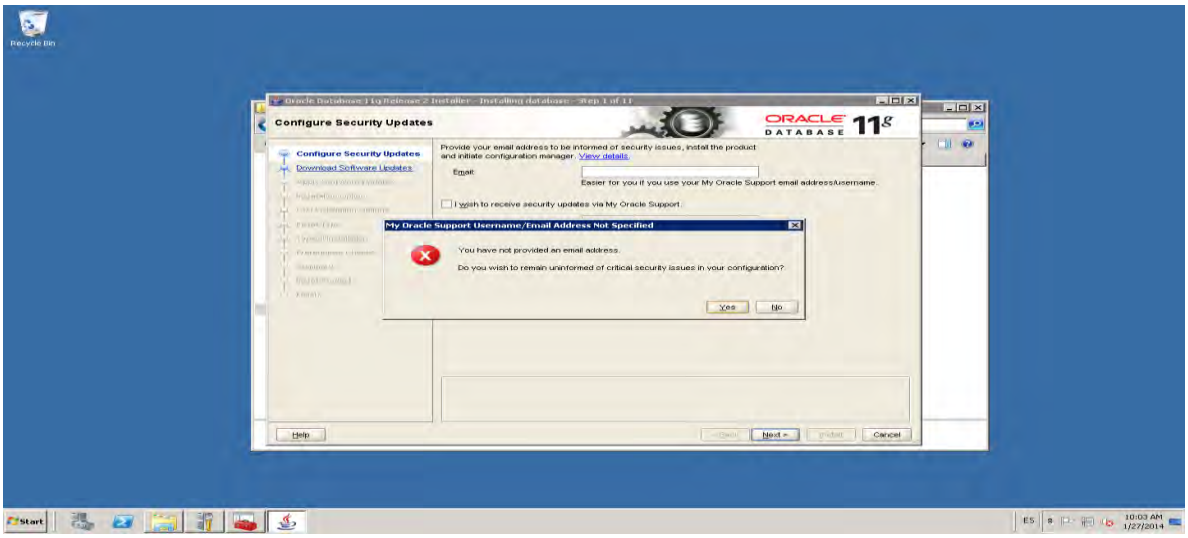


Figura 58 Configuración de Oracle.

Instalación de Oracle 11g, Paso 6:

Seleccione la opción “omitir actualizaciones de software”.

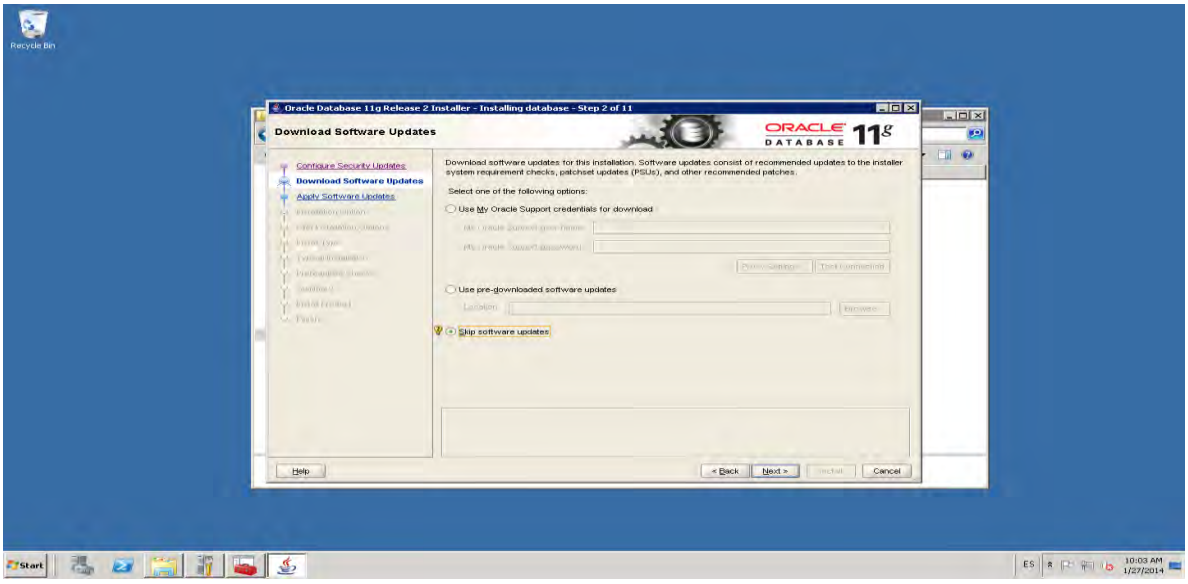


Figura 59 Configuración de Oracle.

Instalación de Oracle 11g, Paso 7:

Parche para Oracle.

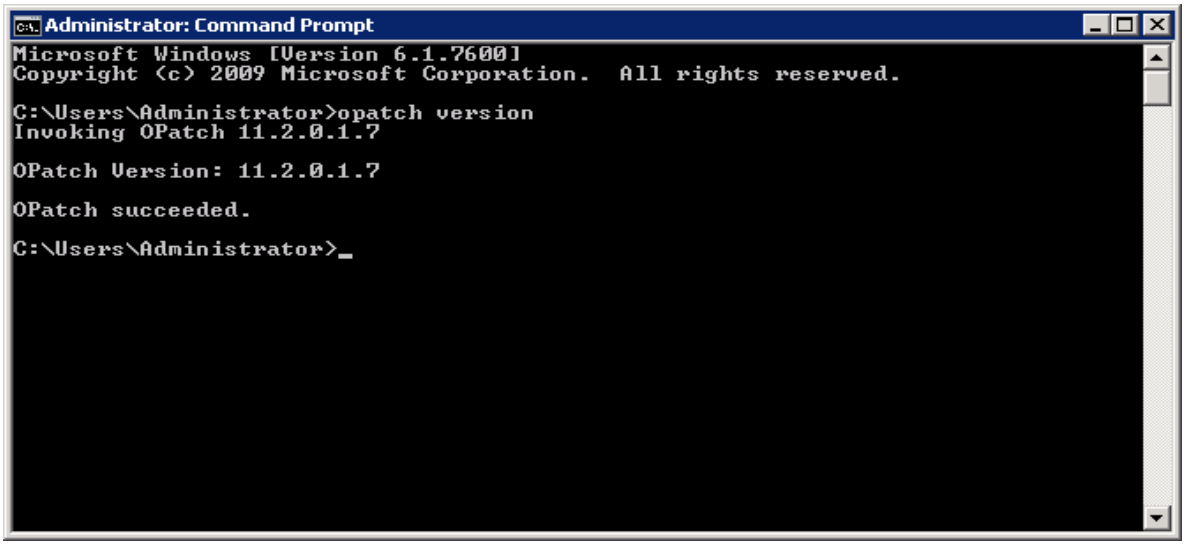


Figura 60 Configuración de Oracle.

Instalación de Oracle 11g, Paso 8:

Únicamente se desea instalar la base de datos, por ello seleccione “Instalar solo software de base de datos”, de clic siguiente.

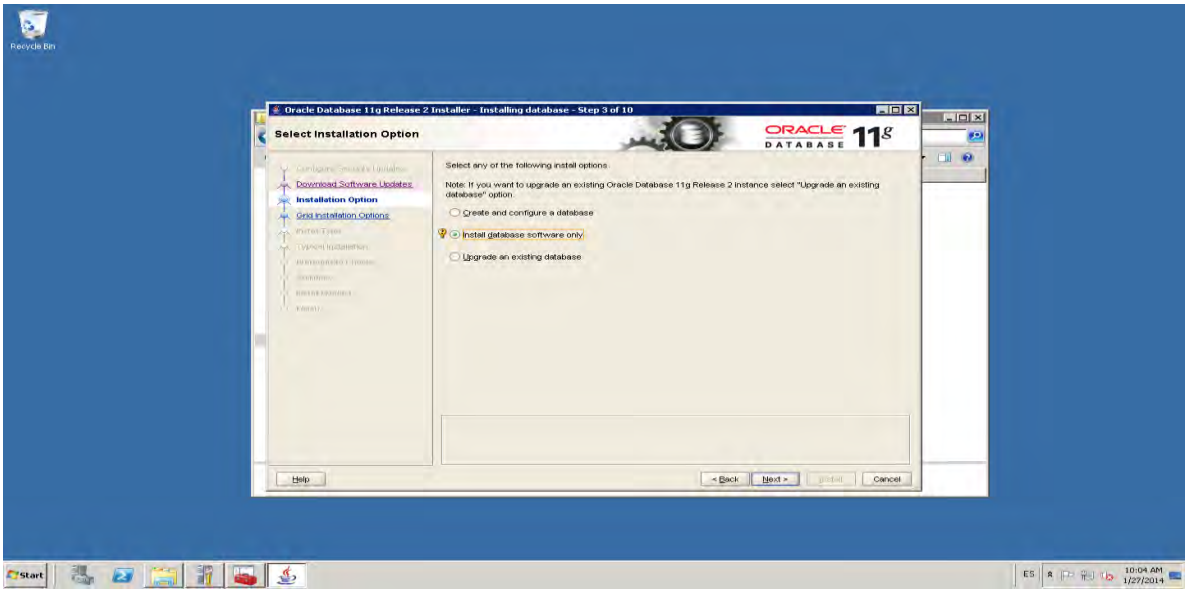


Figura 61 Configuración de Oracle.

Instalación de Oracle 11g, Paso 9:

Seleccione “Instancia única”, puesto que solo se necesita una para Symantec DLP.

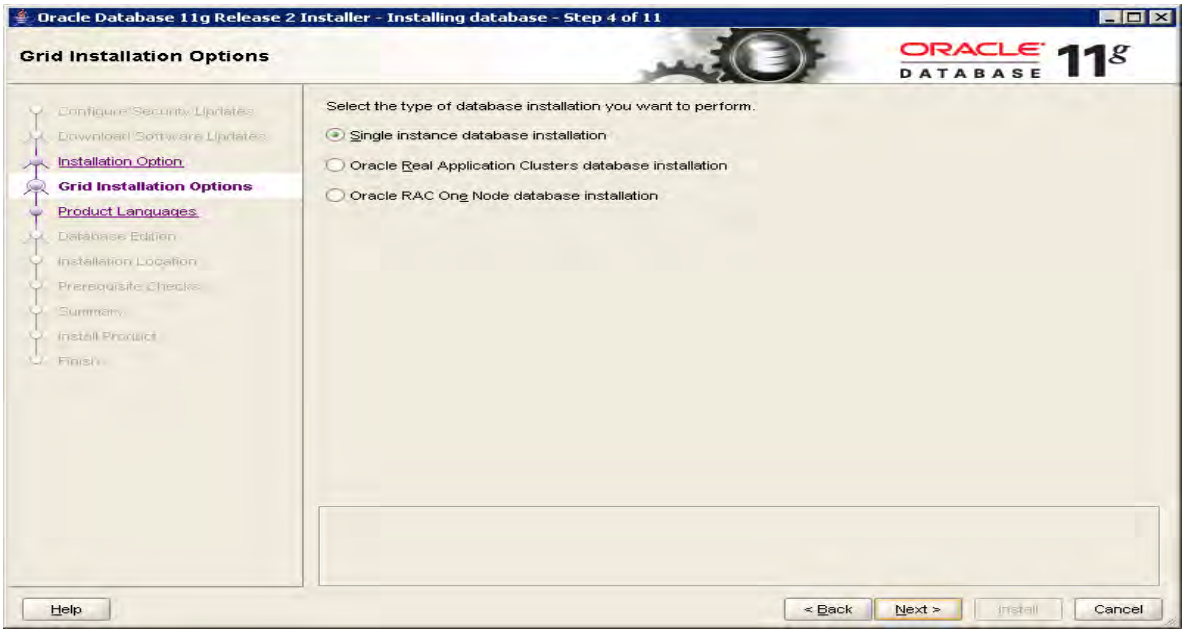


Figura 62 Configuración de Oracle.

Instalación de Oracle 11g, Paso 10:

Únicamente seleccionar idioma inglés, por recomendaciones del fabricante.

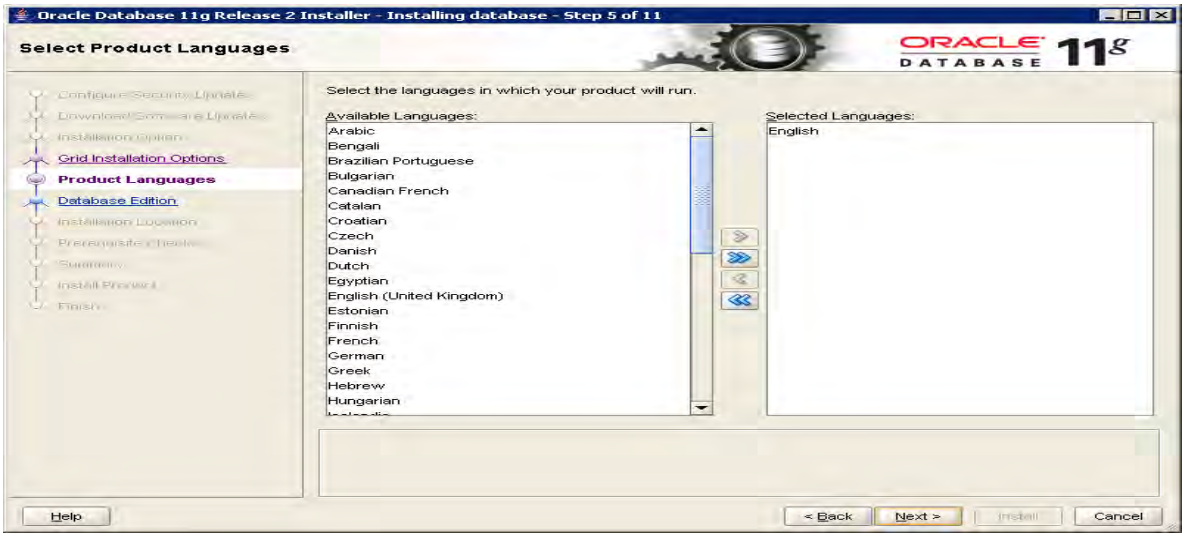


Figura 63 Instalación de Oracle.

Instalación de Oracle 11g, Paso 11:

Por recomendación del fabricante seleccione “Estándar Edition”.

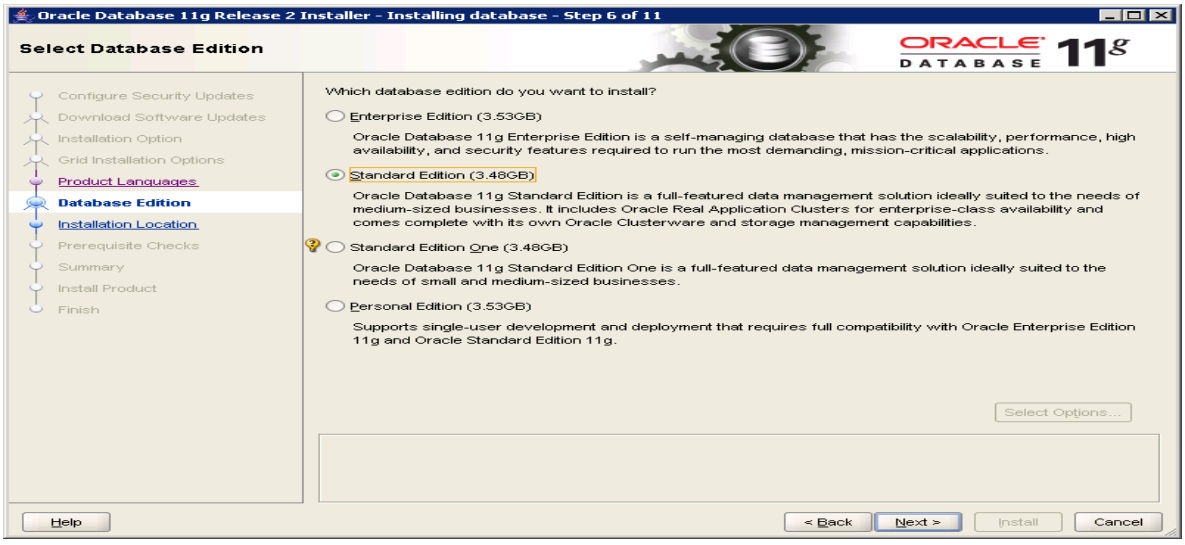


Figura 64 Instalación de Oracle.

Instalación de Oracle 11g, Paso 12:

Especifique las rutas de instalación para la base de datos.

- Directorio de Base de Datos: D:\oracle
- Ubicación del software: D:\oracle\product\11.2.0.3\db_1.

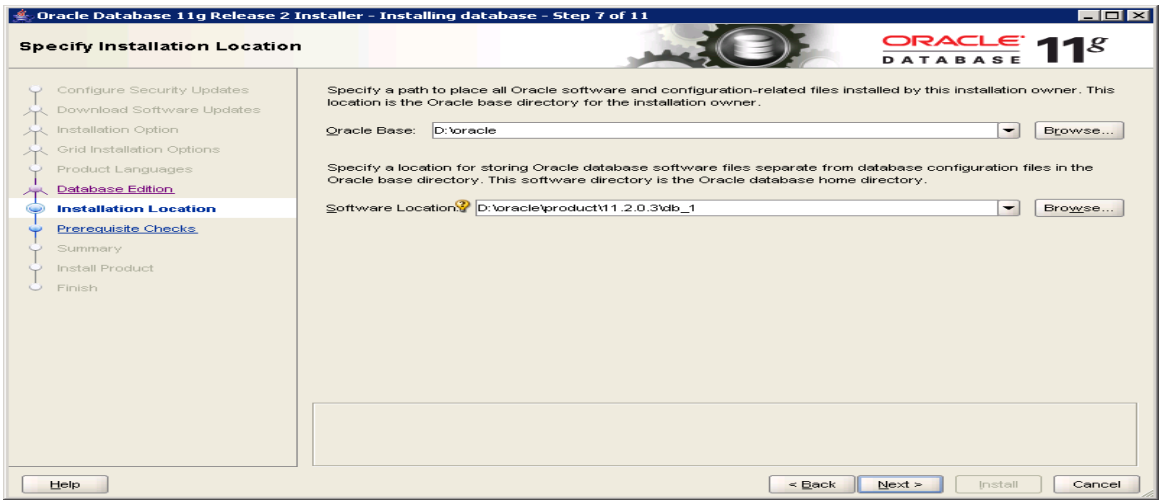


Figura 65 Instalación de Oracle.

Instalación de Oracle 11g, Paso 13:

En la siguiente pantalla se ejecuta la instalación de Oracle 11g.

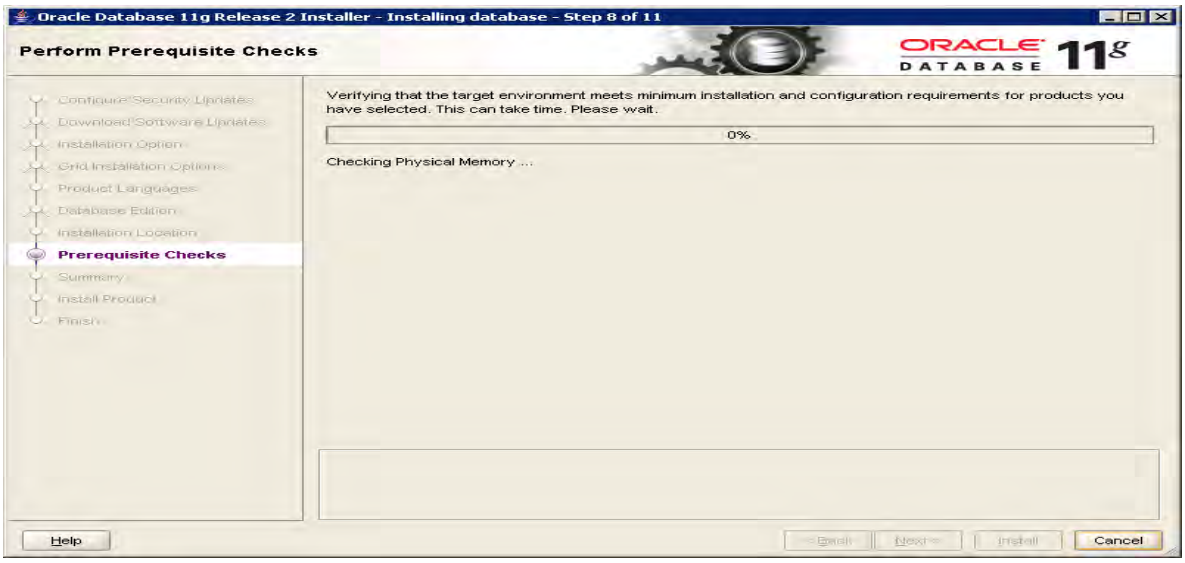


Figura 66 Instalación de Oracle.

Instalación de Oracle 11g, Paso 14:

En la siguiente pantalla se da clic para instalar.

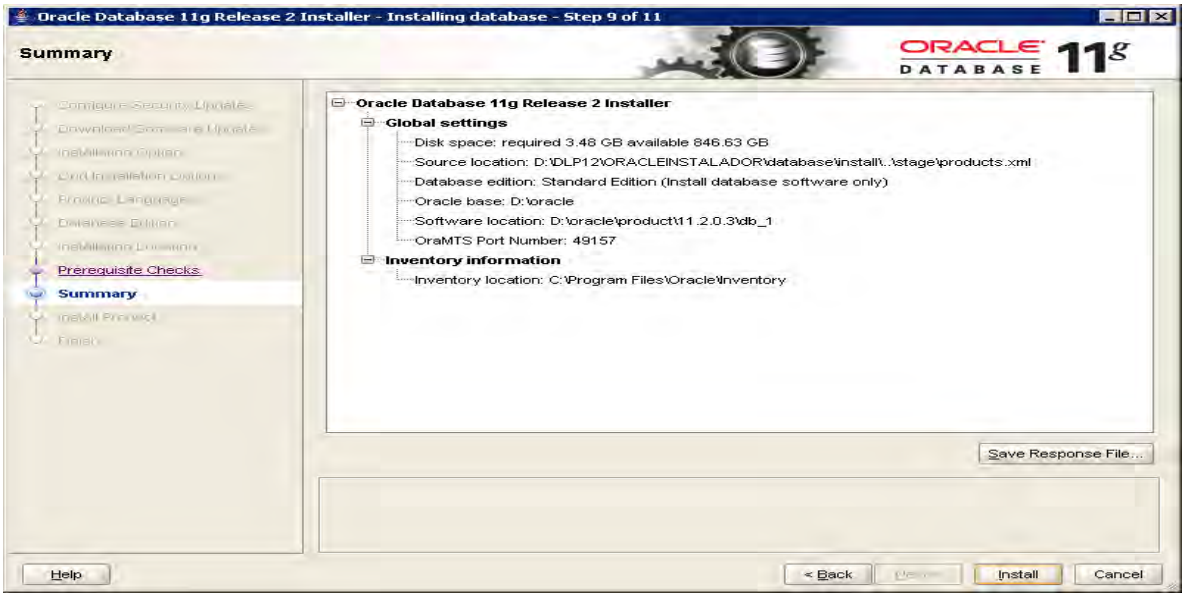


Figura 67 Instalación de Oracle.

Instalación de Oracle 11g, Paso 15:

En la siguiente pantalla se muestra es proceso de instalación.

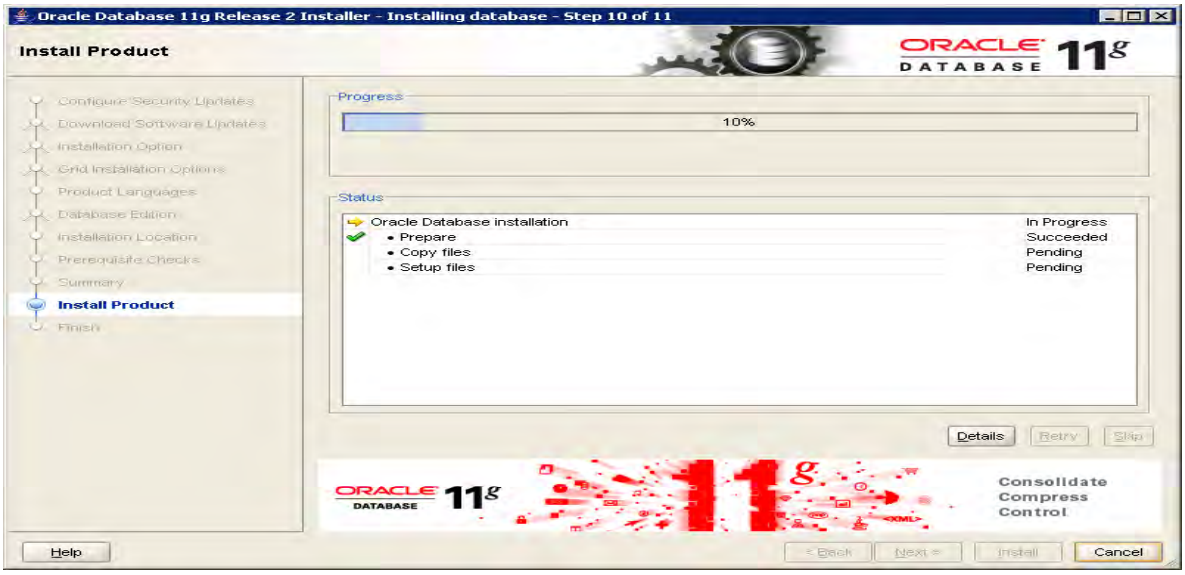


Figura 68 Instalación de Oracle.

Instalación de Oracle 11g, Paso 16:

Al terminar la instalación presionamos “Cancel” para continuar con la configuración.

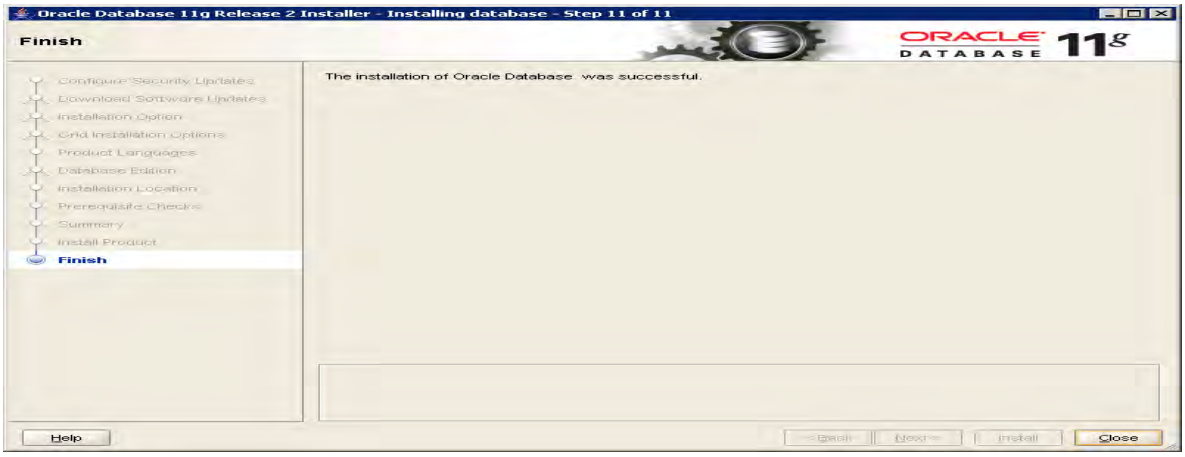


Figura 69 Instalación de Oracle.

Configuración de Oracle 11G

Configuración de Oracle 11g, Paso 1:

Variables de Entorno ORACLE_HOME

Se necesita declarar dos variables las cuales harán referencia al directorio raíz de Oracle.

Variables de usuario y del sistema

- ORACLE_HOME
- D:\oracle\product\11.2.0.3\db_1

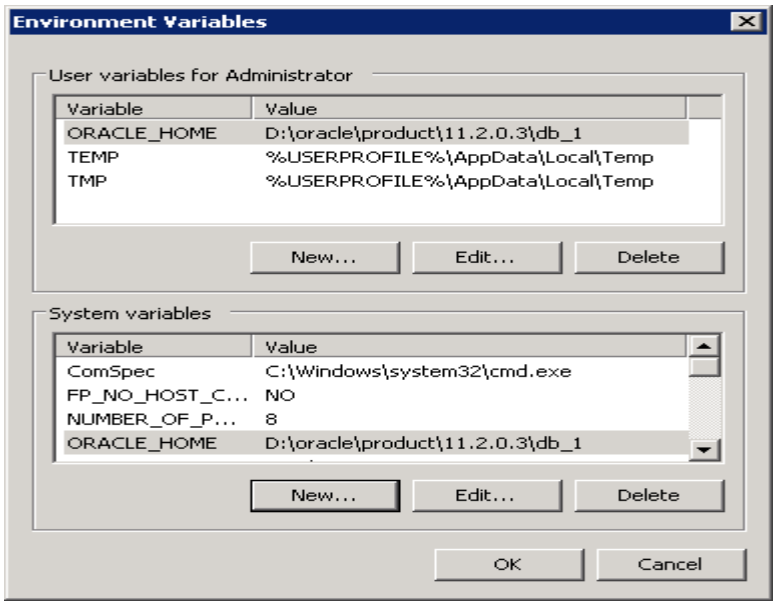


Figura 70 Configuración de variables de entorno de Oracle.

Configuración de Oracle 11g, Paso 2:

Se ejecuta Oracle_11g_Database_for_vontu_v12

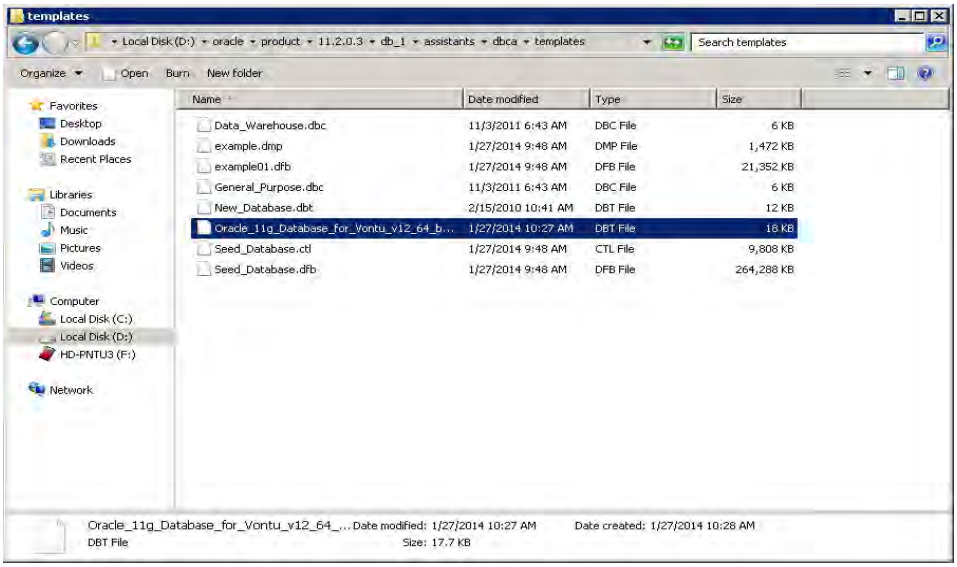


Figura 71 Selección de del template BD de Symantec.

Configuración de Oracle 11g, Paso 3:

Asistente de configuración de la base de datos, da clic en “Next”.

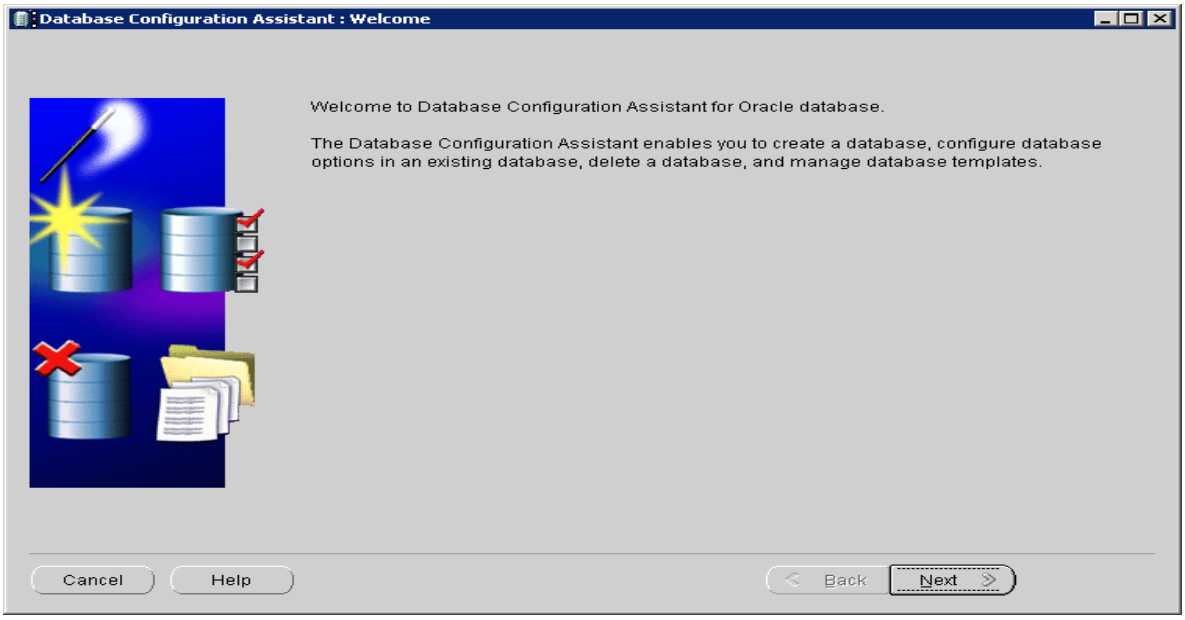


Figura 72 Selección del template BD de Symantec.

Configuración de Oracle 11g, Paso 4:

Seleccionamos la opción crear base de datos, clic en “Next”.

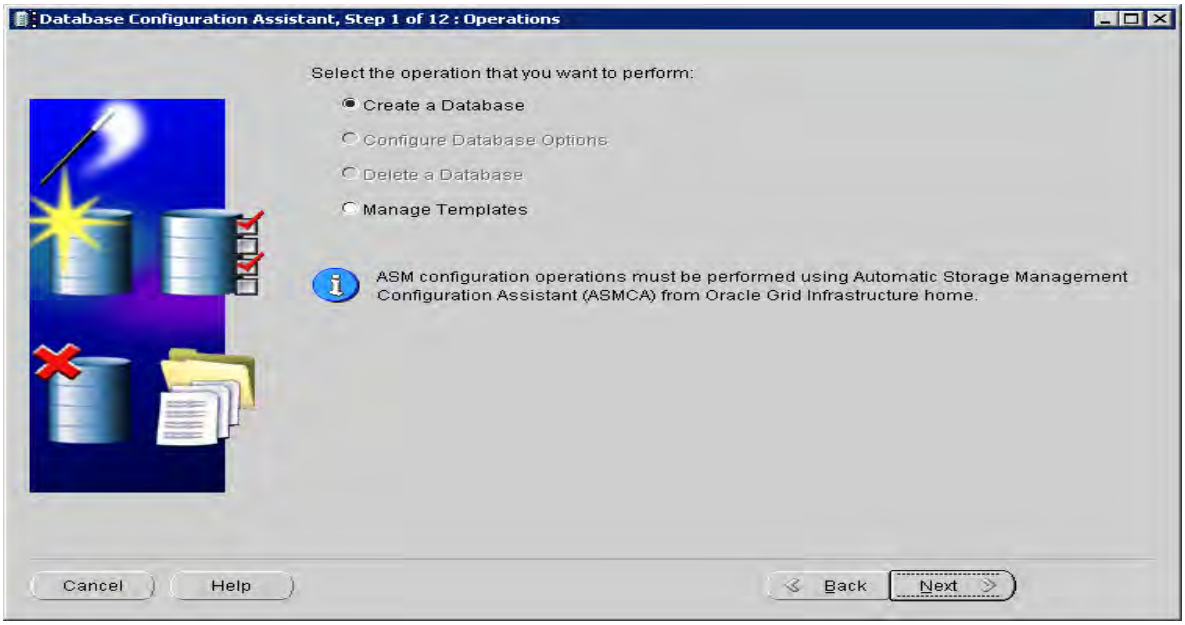


Figura 73 Instalación BD de Symantec.

Configuración de Oracle 11g, Paso 5:

Selecciona “Oracle 11g database for Vuntu v12 64 bits “, da clic en “Next”.

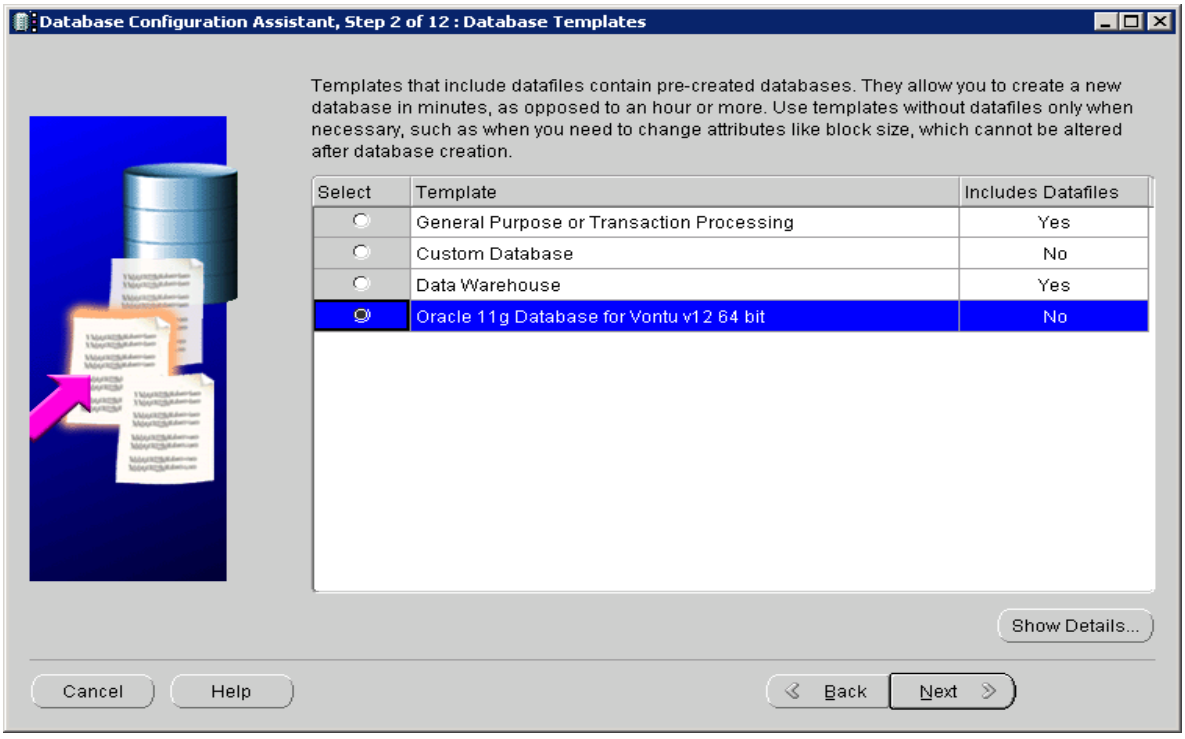


Figura 74 Selección del template BD de Symantec.

Configuración de Oracle 11g, Paso 6:

Se asignar un nombre para identificar la base de datos, se da clic en “Next”

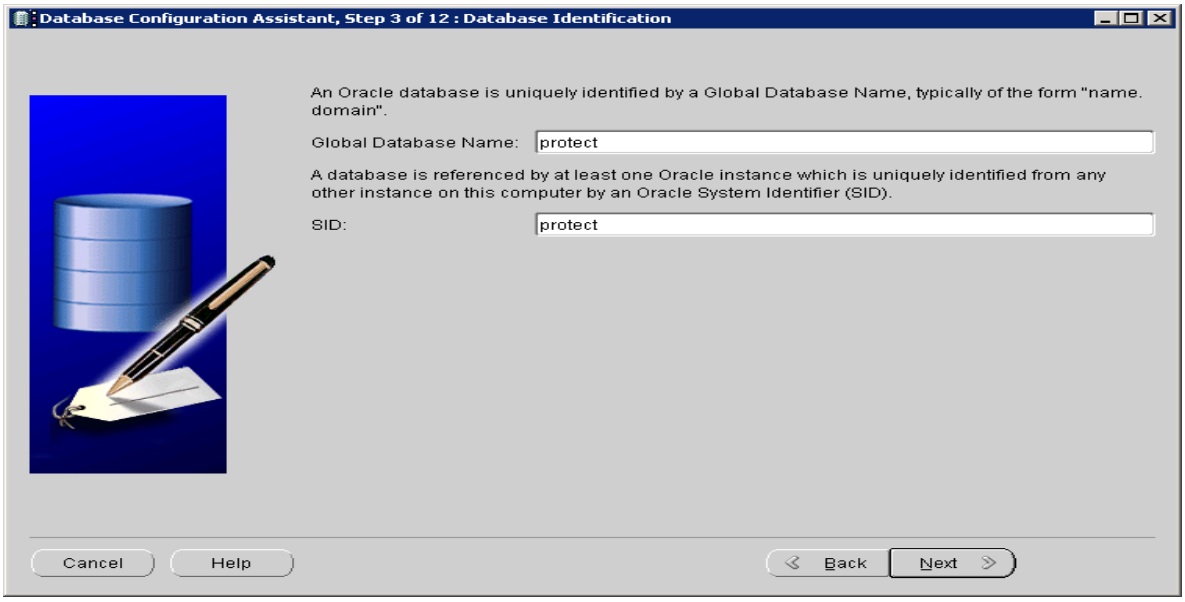


Figura 75 Nombre de la BD de Symantec.

Configuración de Oracle 11g, Paso 7:

En la sección “Enterprise Manager”, da clic “Next”:

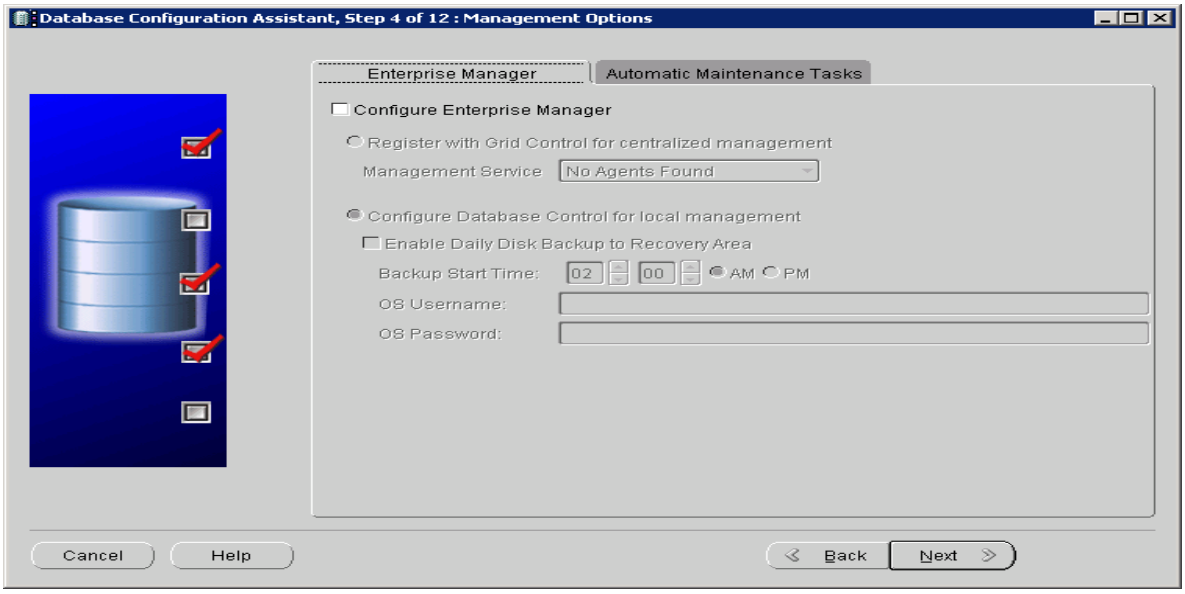


Figura 76 Configuración de BD de Symantec.

Configuración de Oracle 11g, Paso 8:

En la sección “tareas de mantenimiento automáticas”, da clic “Next”:

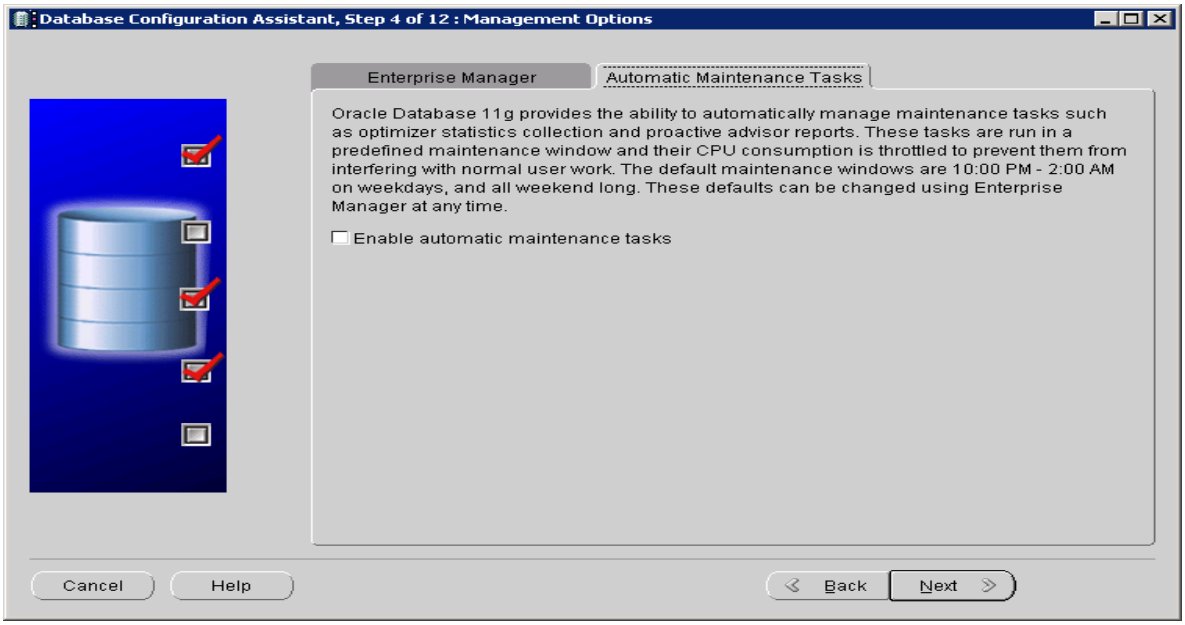


Figura 77 Configuración de BD de Symantec.

Configuración de Oracle 11g, Paso 8:

Define la contraseña para la cuenta del usuario de la base de datos, utilizando el método “usar la misma contraseña administrativa”.

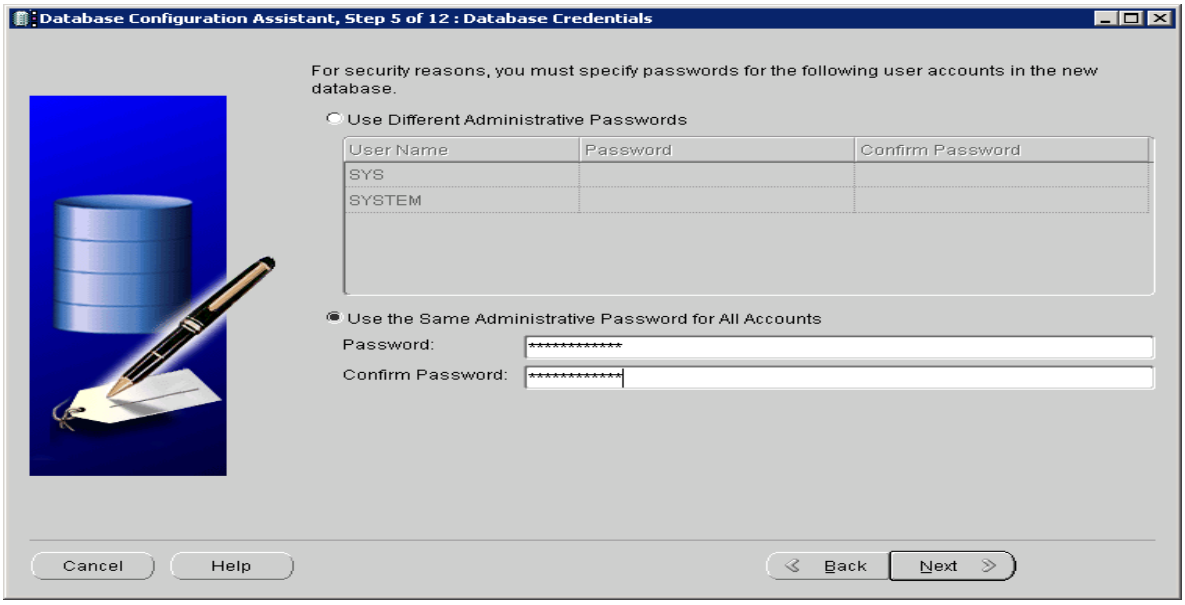


Figura 78 Configuración de BD de Symantec.

Configuración de Oracle 11g, Paso 9:

Este paso seleccione “usar ubicación de archivo de base de datos de la plantilla”, da clic en “finish”

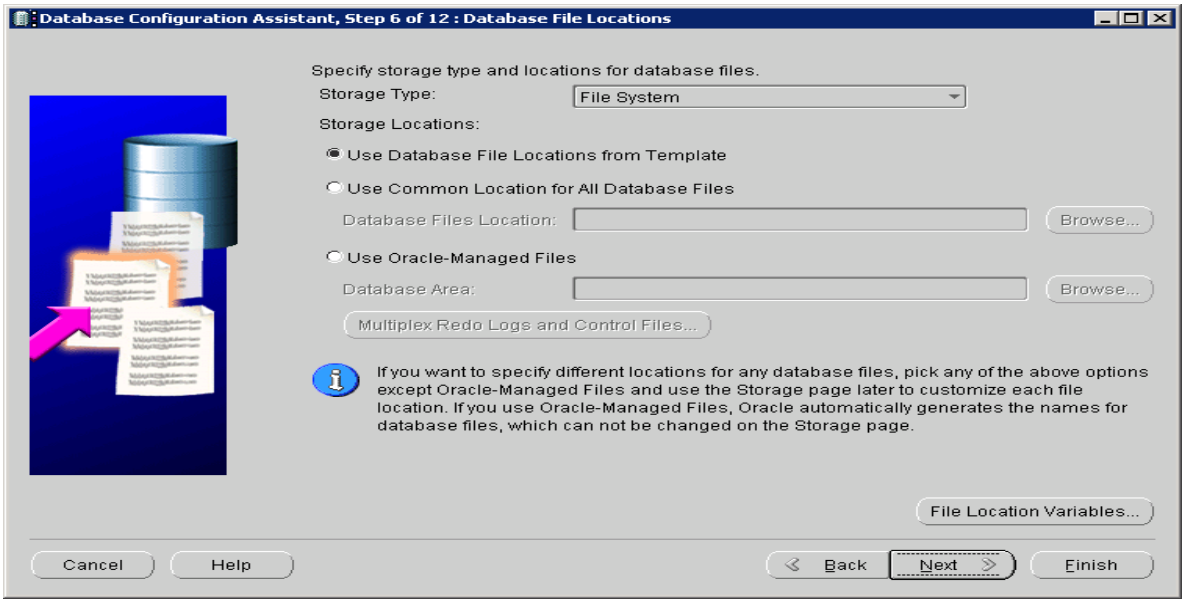


Figura 79 Configuración de BD de Symantec.

Configuración de Oracle 11g, Paso 10:

Se confirmar los detalles de la base de datos para iniciar la configuración de la aplicación.

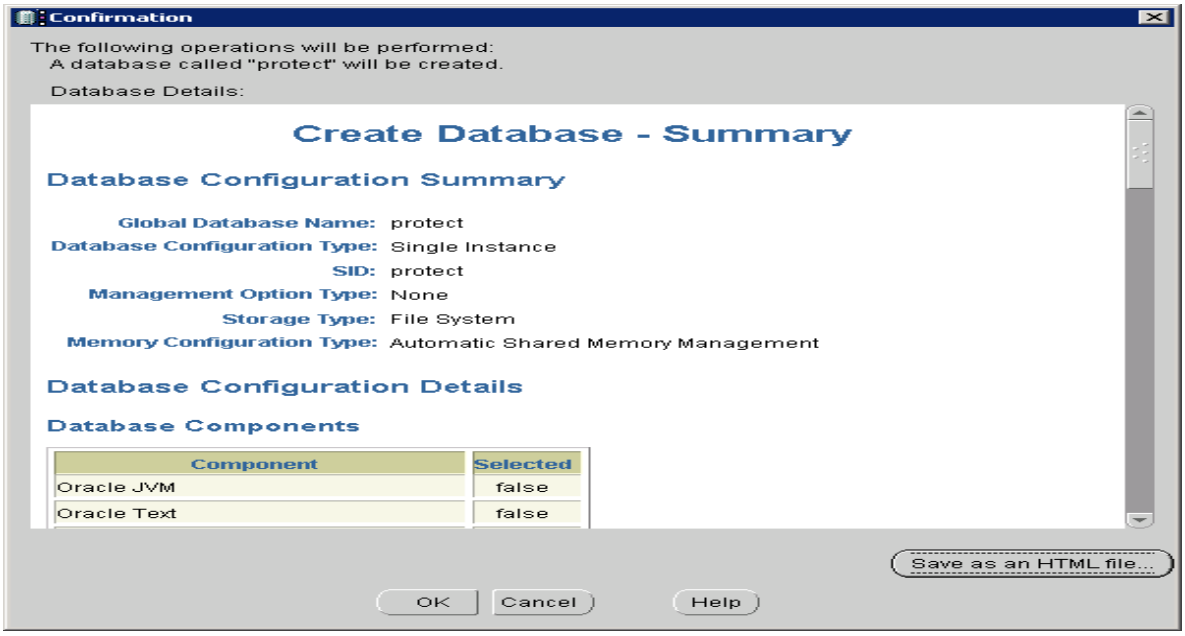


Figura 80 Configuración de BD de Symantec.

Configuración de Oracle 11g, Paso 11:

Se muestra el progreso de la base de datos.

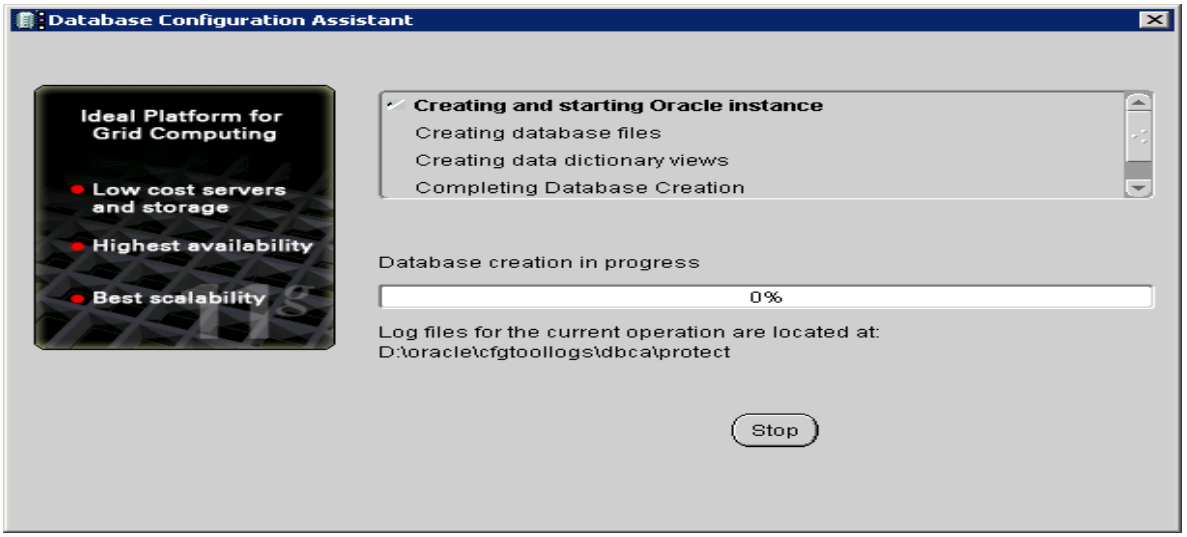


Figura 81 Instalación de BD de Symantec.

Configuración de Oracle 11g, Paso 12:

Al terminar este proceso una ventana nos pregunta se deseamos configurar otra base de datos, damos clic sobre Salir.

Figura 82 Finalización de instalación de BD de Symantec.

Verificar el servicio de Oracle 11G

Verificar servicio de Oracle 11g, Paso 1:

Verificar el status de “OracleServicePROTECT”

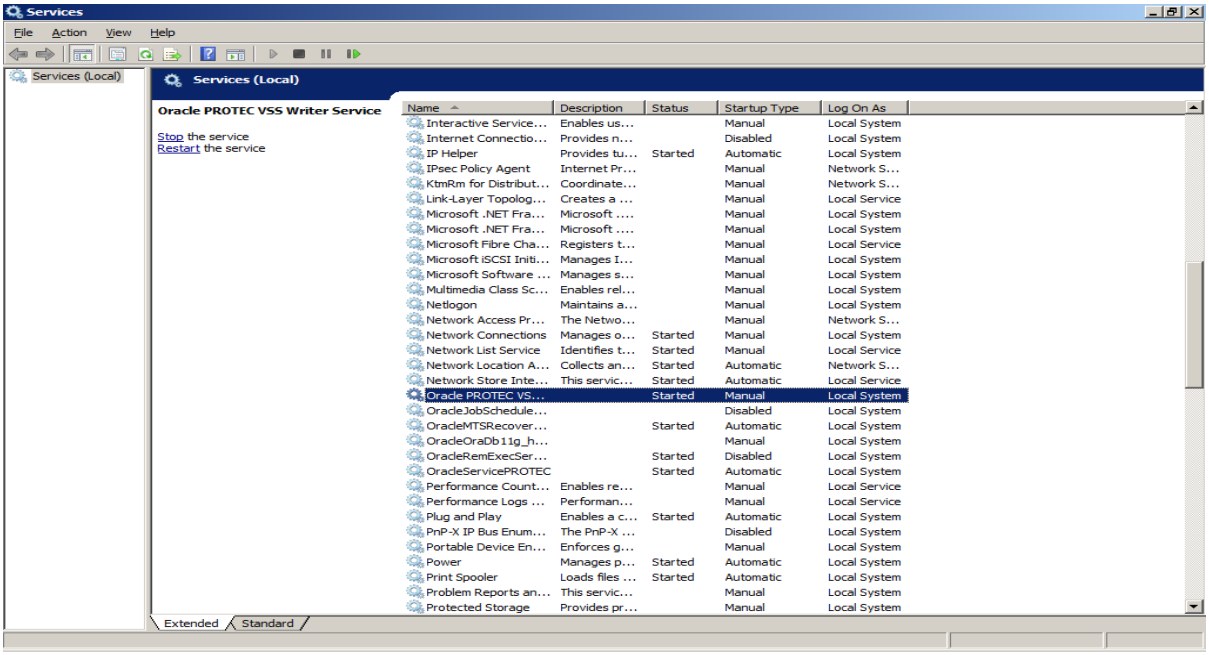


Figura 83 Validación de servicios de BD de Symantec.

Verificar el servicio DLP en la base de datos.

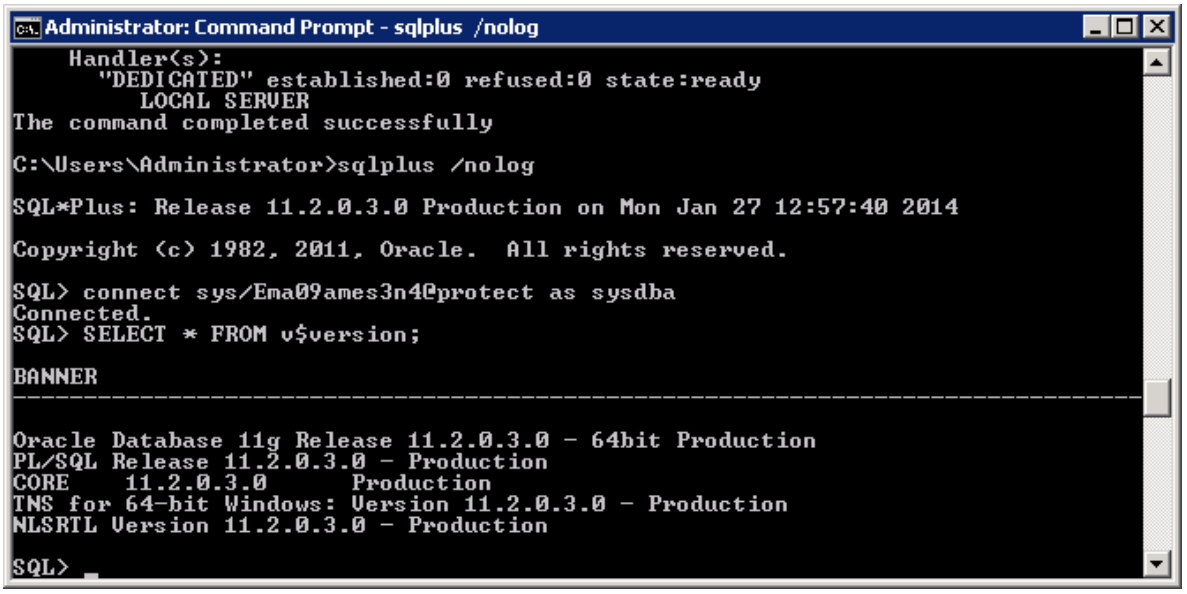


Figura 84 Validación de servicios BD de Symantec.

Creación del usuario de Oracle para DLP.

Creación del usuario de Oracle, paso 1:

Se creará un usuario llamado protect.

- Utilizar el archivo oracle_create_user.sql, que está en los installation tool´s
- Abrir un cmd y dirigirse la ubicación del archivo.

Abrir un SQL PLUS

- sqlplus /nolog
- **Correr el script**

SQL> @oracle_create_user.sql

- **Especificar el password del SYS**
- **En el SID especificar protect**
- **En la de username del nuevo usuario creado poner protect**
- **Especificar un password para el nuevo usuario**

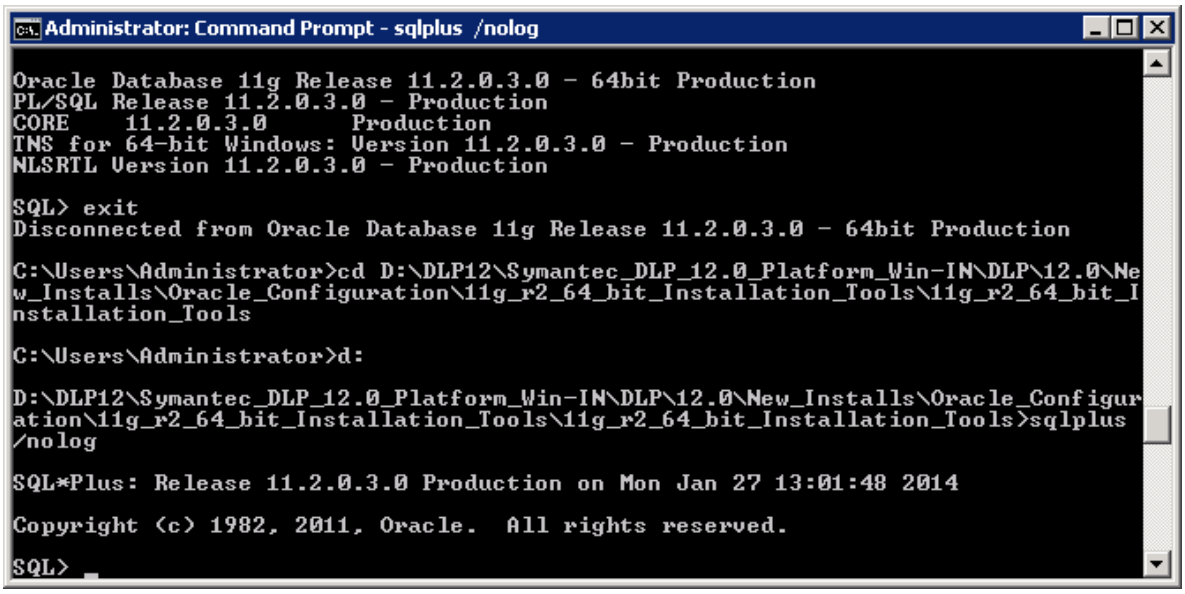


Figura 85 Creación del usuario de Oracle.

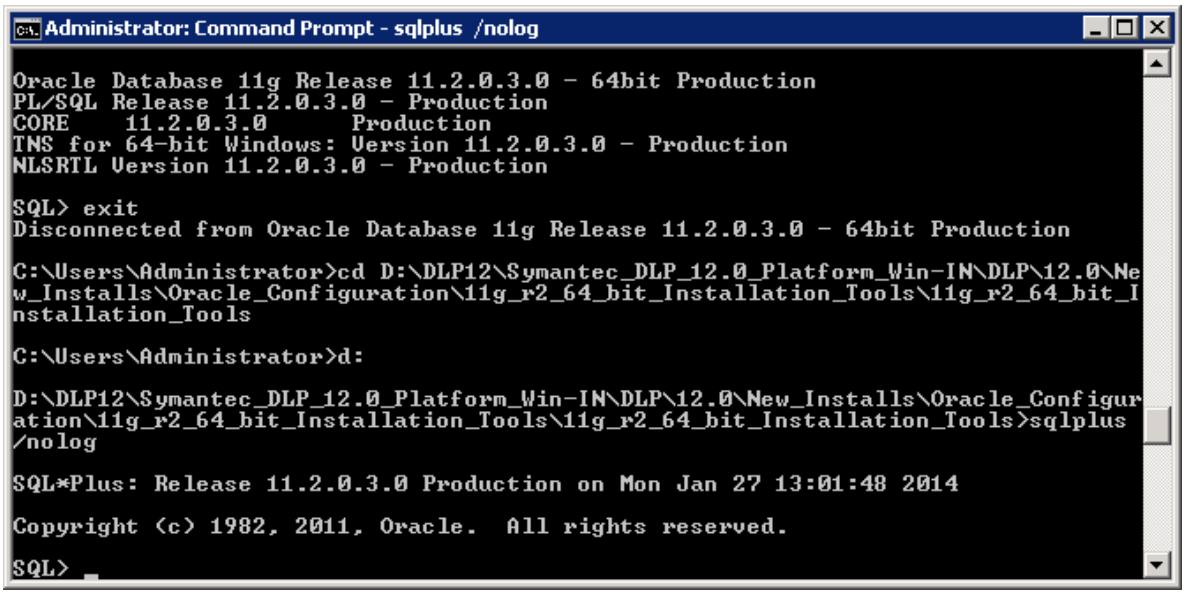


Figura 86 Creación del usuario de Oracle.

Bloqueo de la cuenta de usuario de Oracle DBSNMP

Bloqueo de cuenta Oracle DBSNMPe, paso 1:

Abrir un SQL PLUS

- sqlplus /nolog
- **Correr el script**

SQL> **ALTER USER dbsnmp ACCOUNT LOCK;**

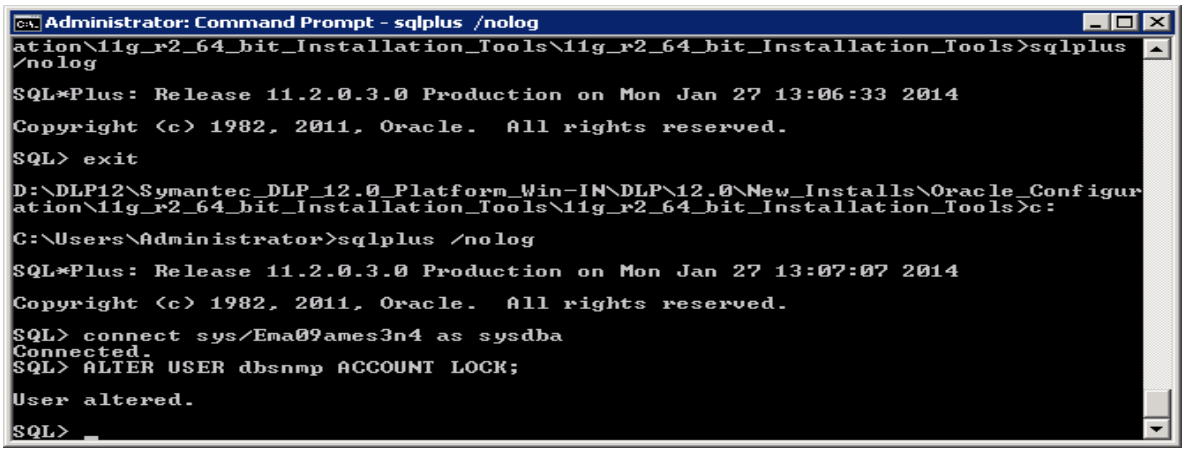


Figura 87 Bloqueo de la cuenta de usuario de Oracle DBSNMP.

Instalación de WinPcap

Instalación de WinPcap, paso 1:

Se ejecuta el archivo WinPcap.

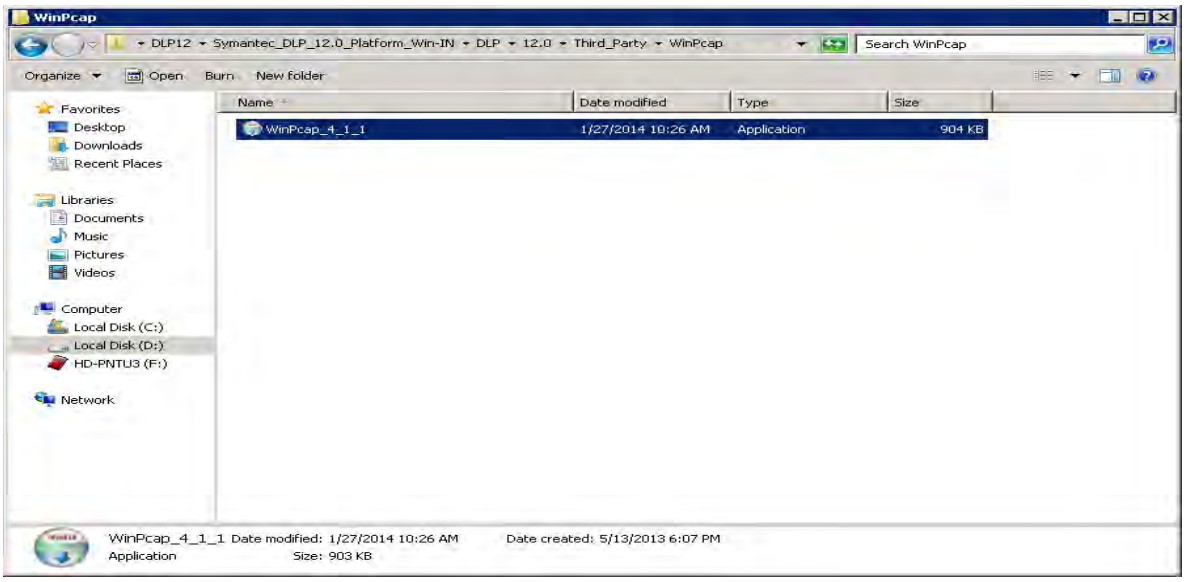


Figura 88 Instalación de WinCap.

Instalación de WinPcap, paso 2:

Se da clic en “Next”.

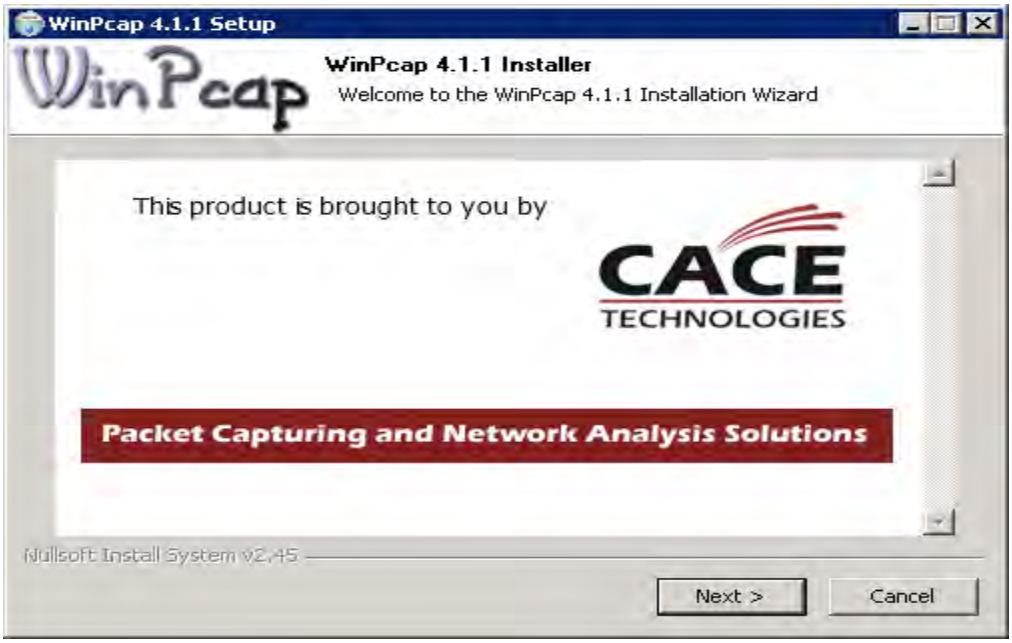


Figura 89 Instalación de WinCap.

Instalación de WinPcap, paso 3:

Se da clic en “Next”.

Figura 90 Instalación de WinCap.

Instalación de WinPcap, paso 4:

Se da clic en “ I agree”.

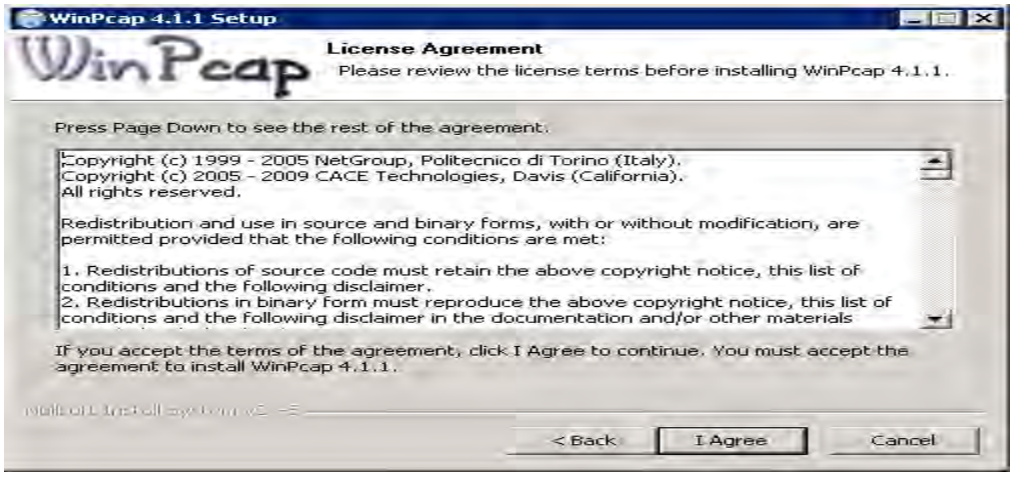


Figura 91 Instalación de WinCap.

Instalación de WinPcap, paso 5:

Se da clic en “Install”.

Figura 92 Instalación de WinCap.

Instalación de WinPcap, paso 6:

Se da clic en “ Finish”.

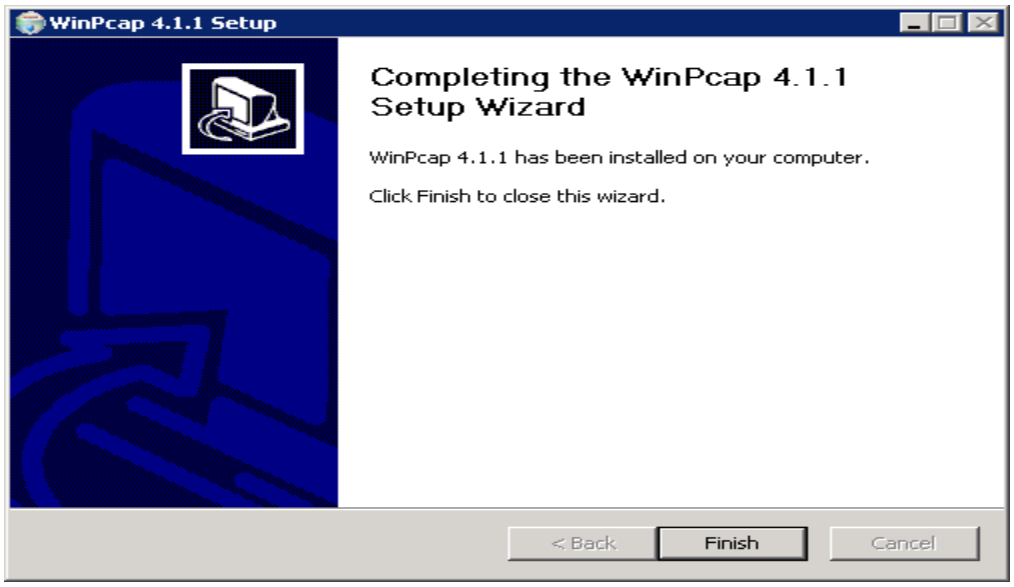


Figura 93 Instalación de WinCap.

Instalación Symantec DLP Enforce

Instalación Symantec DLP Enforce, Paso 1:

Ejecutar el archivo de instalación ***ProtectInstaller64_12.0***, en su versión de Windows

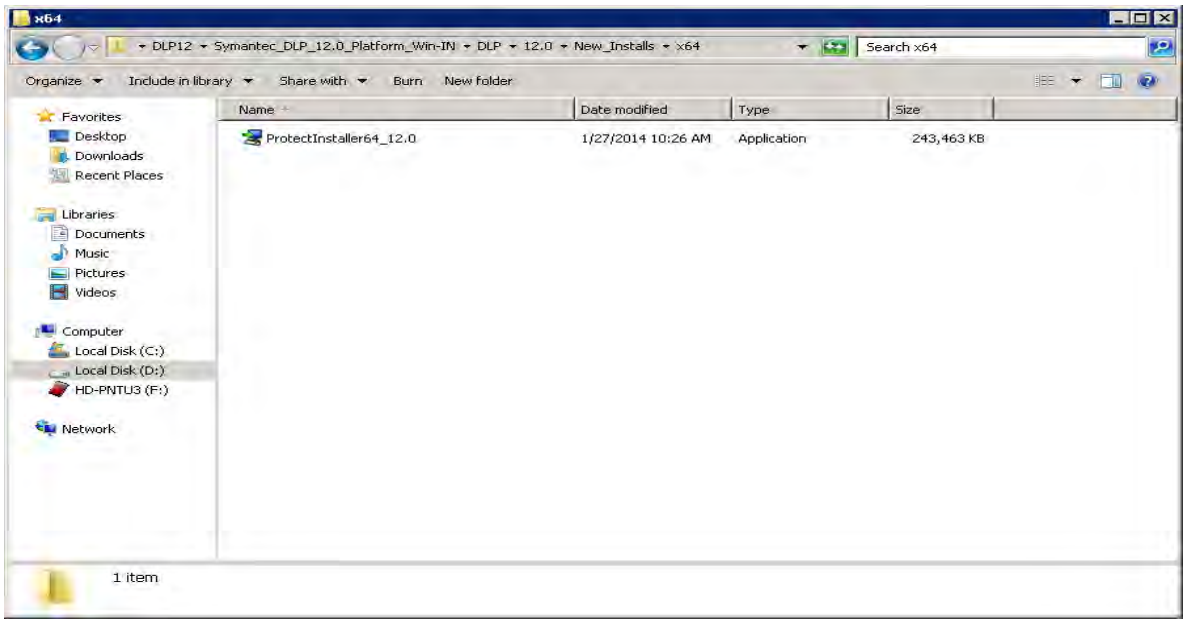
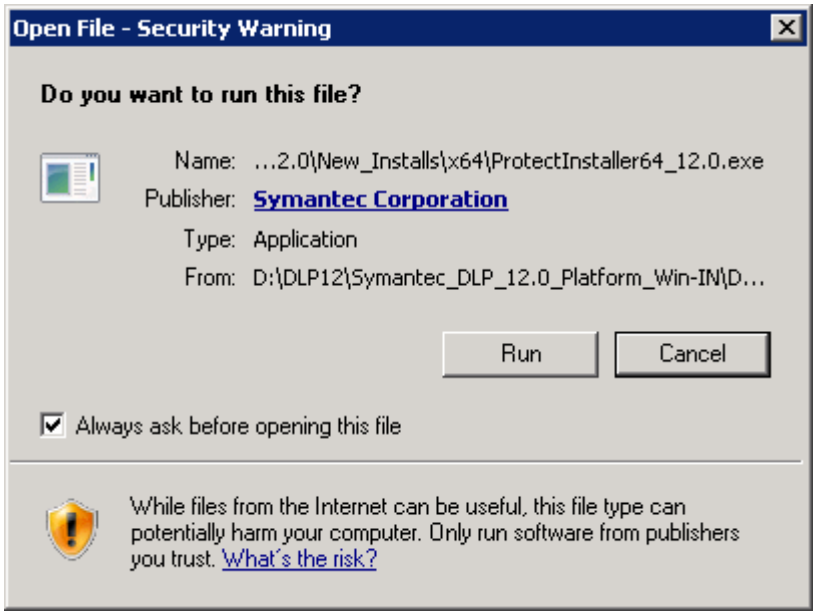


Figura 94 Instalación de Symantec DLP Enforce.



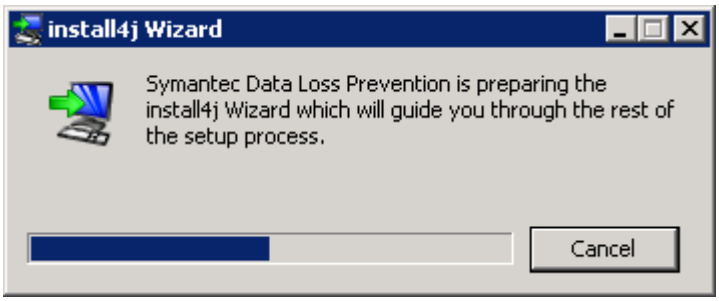


Figura 95 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 2:

El asistente de instalación de *Symantec Data Loss Prevention* será mostrado, para continuar se presiona el botón ***Next***

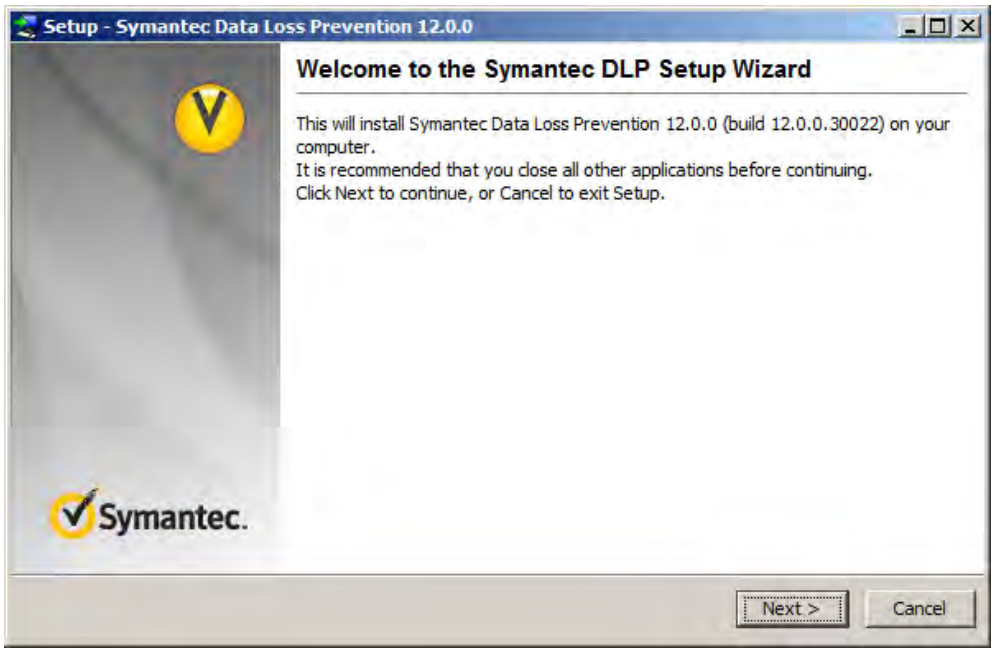


Figura 96 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 3:

La siguiente ventana indica la información del contrato de licencia, el cual debe ser aceptado para continuar con el proceso de instalación, para continuar se presiona el botón ***Next***.

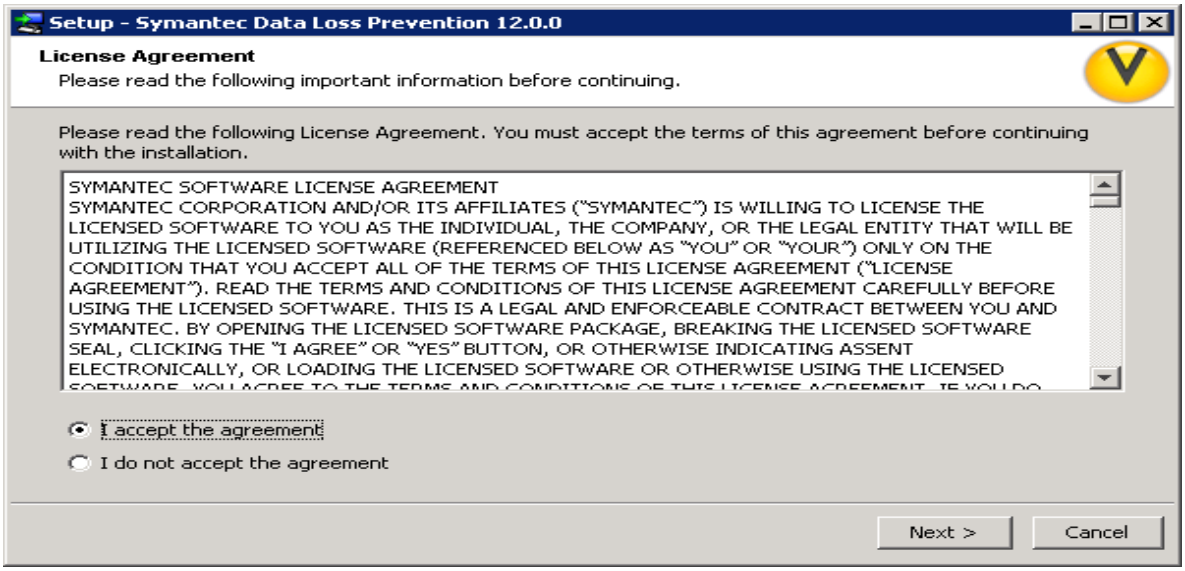


Figura 97 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 4:

En la siguiente ventana del asistente debe indicarse qué tipo de servidor es el que será instalado, en este caso seleccionamos Enforce, para continuar se presiona el botón ***Next***.

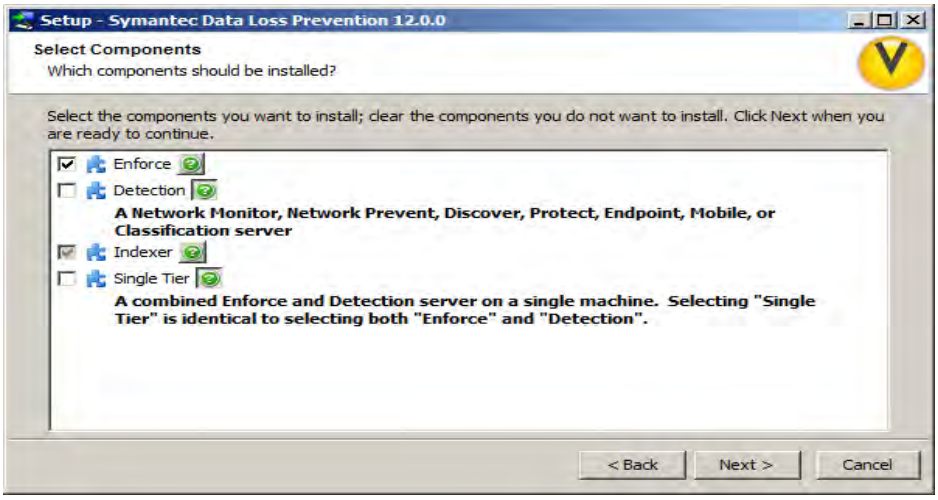


Figura 98 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 5:

En la siguiente ventana del asistente debe especificarse la ruta donde se encuentra el archivo de licencia el cual será validado, para continuar se presiona el botón ***Next***

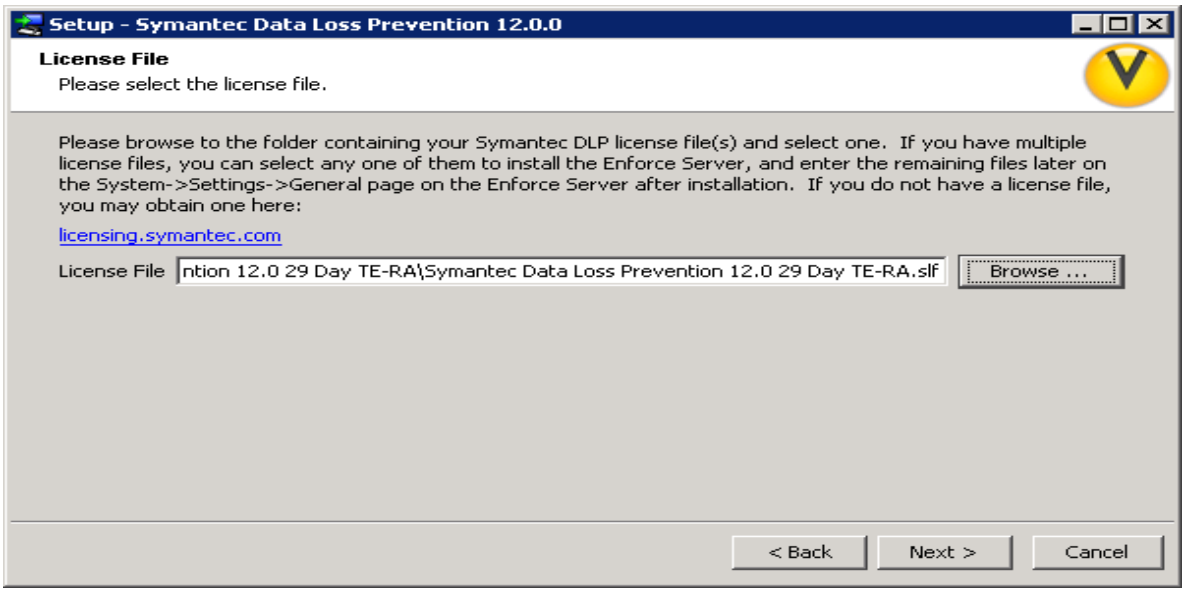


Figura 99 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 6:

En la siguiente ventana del asistente debe especificarse la ruta donde será instalado Symantec dlp seleccionamos la ruta default recomendada.

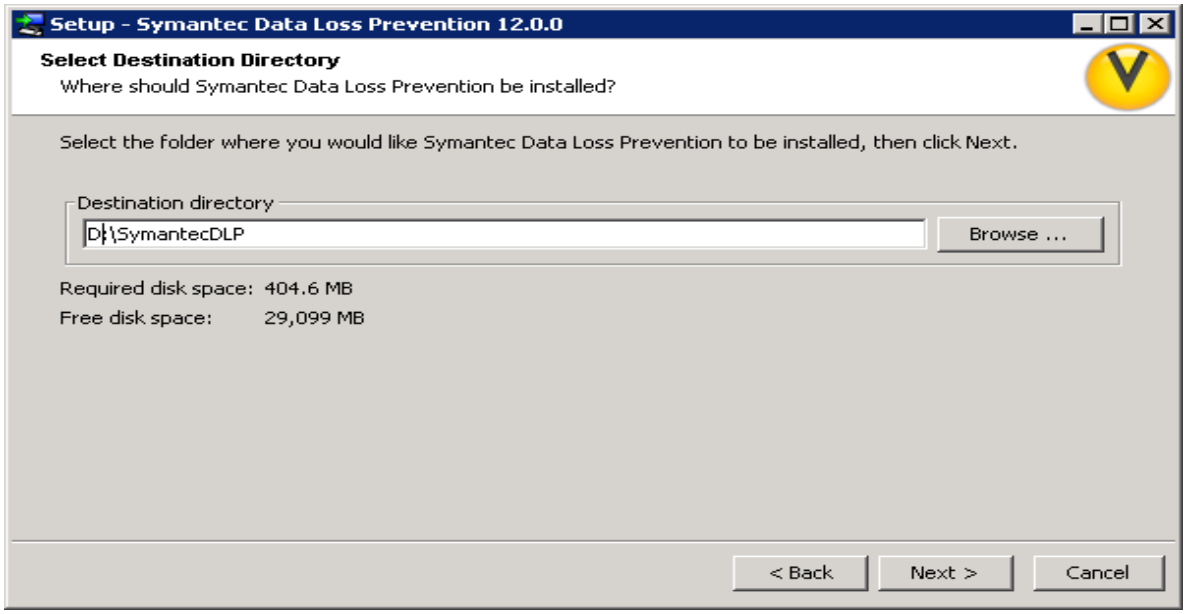


Figura 100 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 7:

Especificar las credenciales para los servicios de Symantec DLP.

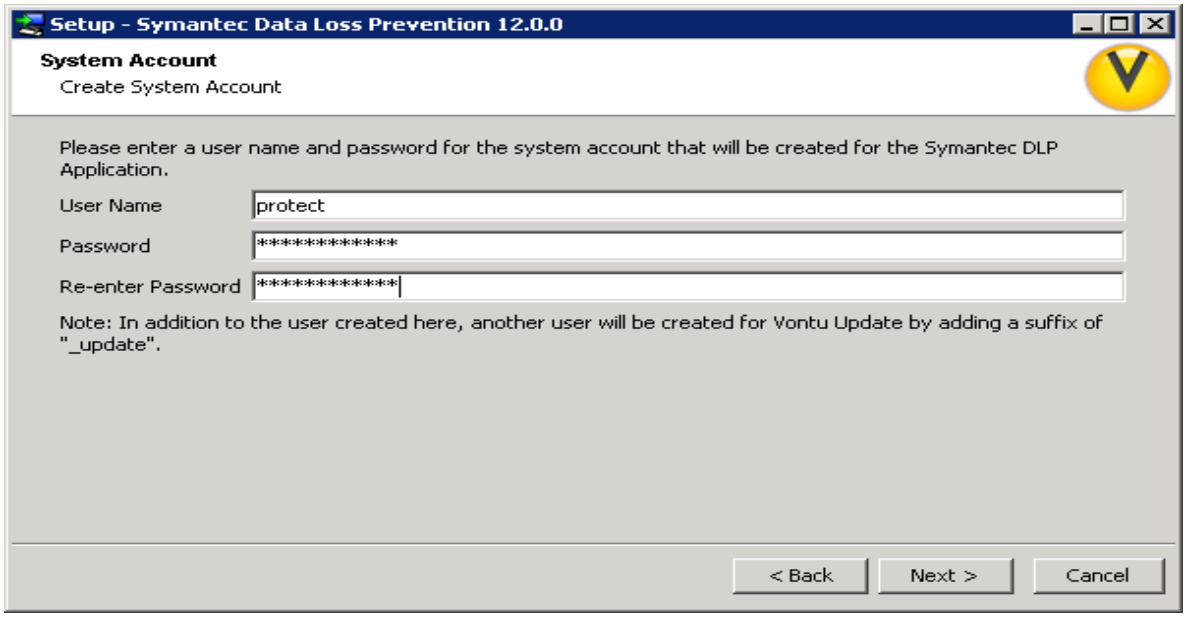


Figura 101 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 8:

Especificar las la conexión a Symantec Management Platform, la cual no es requerida para durante esta implementación.

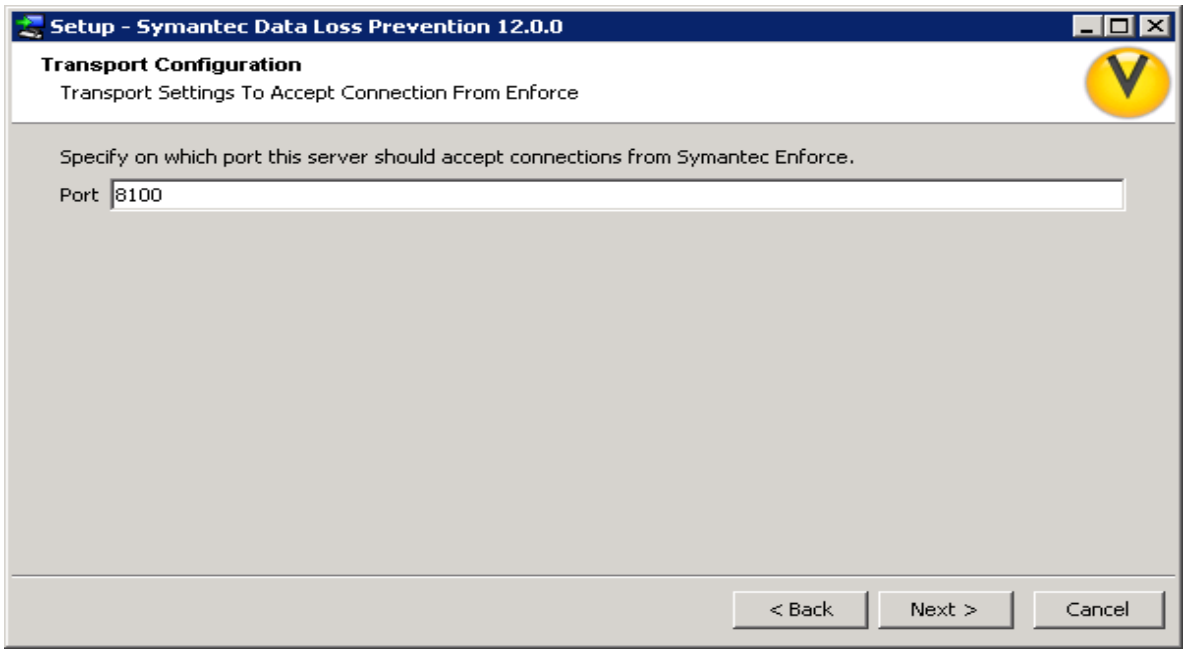


Figura 102 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 9:

En la siguiente ventana del asistente debe especificarse la conexión al servidor de base de datos, dirección IP y puerto de comunicación, en este caso Oracle se encuentra en el mismo servidor, por lo cual la dirección local es: 127.0.0.1 , se presiona el botón ***Next***.

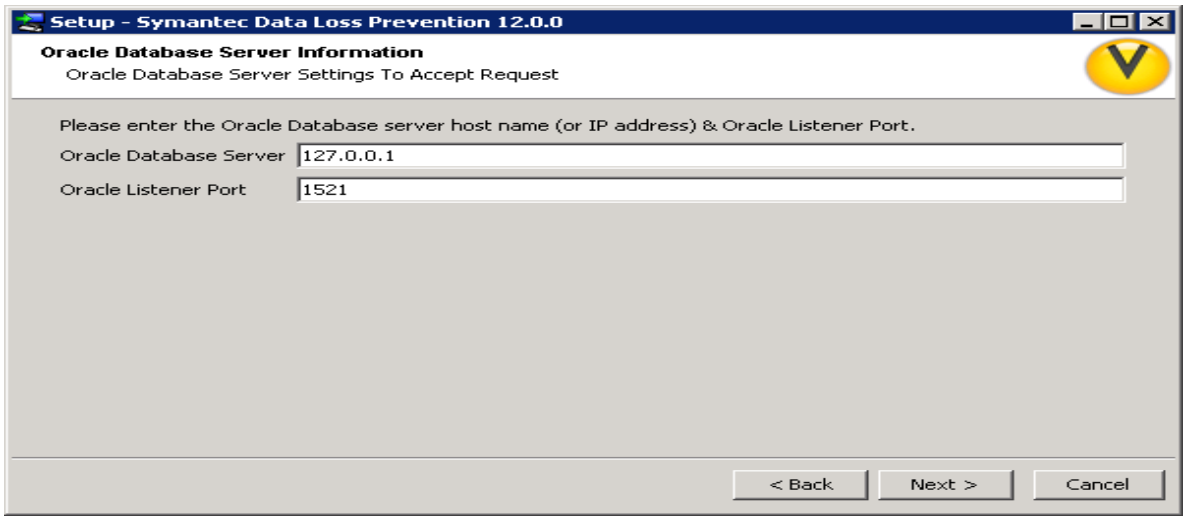


Figura 103 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 10:

Especificar las credenciales para la conexión con Oracle y Symantec DLP.

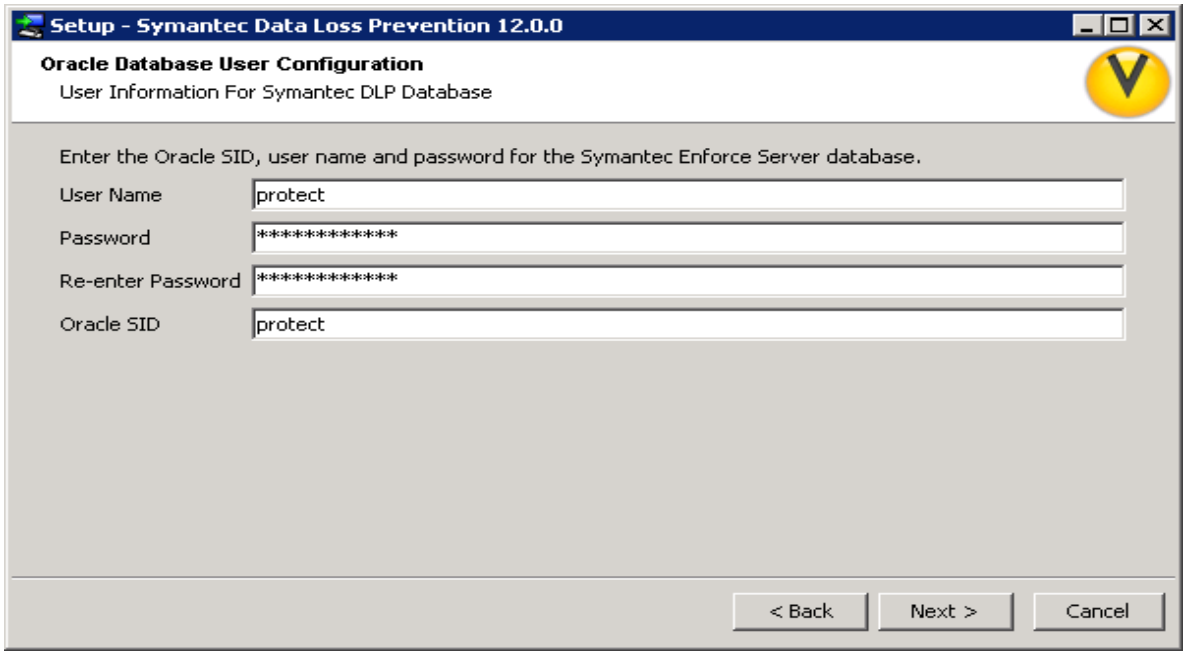


Figura 104 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 11:

En la siguiente ventana del asistente debe especificarse si es requerido agregar una ubicación adicional, el default es ***English***, así que se cambia al valor ***None***, para continuar se presiona el botón ***Next***.

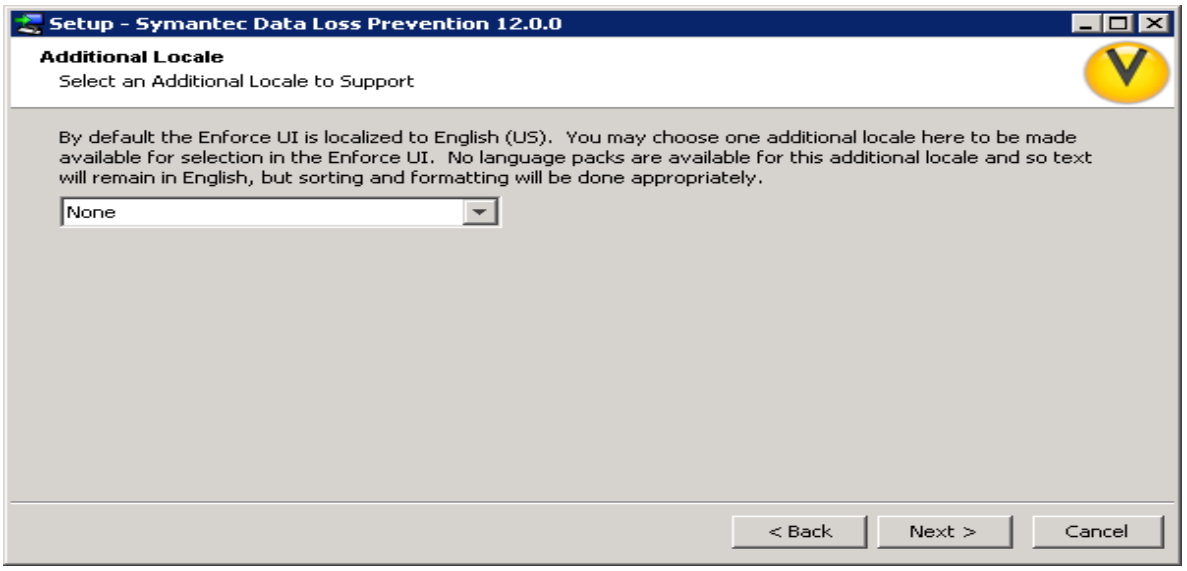


Figura 105 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 12:

En la siguiente ventana del asistente debe especificarse las características del Server

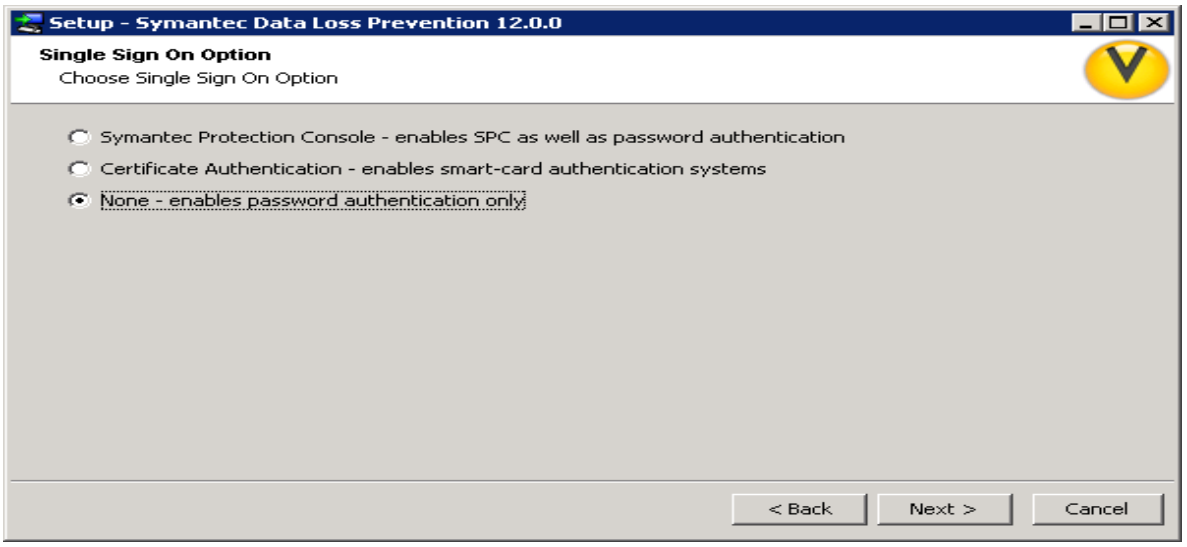


Figura 106 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 13:

En la siguiente ventana del asistente deben especificarse las credenciales de acceso a la consola.

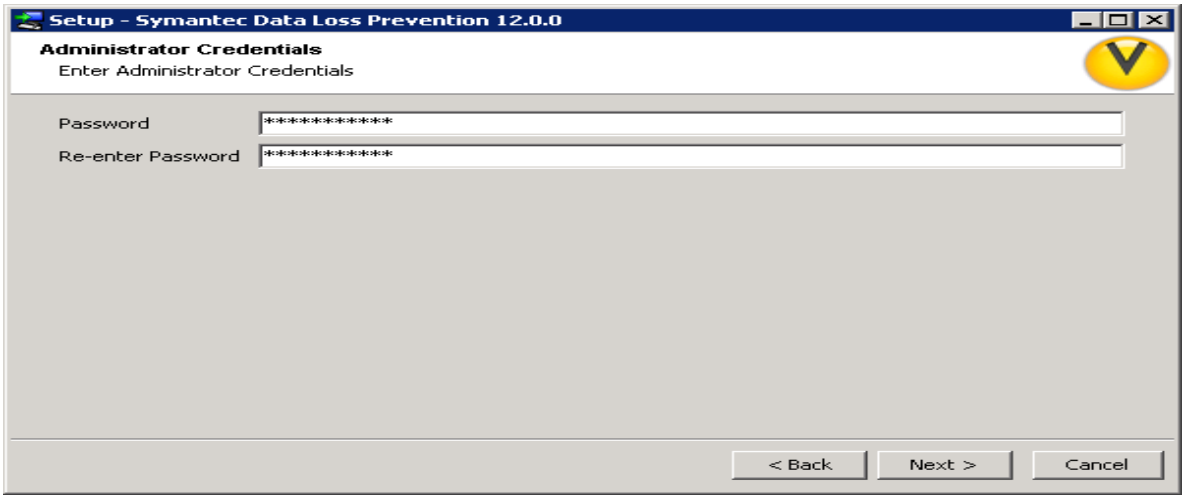


Figura 107 Instalación de Symantec DLP Enforce.

Instalación Symantec DLP Enforce, Paso 14:

La siguiente ventana mostrará el progreso de la instalación (***preloader***).

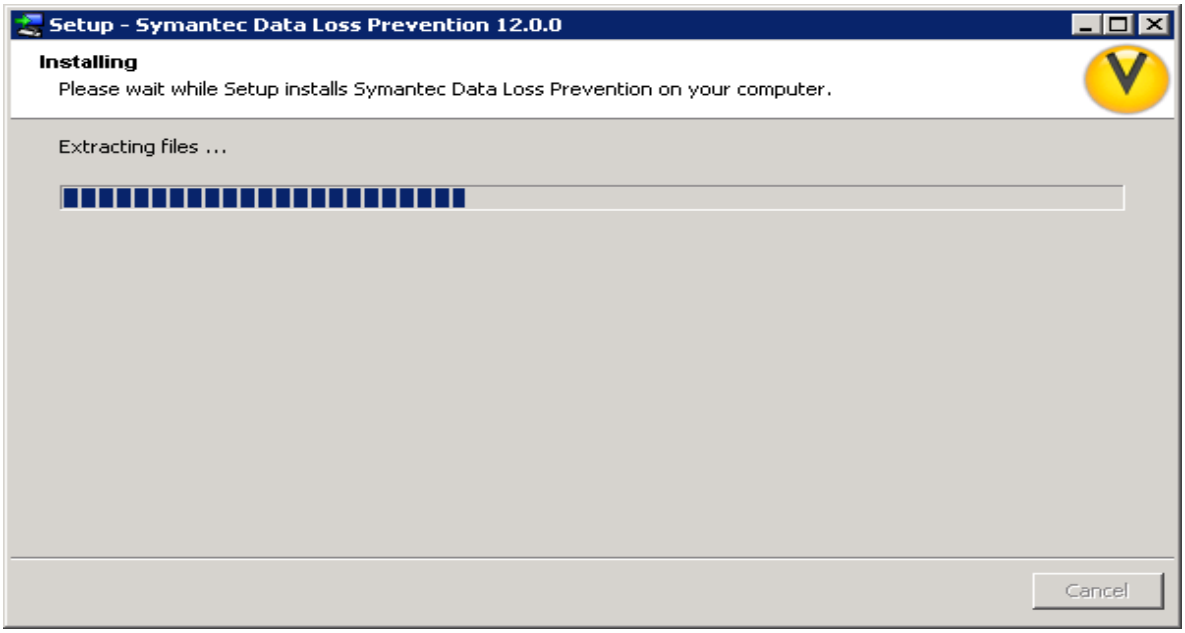


Figura 108 Instalación de Symantec DLP Enforce.

Symantec DLP Enforce, Paso 15:

Al finalizar el proceso de instalación, la ventana siguiente indica si se desean iniciar los servicios de Symantec DLP, se debe verificar que la casilla este activa, para concluir se presiona el botón ***Finish***.

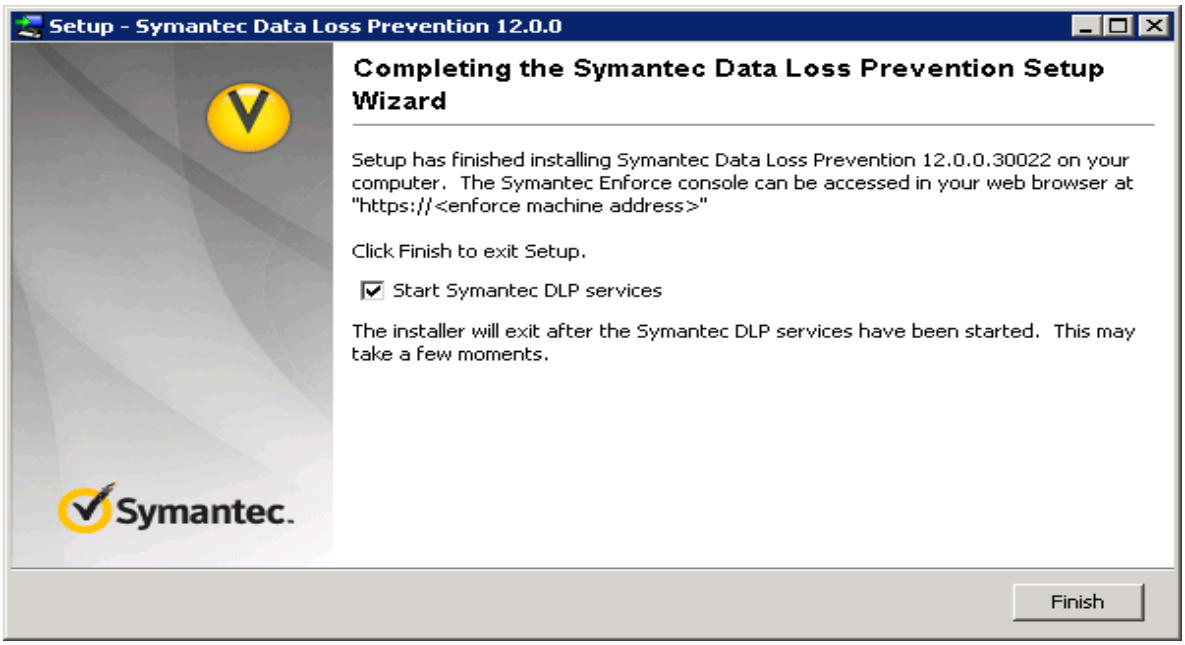


Figura 109 Instalación de Symantec DLP Enforce.

6.2 Manual de Usuario

Sistema.

Esta pantalla proporciona una descripción general de su sistema, incluyendo el estado del servidor y los eventos del sistema recientes. Muestra la información resumen sobre todos los servidores de Symantec Data Loss Prevention, una lista de eventos recientes de error y de advertencia, y la información sobre su licencia. Desde esta pantalla se pueden agregar o eliminar los servidores de detección.

Configuración servidores.

Agregar un servidor de detección.

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 110 Agregar un servidor de detección.

Nos dirigimos a la siguiente ruta System>Servers>overview.

Figura 111 Agregar un servidor de detección.

Damos clic en la opción Add Server.

Figura 112 Agregar un servidor de detección.

Seleccionar el servidor de detección que se desea agregar.

Nota: para este caso agregaremos un Network Monitor.

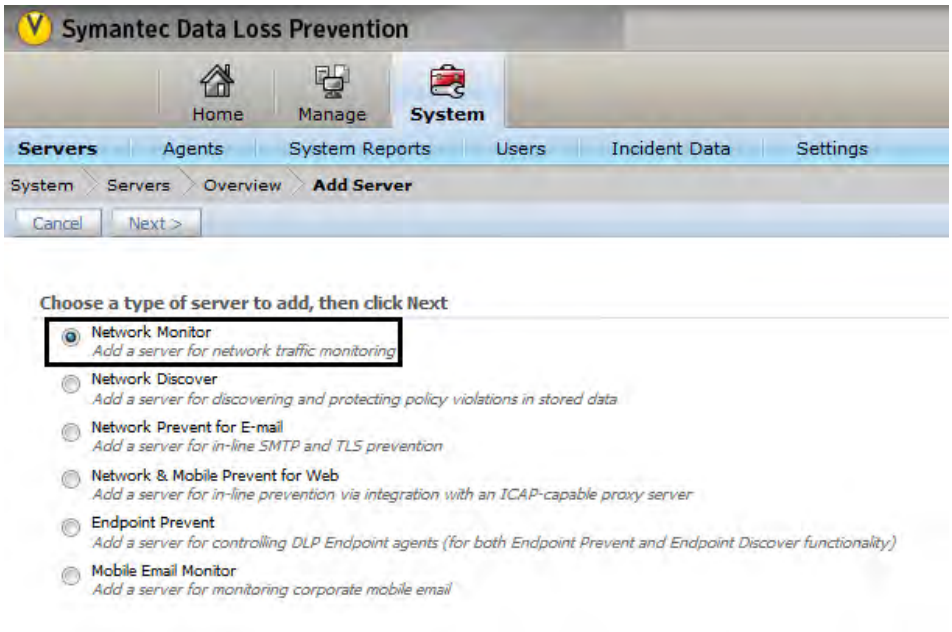


Figura 113 Agregar un servidor de detección.

En la ventana de configuración del servidor se agregan los parámetros de Name (nombre de identificación del servidor), Host (IP del servidor de detección), el puerto 8100 se queda por defecto ya que es el puerto de comunicación con la consola de administración.

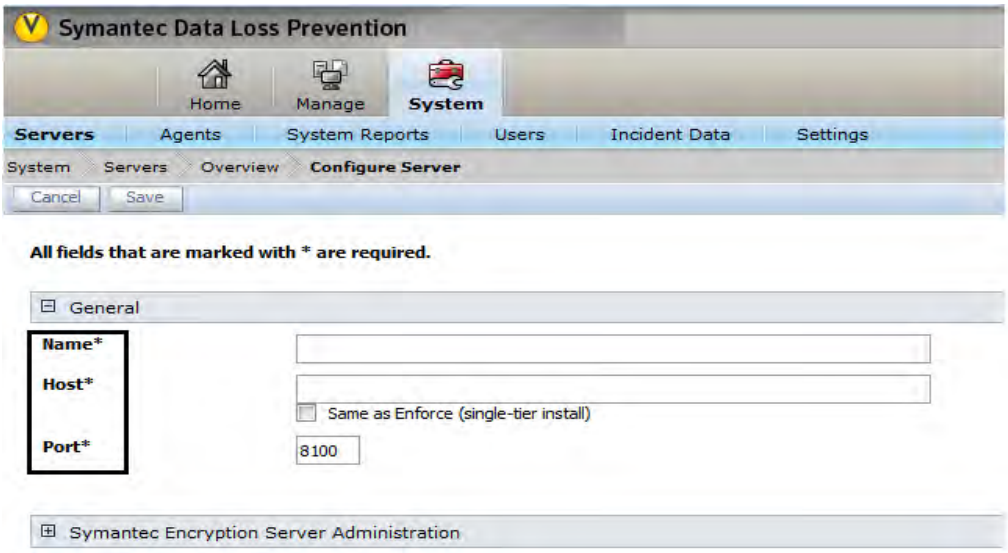


Figura 114 Agregar un servidor de detección.

Para finalizar damos clic en save.

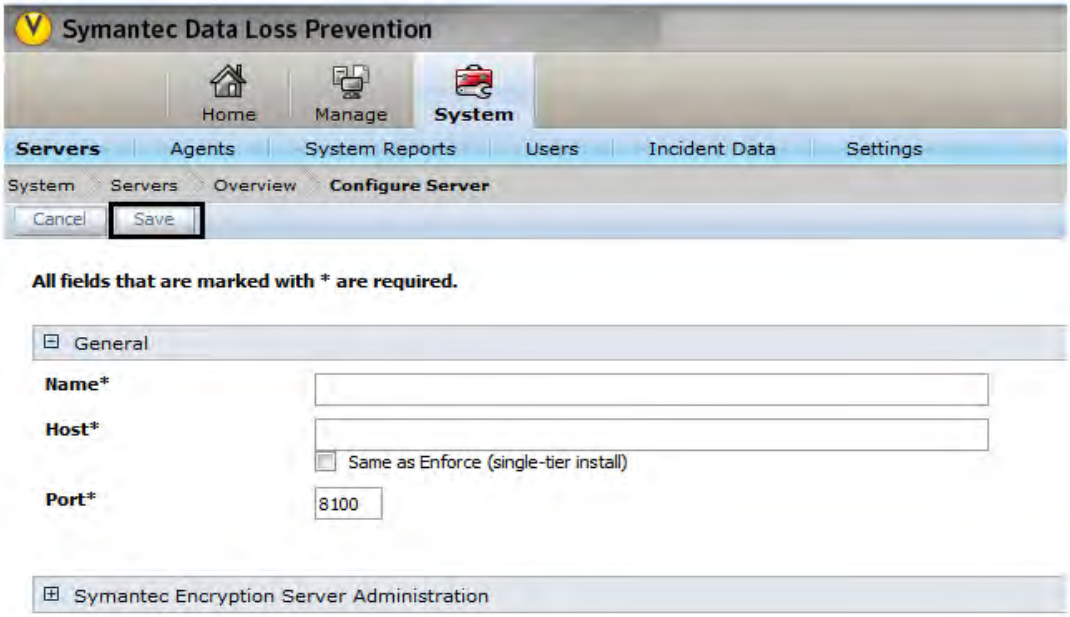


Figura 115 Agregar un servidor de detección.

Verificar que los servicios estén en running.

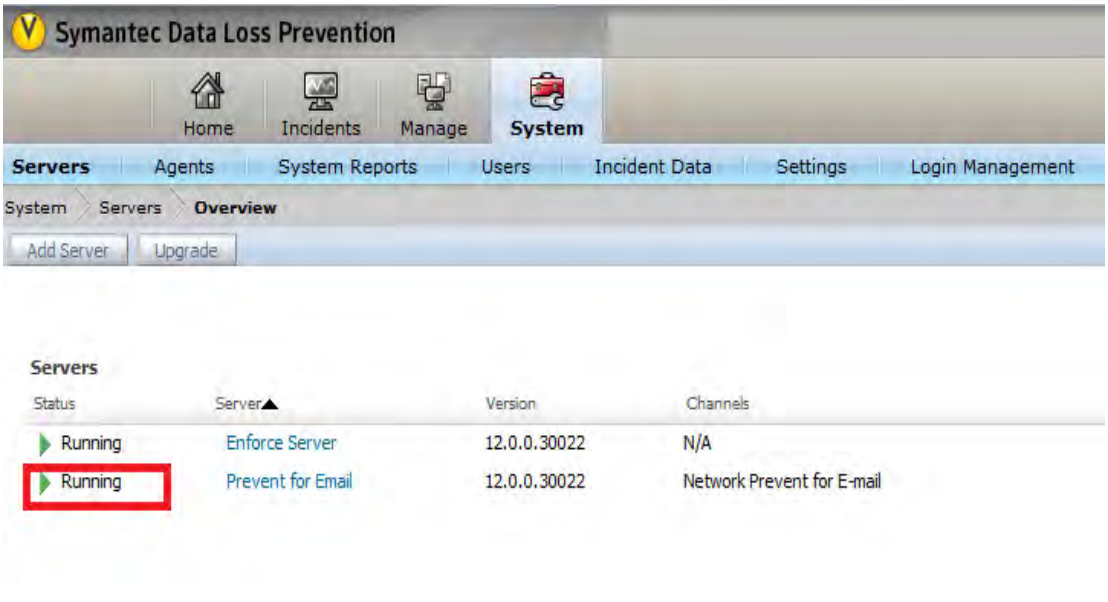


Figura 116 Agregar un servidor de detección.

Controles del servidor.

El Control de proceso avanzado de Symantec Data Loss Prevention le permite iniciar o detener procesos de servidor individuales de la consola de administración de Enforce Server. No es necesario iniciar o detener un servidor entero. Esta función puede ser útil para depurar.

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

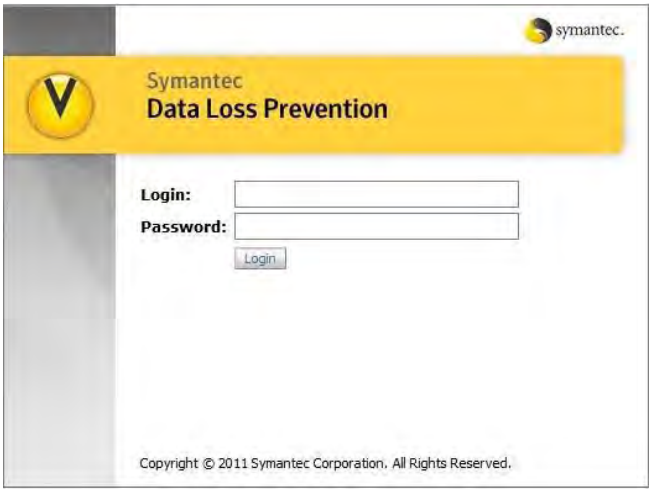


Figura 117 Controles un servidor de detección.

Nos dirigimos a la siguiente ruta System>Servers>overview.

Figura 118 Controles un servidor de detección.

Seleccionamos el servidor que deseamos controlar.

Nota: para este caso seleccionamos el servidor network monitor.

La opción de General podemos hacer lo siguiente:

Iniciar. Para iniciar un servidor o un proceso, haga clic en Iniciar.

Reciclar. Para detener y reiniciar un servidor, haga clic en Reciclar.

Detener. Para detener un servidor o un proceso, haga clic en Detener.

Para parar un proceso durante su procedimiento de inicio, haga clic en Finalizar.

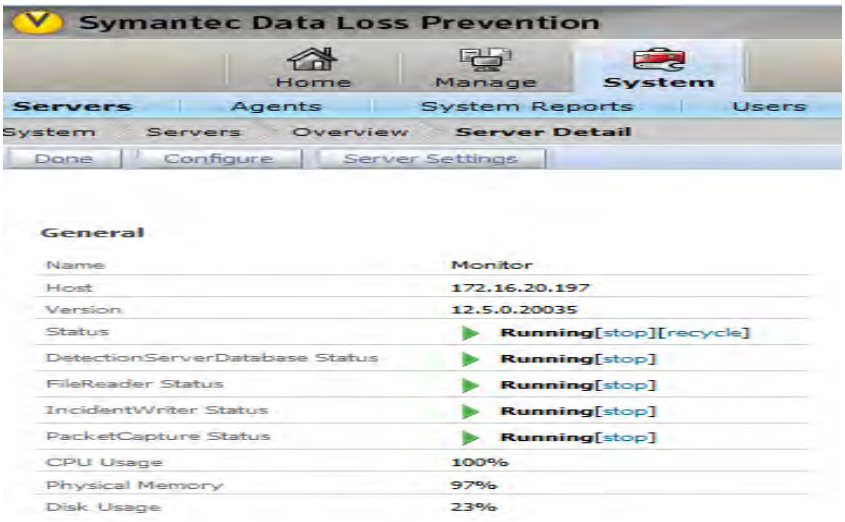


Figura 119 Controles un servidor de detección.

Valores del estado del servidor

	Iniciando: en proceso de inicio.
	En ejecución: ejecutándose sin errores.
	Ejecución seleccionada: algunos procesos en el servidor se detuvieron o tienen errores. Para ver los estados de procesos individuales, se debe habilitar primero el **Control de proceso avanzado** en la pantalla **Configuración del sistema**.
	Deteniendo: en proceso de detención.
	Detenido: detenido completamente.
?	Desconocido: el servidor ha encontrado uno de los siguientes errores:

Figura 120 Controles un servidor de detección.

Nos dirigimos a la siguiente ruta System>Servers>Alerts.

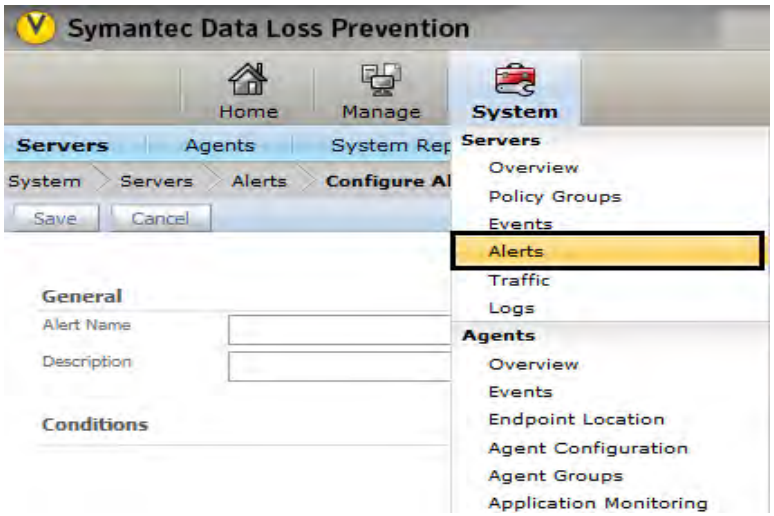


Figura 121 Alertas de Sistema.

Damos clic en la opción Add alert.

Figura 122 Alertas de Sistema.

En la sección de General llenar los siguientes parámetros:

Alert name: Nombre de la alerta

Description: Descripción de la alerta.

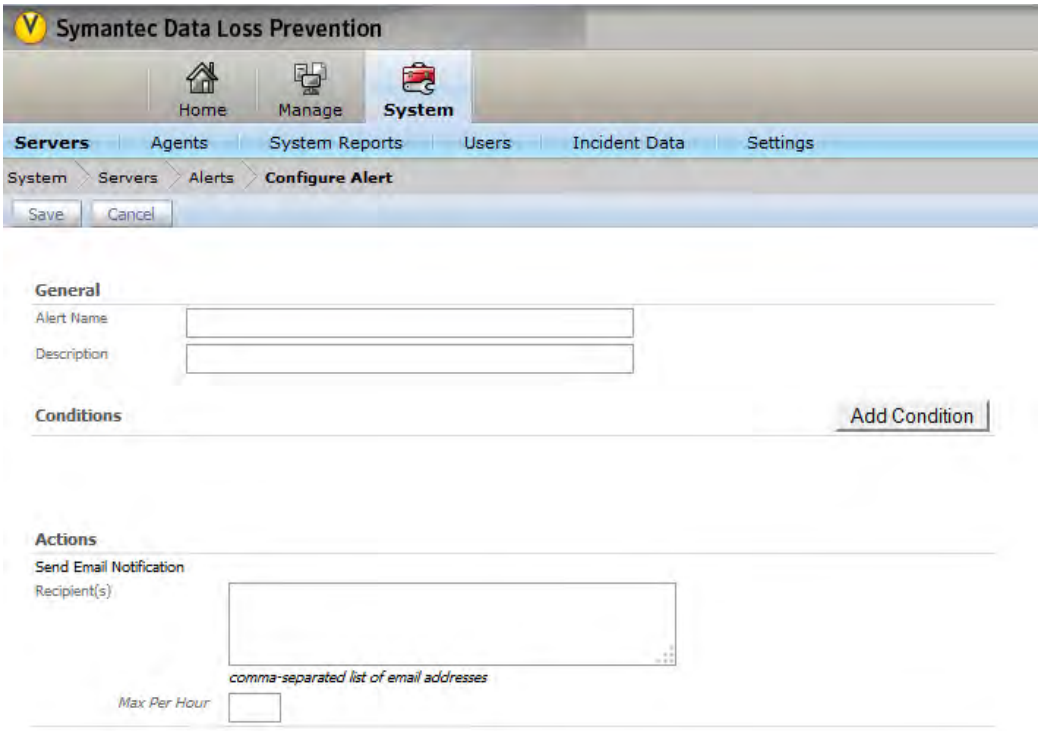


Figura 123 Alertas de Sistema.

Damos clic en la opción Add Condition.

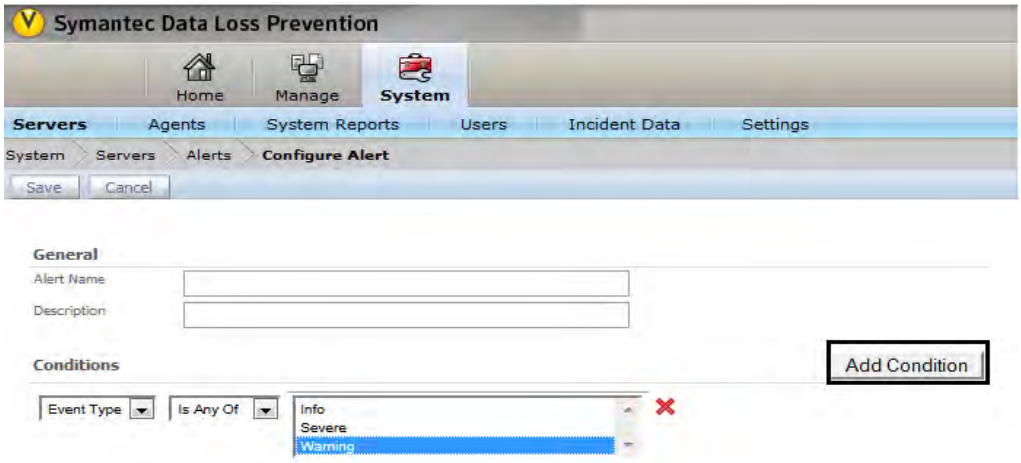


Figura 124 Alertas de Sistema.

Seleccionamos la condición que se debe cumplir para mandar la alerta.

Nota: para este caso seleccionamos notificar los eventos de precaución.

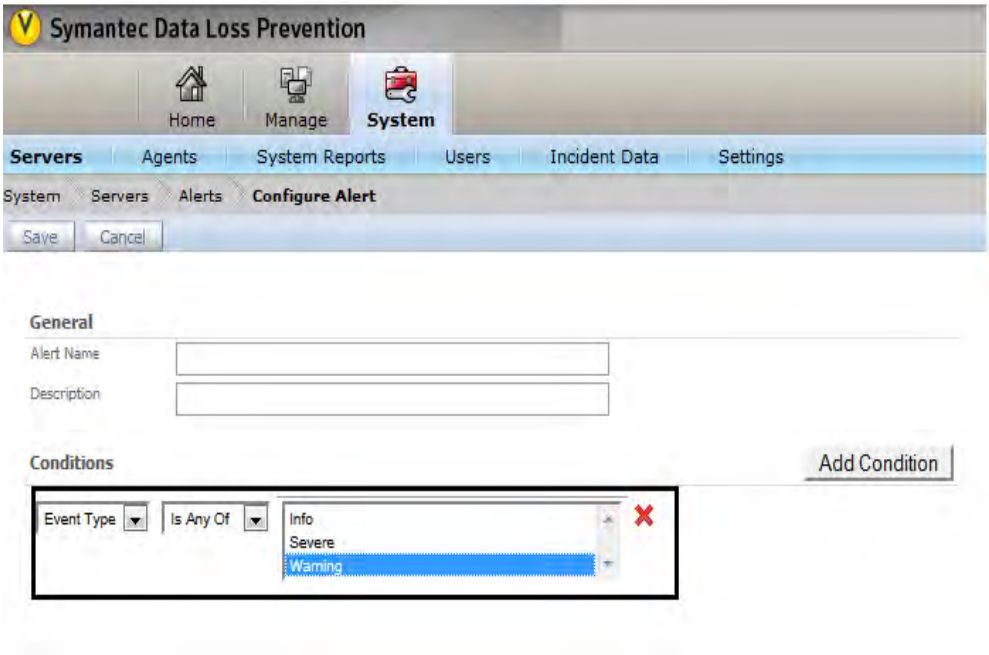


Figura 125 Alertas de Sistema.

En la sección de Action escribimos el correo del usuario al cual se notificara la alerta.

Figura 126 Alertas de Sistema.

Damos clic en la opción save para guardar los cambios.

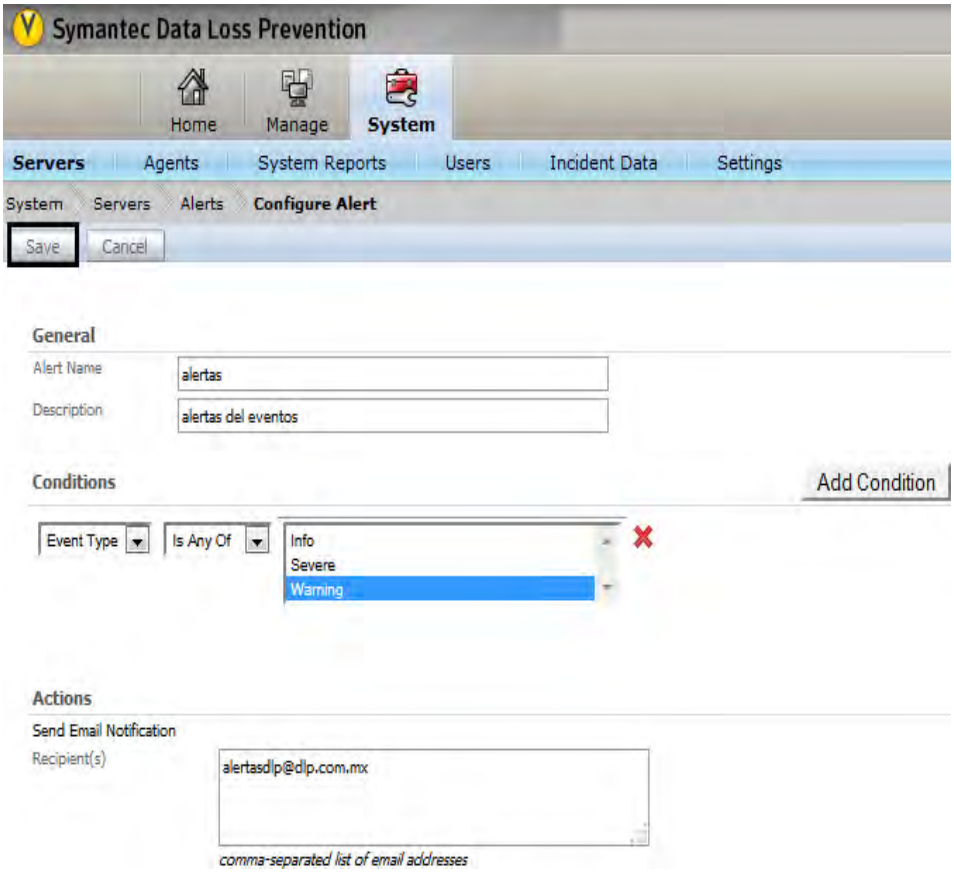


Figura 127 Alertas de Sistema.

Al finalizar nos manda una ventana en donde nos dice que la Alerta fue guardada con éxito.

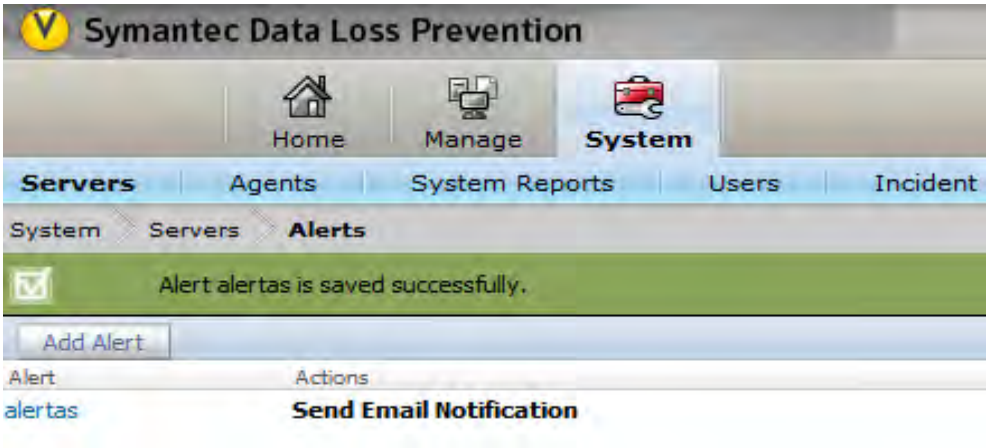


Figura 128 Alertas de Sistema.

Trafico.

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 129 Tráfico del Sistema.

Nos dirigimos a la siguiente ruta System>Servers>traffic.

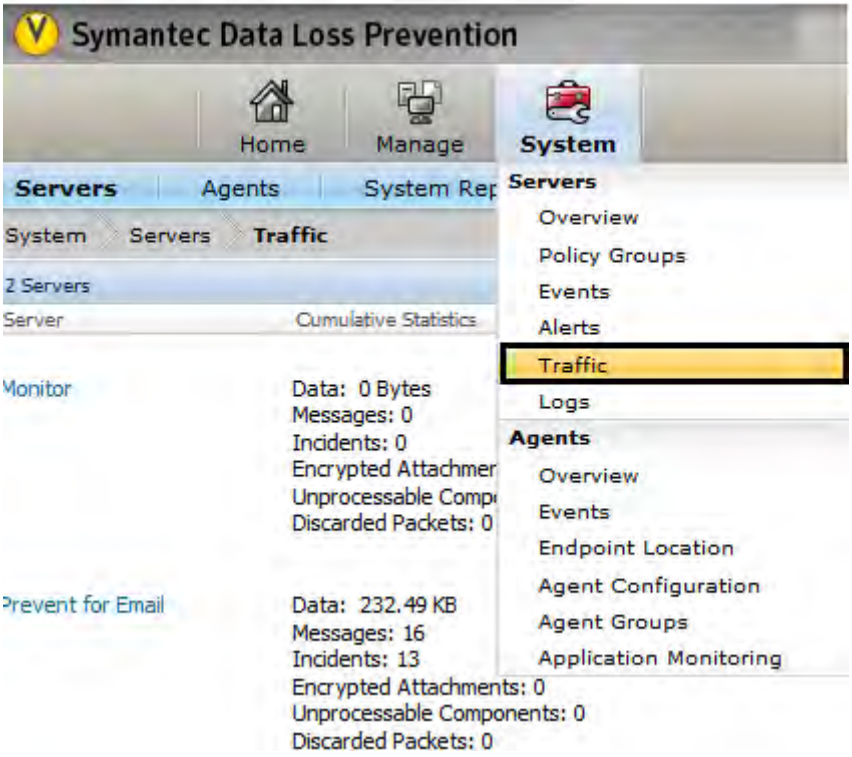


Figura 130 Trafico del Sistema.

Seleccionamos el servidor de detección para ver su tráfico capturado.

Nota: Para este caso se seleccionó un Network Prevent for Web.

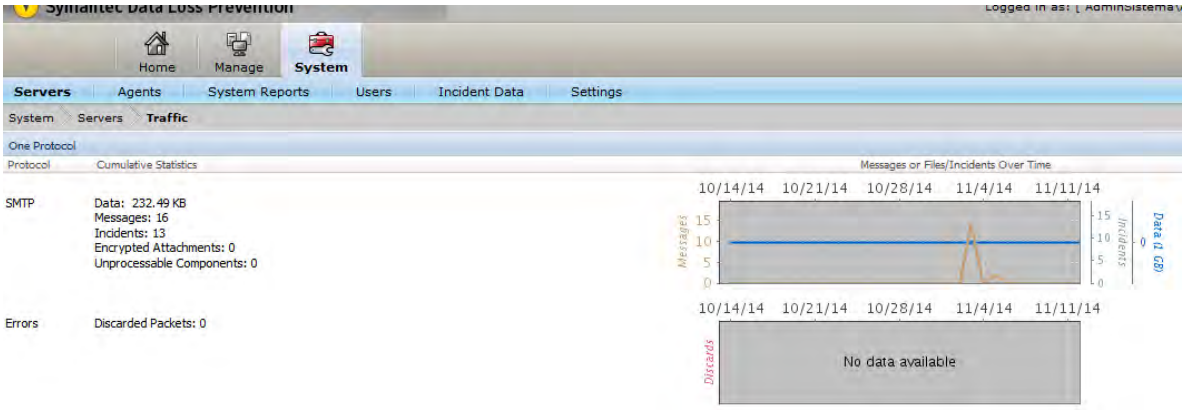


Figura 131 Tráfico del Sistema.

LOGS.

Los archivos de registro operativo registran información detallada sobre las tareas que el software realiza y cualquier error que se produzca mientras el software realiza esas tareas. Es posible usar los contenidos de los archivos de registro operativo para verificar que el software funcione como se espera. Puede también usar estos archivos para solucionar problemas en la manera que el software se integra con otros componentes del sistema, la configuración seria la siguiente:

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 132 Logs del Sistema.

Nos dirigimos a la siguiente ruta System>Servers>logs.

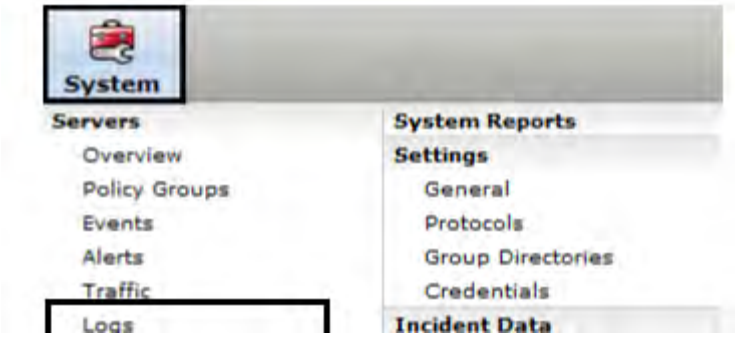


Figura 133 Logs del Sistema.

Dar clic en List Box y seleccionar la opción Endpo int Server, activar el Check Box en Agent Logs y para finalizar dar clic en Collect Logs

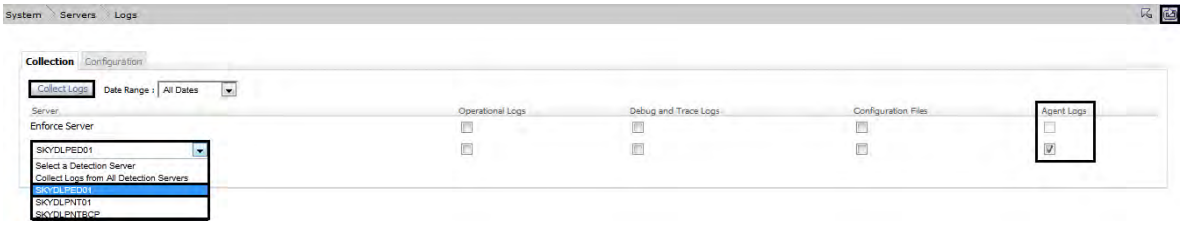


Figura 134 Logs del Sistema.

Proceso previo del archivo Log

Figura 135 Logs del Sistema.

Para descargar el archivo Log generado, clic en para actualizar y dar clic en Download

Figura 136 Logs del Sistema.

Se descomprime el archivo .zip, genera un directorio SKYDLPED01 y después se dirige a la ruta \SKYDLPED01\ y se selecciona el log que se desee ver, en este caso _edpa.log el cual tiene un tamaño de archivo en KB

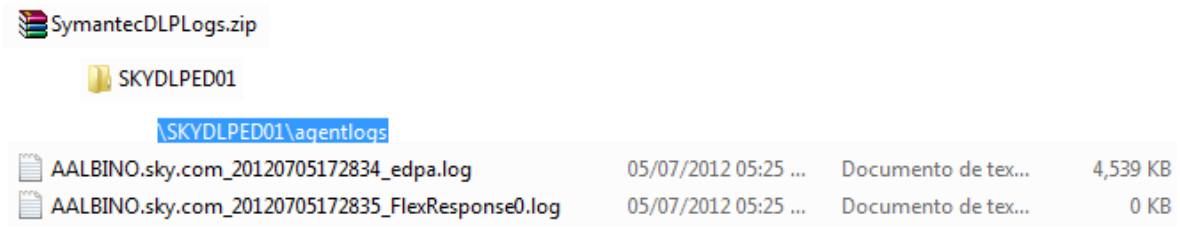


Figura 137 Logs del Sistema.

Para poder ver el Log deseado, se abre el archivo con cualquier Editor para ver su contenido.

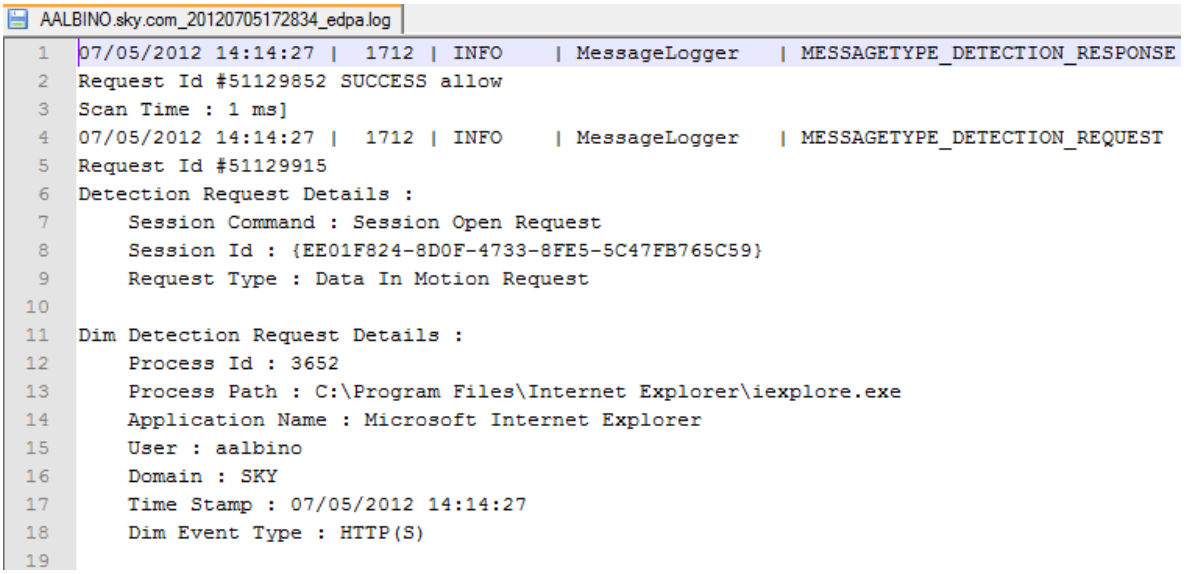


Figura 138 Logs del Sistema.

Configuración de Agentes.

Estas opciones de configuración determinan los tipos de detección que ocurren en los endpoints. Es posible también especificar filtros y límites del consumo de recursos. Es posible crear tantas configuraciones de agente como desee. Sin embargo, no se puede eliminar la configuración de agente predeterminada. La protección de endpoint de Symantec Data Loss Prevention debe contener por lo menos una configuración de agente.

Puede modificar la configuración predeterminada tantas veces como desee. Los grupos de agentes pueden utilizar solamente una configuración al mismo tiempo. Sin embargo, puede asociar una configuración de agente a varios grupos de agentes. Es posible también clonar la configuración de agente.

Overview

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 139 Configuración de agentes.

Nos dirigimos a la siguiente ruta System>Agents>Overview.

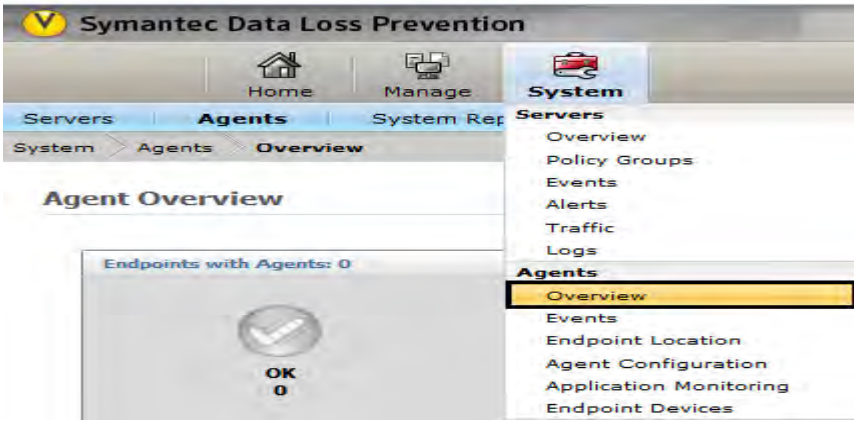


Figura 140 Configuración de agentes.

En este apartado podemos ver información de los estados del agente.

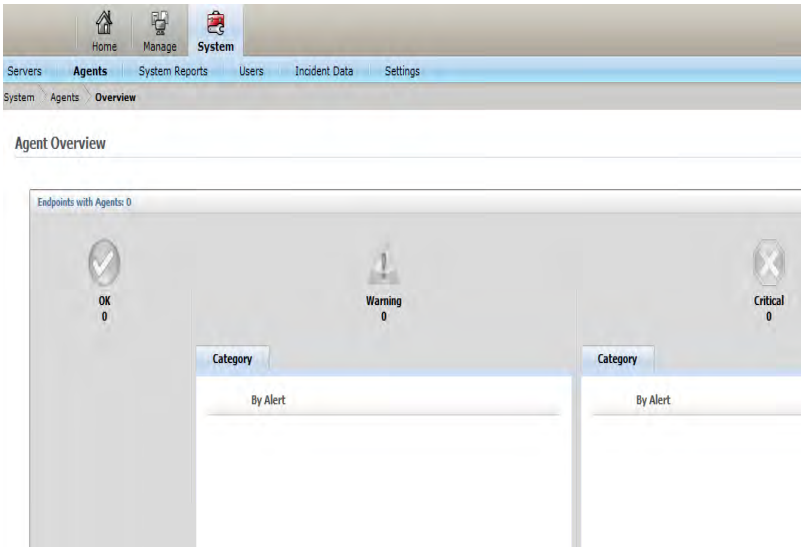


Figura 141 Configuración de agentes.

Estados del agente.

El estado Correcto indica que los Agentes DLP en este estado están funcionando en condiciones normales. Este estado indica:

■ Que los servicios y los controladores del sistema de archivos del Agente DLP están en ejecución.
■ Que la memoria caché del Agente DLP está creada y disponible.
■ Que el Agente DLP informa al Servidor de endpoints según lo esperado.

Un estado Advertencia indica que los agentes DLP en este estado han experimentado condiciones que pueden requerir atención.
Las alertas del agente de advertencia generalmente incluyen lo siguiente:
■ Versión anterior del Agente DLP
■ Error de resolución del grupo de Active Directory
■ Se ha producido un error de complemento
■ El Agente DLP necesita ser reiniciado

Un estado Crítico indica que los agentes DLP en este estado han experimentado condiciones que requieren atención inmediata:
■ Un controlador no está en ejecución
■ La versión de Agente DLP no es compatible con Servidor de endpoints

■ Los permisos de Active Directory están en conflicto con los permisos de Symantec Data Loss Prevention.

■ El Agente DLP no puede informar al Servidor de endpoints

La sección siguiente proporciona una lista completa de estado Crítico.

Creación de Usuarios.

Ingresar a la Consola de DLP con las credenciales válidas de Administrator.

Figura 142 Creación de usuarios.

En la consola de DLP, ir a System > Login Management > DLP Users

Figura 143 Creación de usuarios.

Se muestra una pantalla con los usuarios dados de alta y el botón “Add User” que sirve para agregar nuevos usuarios a la Consola de DLP, en este caso vamos agregar al usuario Administrador de Sistema.

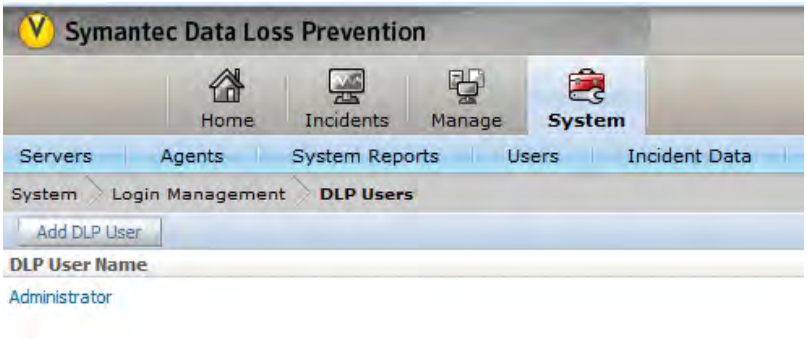


Figura 144 Creación de usuarios.

Presionamos el botón de “Add User”.

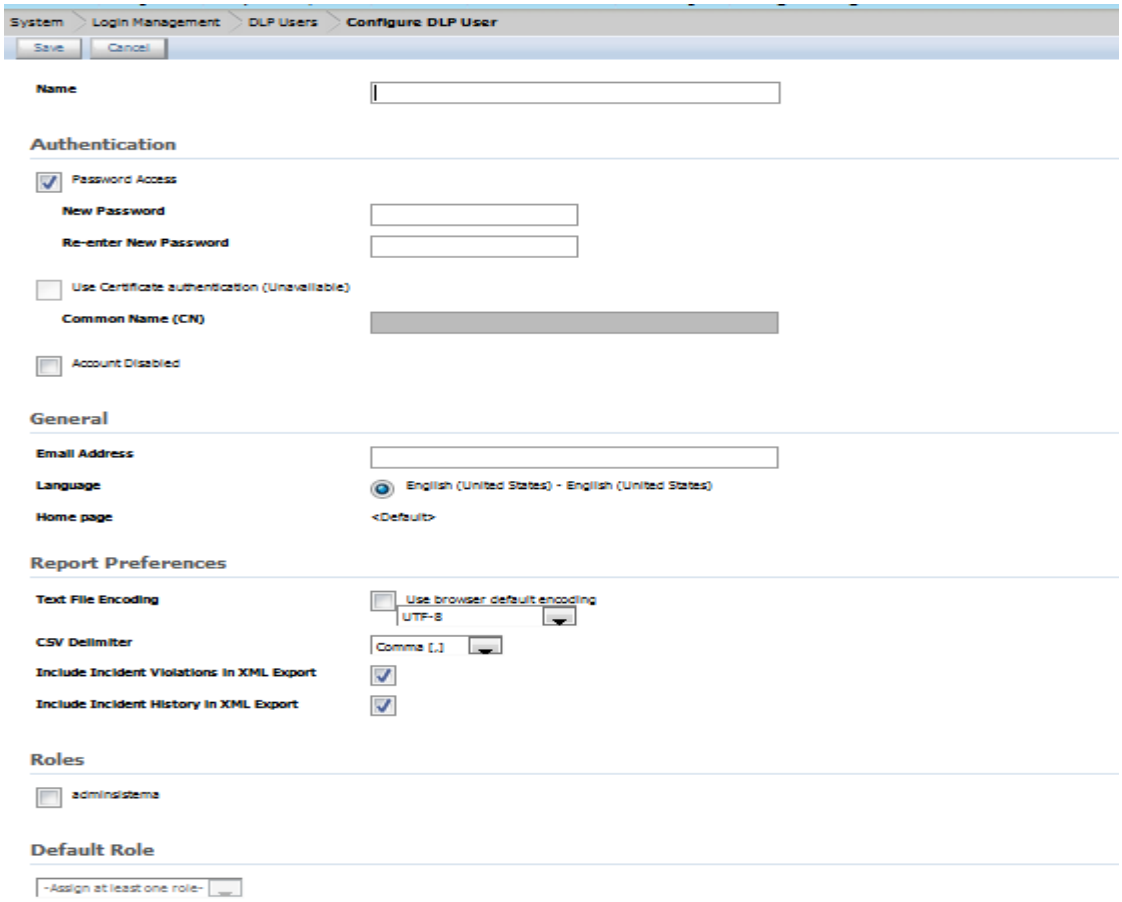


Figura 145 Creación de usuarios.

Se despliega una pantalla en la que se puede establecer las características de la nueva cuenta de usuario:

Name: Nombre de la cuenta de usuario

Authentication: La manera en que el usuario se autenticará el usuario.

General: Correo del usuario e idioma.

Report Preferences: Configuraciones pertinentes a los reportes, por lo general no se requiere modificar las que vienen por defecto.

Roles: El rol1 que se aplicará a la cuenta de usuario, es decir, lo que el nuevo usuario podrá realizar cuando acceda a la Consola de DLP.

Una vez que se configuran las opciones de la cuenta, se presiona el botón “Save” para crear la cuenta de usuario, que podrá ser usada a partir de ese momento.

Roles.

Figura 146 Roles de usuarios.

Iniciar Sesión como Administrador del sistema.

Figura 147 Roles de usuarios.

Ir a la siguiente ruta System >User Management >Roles.

Figura 148 Roles de usuarios.

Dar clic en Add Role.

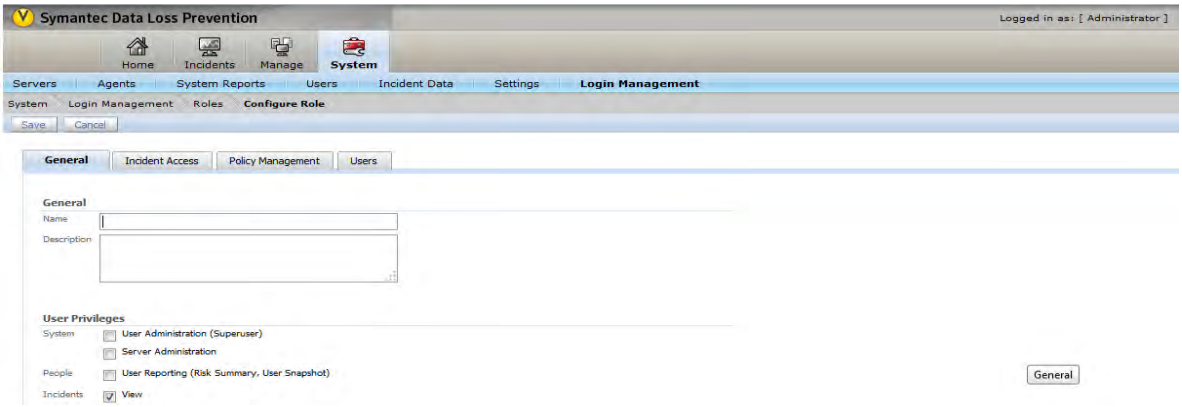


Figura 149 Roles de usuarios.

La pantalla Configurar rol aparece, mostrando las fichas siguientes: General, Acceso a incidente, Administración de políticas y Usuarios.

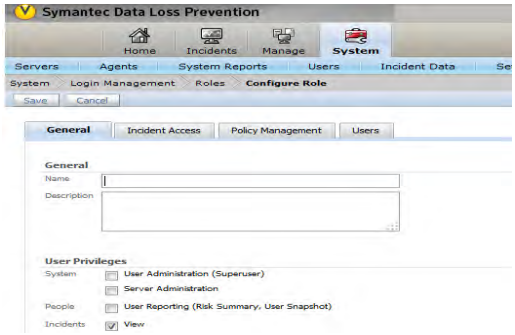


Figura 150 Roles de usuarios.

En la ficha General:

Escriba un Nombre único para el rol. El campo de nombre distingue entre mayúsculas y minúsculas, y se limita a 30 caracteres. El nombre que se escribe debe ser corto y descriptivo. Use el campo Descriptión para anotar el nombre del rol y para explicar su propósito más en detalle. El nombre del rol y la descripción aparece en la pantalla Lista de roles.

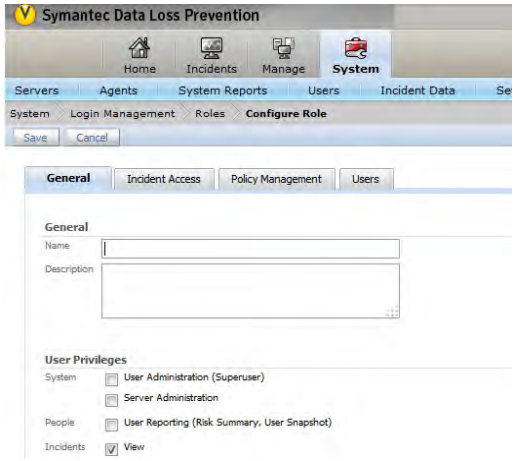


Figura 151 Roles de usuarios.

En la sección User privileges, se conceden los privilegios de usuario para el rol.

Privilegios del sistema:

Seleccione la opción User Administration para permitir a los usuarios crear roles adicionales y usuarios en Enforce Server.

Seleccione la opción Server Administration para permitir a los usuarios realizar las siguientes funciones:

Configurar los servidores de detección.

Crear y administrar perfiles de datos para Coincidencia de datos estructurados (EDM), Coincidencia de documentos indizados (IDM) y Aprendizaje de máquina vectorial (VML).

Configure y asigne los atributos del incidente.

Configure el sistema.

Configure las reglas de respuesta.

Cree los grupos de políticas.

Configure los protocolos del reconocimiento.

Consulte los informes de eventos e informes del sistema.

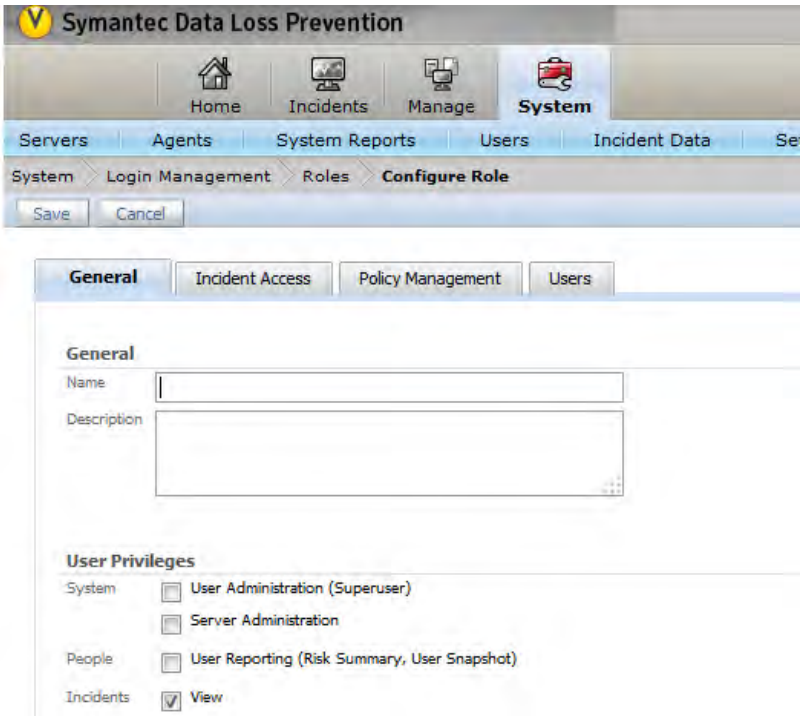


Figura 152 Roles de usuarios.

Privilegio People:

Seleccione la opción User Reporting para permitir a los usuarios ver el resumen de riesgo del usuario.

Nota: El privilegio Incidente > Ver se habilita de forma automática para todos los tipos de incidente de los usuarios con el privilegio User Reporting.

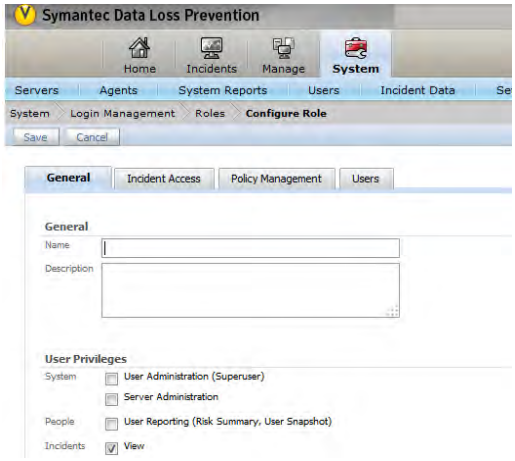


Figura 153 Roles de usuarios.

En la sección Incidents, se concede a usuarios con este rol los privilegios siguientes del incidente: Esta configuración se aplica a todos los informes de incidente en el sistema, incluido el resumen ejecutivo, el resumen de incidentes, la lista de incidentes y las instantáneas de incidentes.

Seleccione la opción View para permitir a los usuarios con este rol ver incidentes de la infracción de políticas. Es posible personalizar el acceso de visualización de incidentes seleccionando diversas opciones de Acciones y Mostrar atributo de la siguiente manera:

De forma predeterminada, se habilita la opción View (seleccionada) para todos los tipos de incidentes: Incidentes de Network, Incidentes de Discover, Incidentes de Endpoint, Incidentes de Mobile y Eventos de clasificación.

Para restringir el acceso de visualización solamente a ciertos tipos de incidentes, seleccione el tipo de incidente que desee autorizar para que este rol pueda ver. (Mantenga presionada la tecla Ctrl para hacer varias selecciones). Si un rol no permite que un usuario vea la parte de un informe de incidentes, la opción se reemplaza con “No autorizó” o está en blanco.

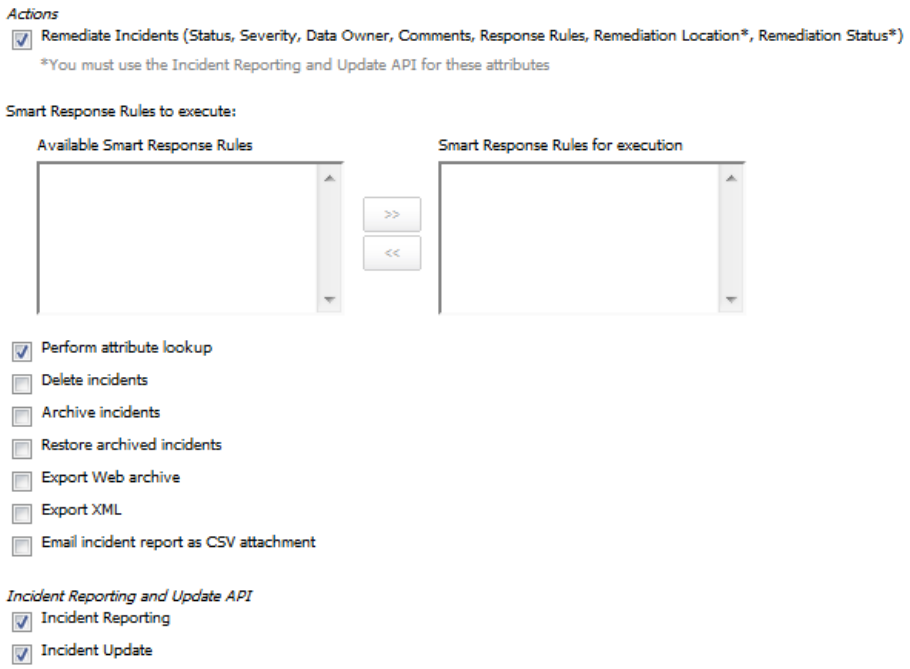


Figura 154 Roles de usuarios.

Seleccione entre las Actions siguientes para personalizar las acciones que un usuario puede realizar cuando ocurre un incidente:

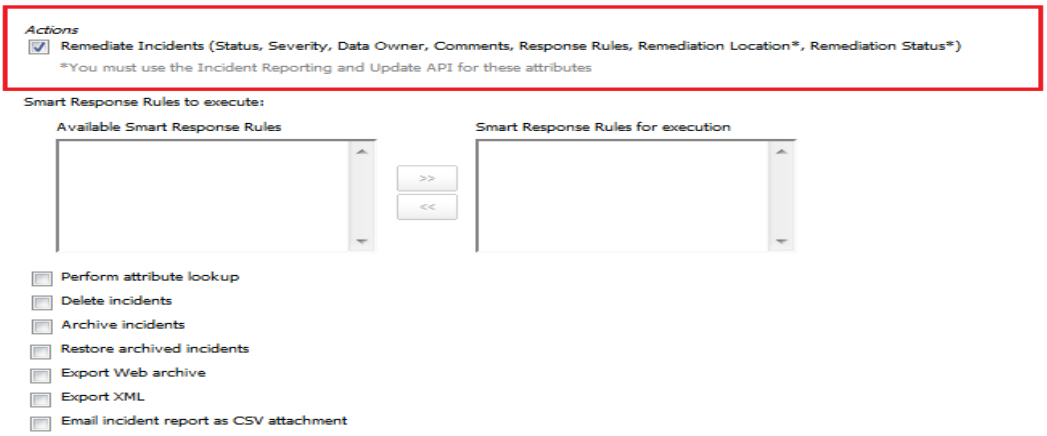


Figura 155 Roles de usuarios.

Remediate Incidents: Este privilegio permite a los usuarios cambiar el estado o la gravedad de un incidente, configurar un propietario de los datos, agregar un comentario al historial del incidente, configurar las opciones No archivar y Permitir archivar, y ejecutar acciones de la regla de respuesta. Además, si usted está utilizando la elaboración de informes de incidente y la API de actualización, seleccione este privilegio para reparar los atributos de ubicación y estado.

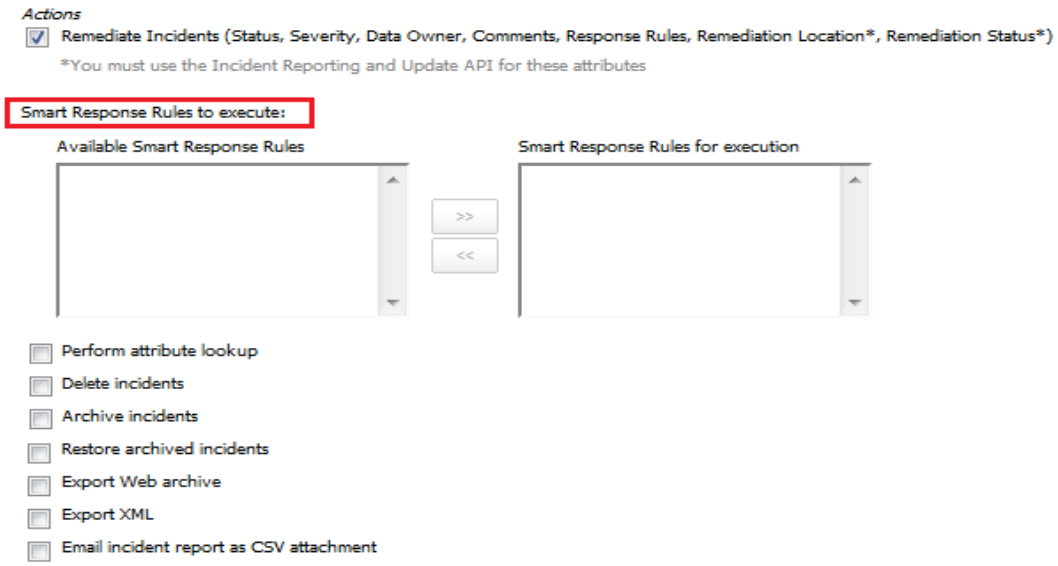


Figura 156 Roles de usuarios.

Smart Response Rules to execute: Se especifica qué reglas de respuesta inteligente puede ejecutar en base al rol. Las reglas de respuesta inteligente configuradas se detallan en la columna de "Disponible" a la izquierda. Para exponer una regla de respuesta inteligente para su ejecución por parte de un usuario de este rol, selecciónela y haga clic en la flecha para agregarla a la columna derecha. Use la tecla CTRL para seleccionar varias reglas.

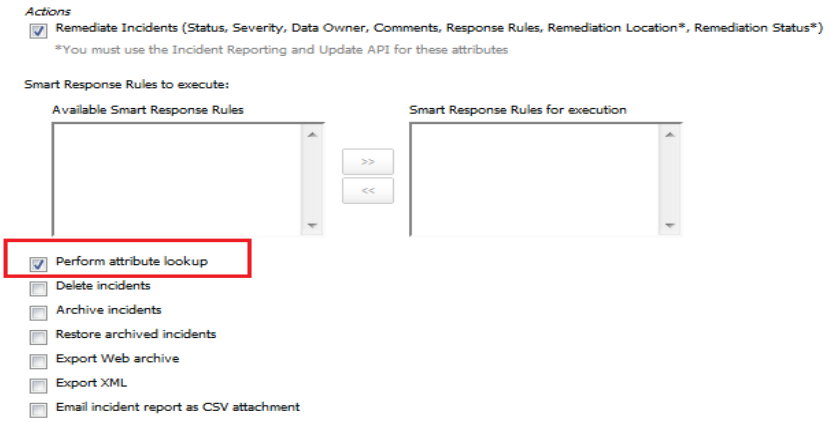


Figura 157 Roles de usuarios.

Perform attribute lookup: Permite a los usuarios buscar los atributos del incidente de los orígenes externos y completar los valores para la reparación del incidente.

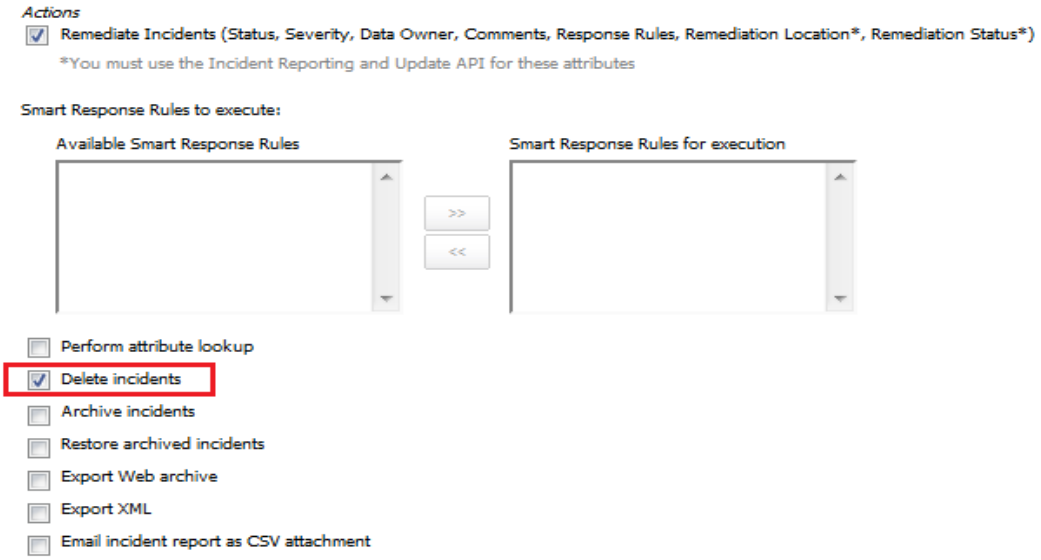


Figura 158 Roles de usuarios.

Delete incidents: Permite a los usuarios eliminar un incidente.

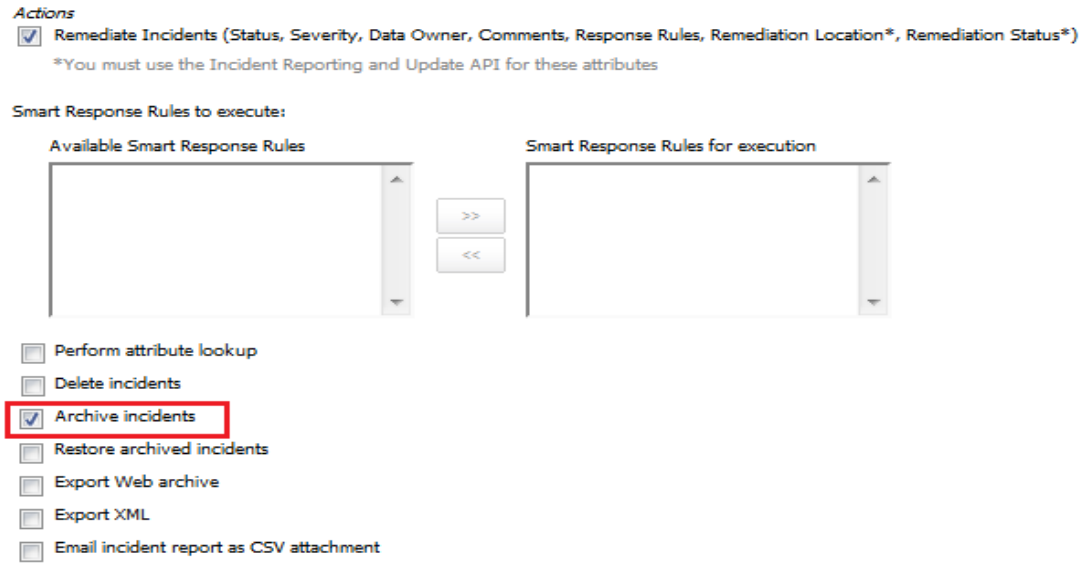


Figura 159 Roles de usuarios.

Archive incidents: Permite a los usuarios archivar un incidente.

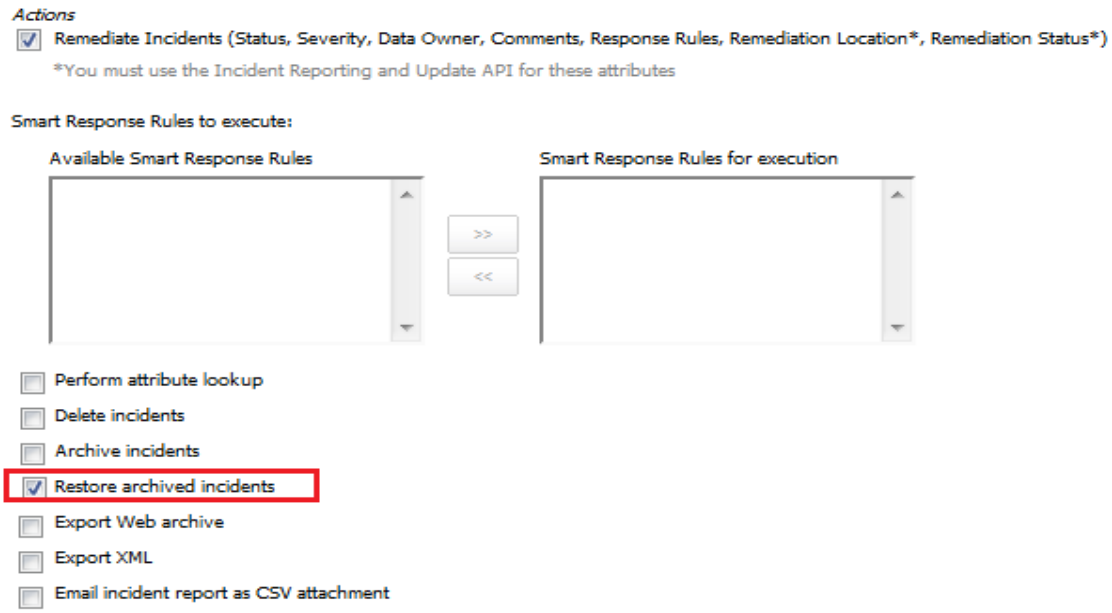


Figura 160 Roles de usuarios.

Restore archived incidents: Permite a los usuarios restaurar incidentes previamente archivados.

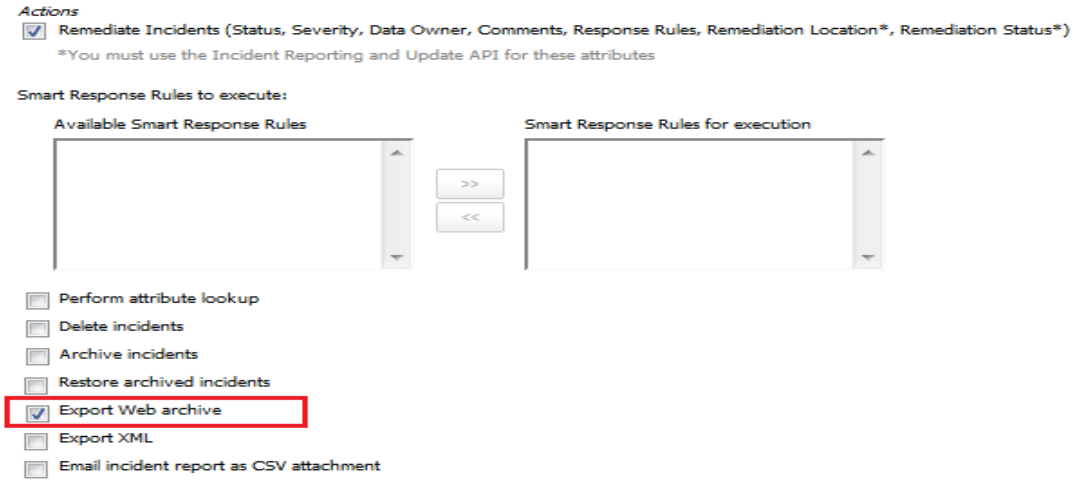


Figura 161 Roles de usuarios.

Export Web archive: Permite a los usuarios exportar un informe que el sistema compila de un archivo de almacenamiento web de incidentes.

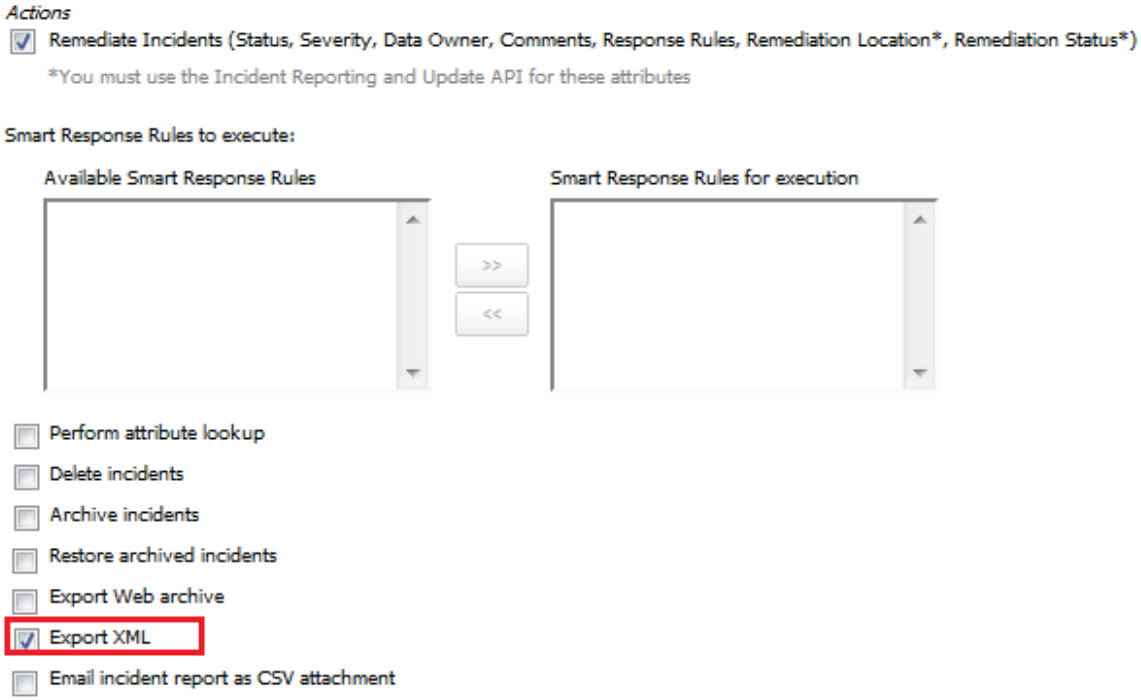


Figura 162 Roles de usuarios.

Export XML: Permite a los usuarios exportar un informe de incidentes en el formato XML.

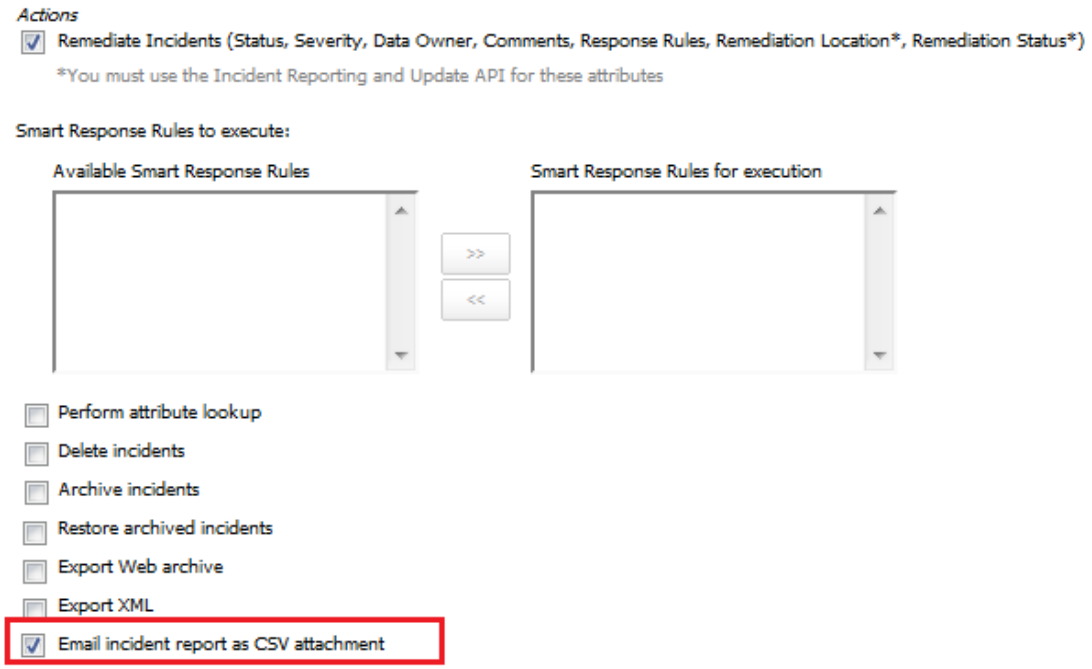


Figura 163 Roles de usuarios.

Email incident report as CSV attachment: Permite a los usuarios enviar por correo electrónico como archivo adjunto un informe que contiene una lista de detalles de incidentes separados por comas.

Manager Policies.

Se implementan políticas para detectar y evitar pérdida de datos. Una política Symantec Data Loss Prevention combina reglas de detección y acciones de respuesta. Si se infringe una regla de política, el sistema genera un incidente que puede informar y sobre el cual puede actuar. Las reglas de políticas que se implementan se basan en los objetivos de seguridad de la información. Las acciones que toma en respuesta a las infracciones de políticas se basan en los requisitos de cumplimiento. La consola de administración de Enforce Server proporciona una interfaz centralizada, intuitiva y basada en Web para la autoría de políticas.

Policy List.

Creación de políticas.

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 164 Interfaz para la creación de políticas.

Nos dirigimos a la siguiente ruta Manage>Policies>Policy list

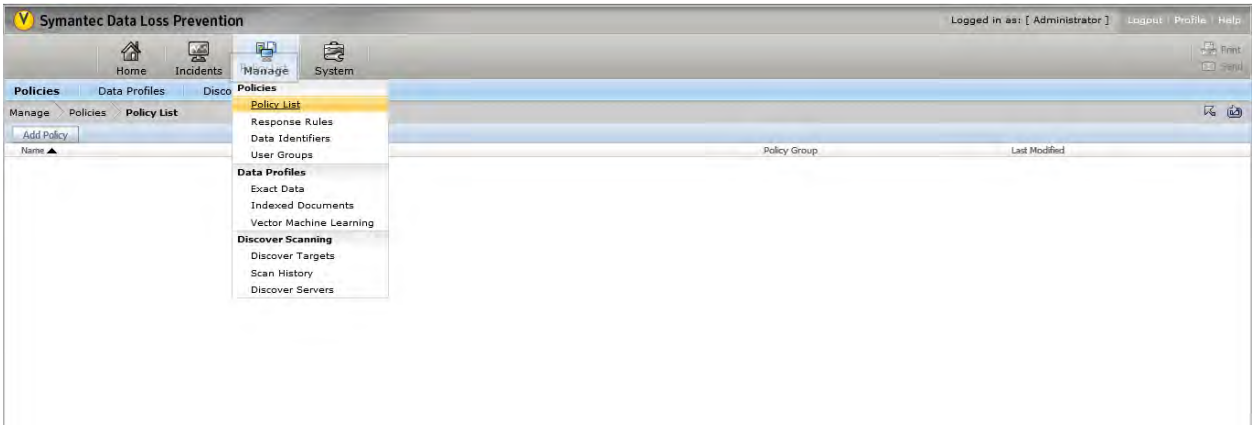


Figura 165 En Manage – Policies para creación de políticas.

Seleccionar Add Policy , Ingresar el nombre, la descripción de la política y seleccionar en el campo de Policy Group Default Policy Group.

Nota: para este caso utilizaremos la siguiente información.

Name: RFC

Descripción: Regla que se encarga de detectar la existencia de un RFC. Es una regla compuesta por palabras claves acompañada de una expresión regular, se construyó a partir de un patrón que genera RFCs.

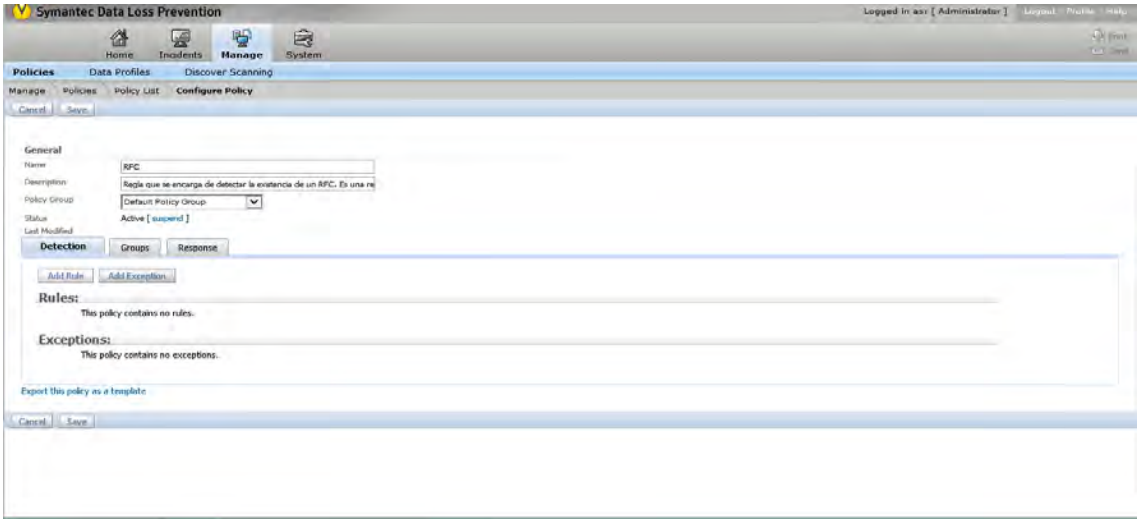


Figura 166 Se define la regla para la creación de políticas.

Dar clic en Save.

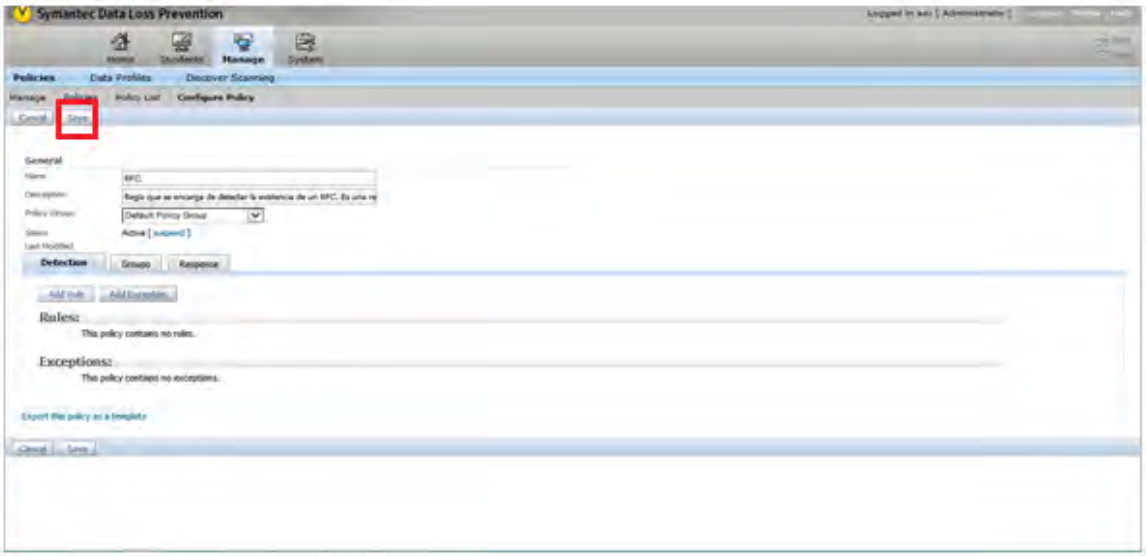


Figura 167 Salvamos la configuración.

Para finalizar nos debe de aparecer una ventana en donde se muestra que se guardaron nuestros cambios satisfactoriamente.

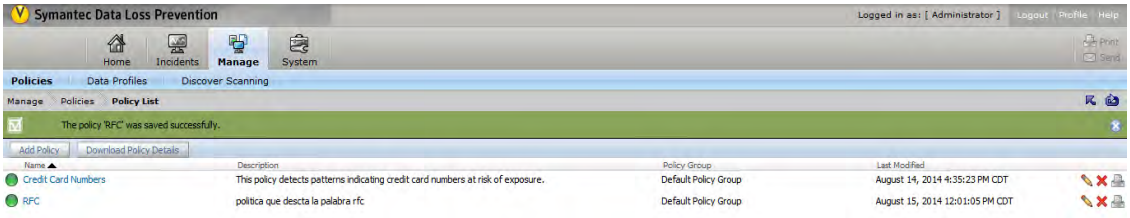


Figura 168 Refrescamos cambios.

Plantillas de políticas.

Symantec Data Loss Prevention proporciona plantillas de políticas para ayudarlo a implementar rápidamente políticas de detección en su empresa. Es posible compartir políticas a través de sistemas y entornos mediante la importación y la exportación de reglas y excepciones como plantillas.
Algunas plantillas de políticas se basan en los conjuntos bien conocidos de regulaciones, como el estándar de seguridad de la industria de tarjetas de pago, Gramm-Leach-Bliley, California SB1386 e HIPAA.
Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 169 Interfaz de DLP.

Nos dirigimos a la siguiente ruta Manage>Policies>Policy list

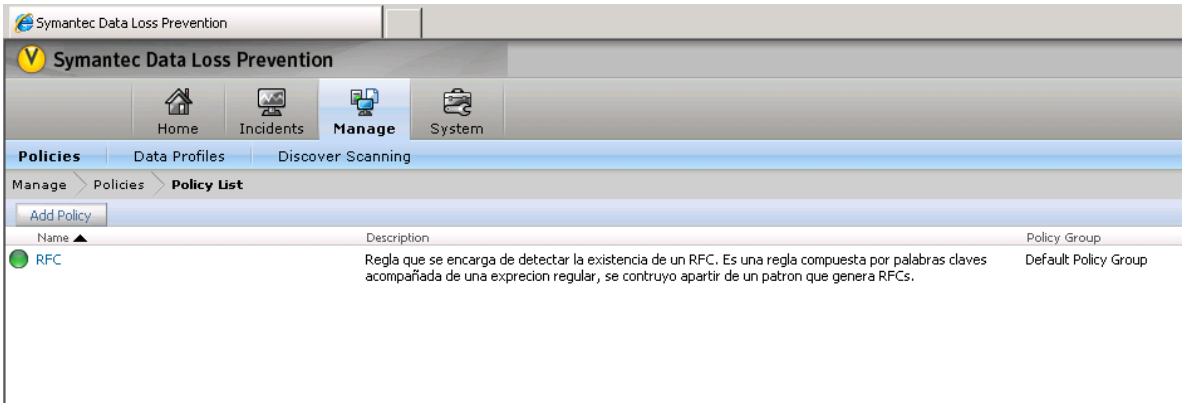


Figura 170 Entramos a Manage.

Seleccionar Add Policy.

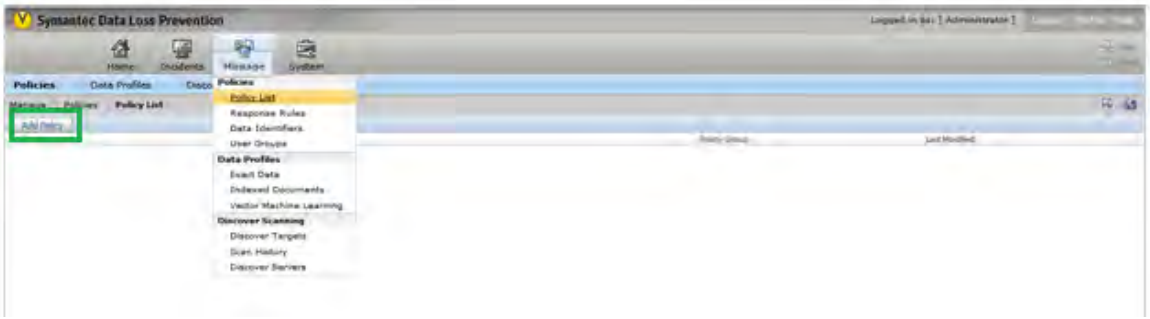


Figura 171 Agregamos políticas.

Seleccionar la opción Add a policy from template y damos clic en Next.

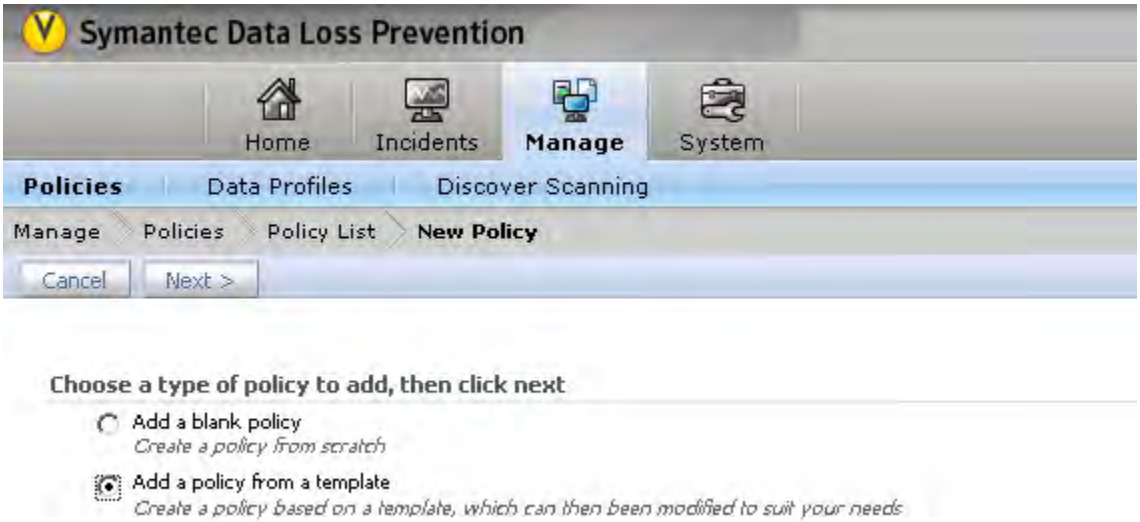


Figura 172 Utilizamos un template de políticas.

Marcamos la plantilla a utilizar, en este caso utilizaremos HIPAA, la seleccionamos y damos clic en Next.

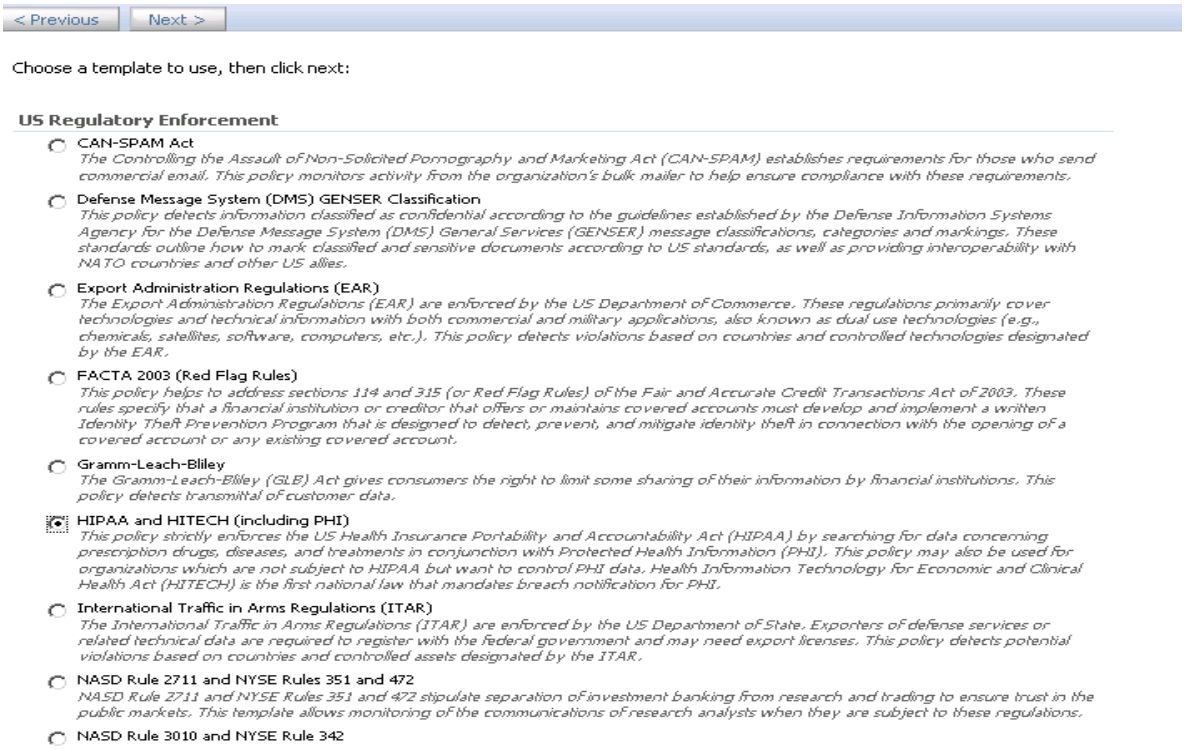


Figura 173 Plantillas HIPAA.

Damos clic en la ventana Next.

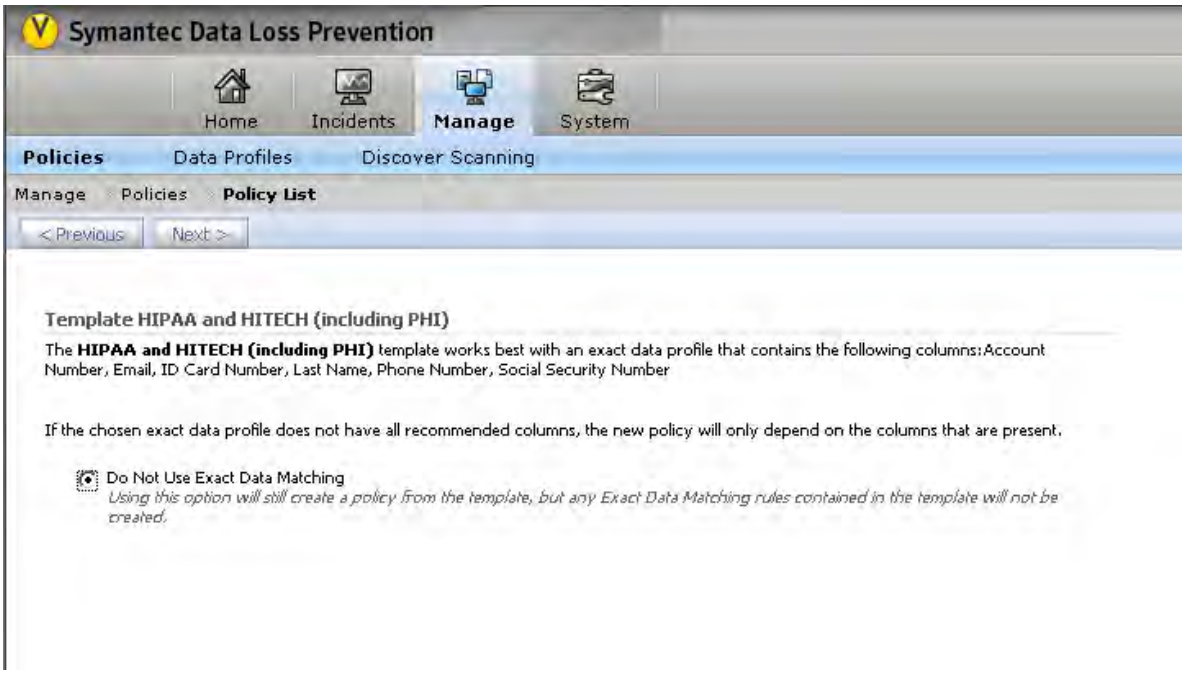


Figura 174 Template de plantillas HIPAA.

Dar clic en Save.

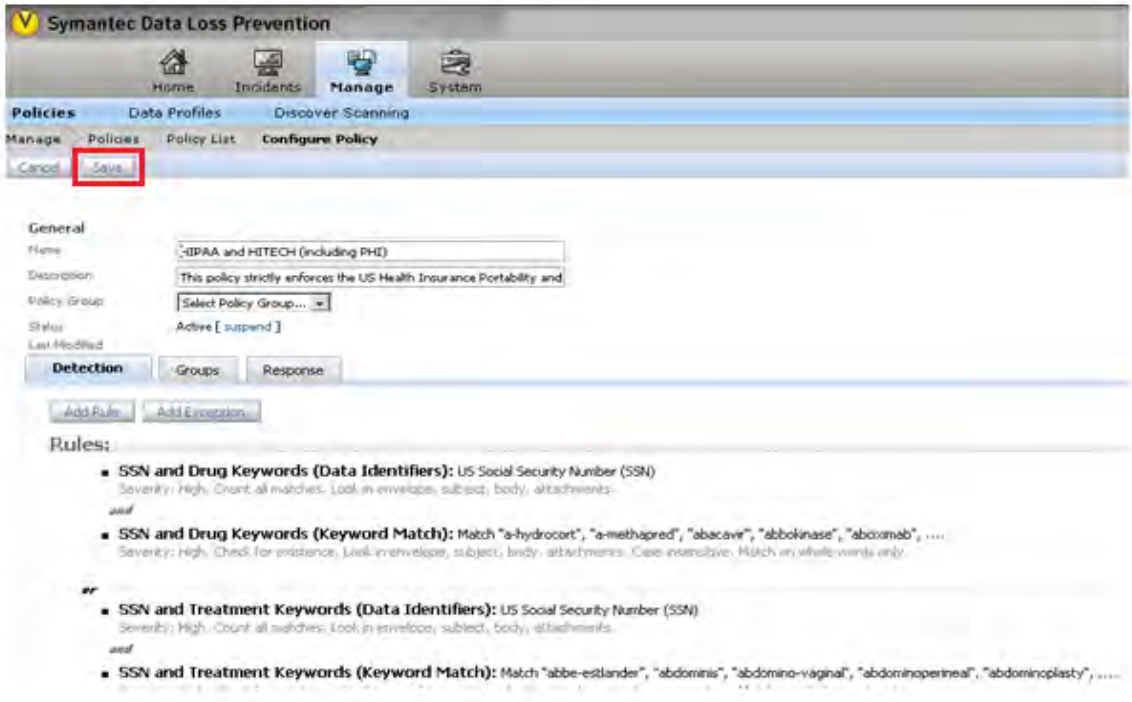


Figura 175 Salvamos Plantillas de políticas.

Para finalizar nos debe de aparecer una ventana en donde se muestra que se guardaron nuestros cambios satisfactoriamente.

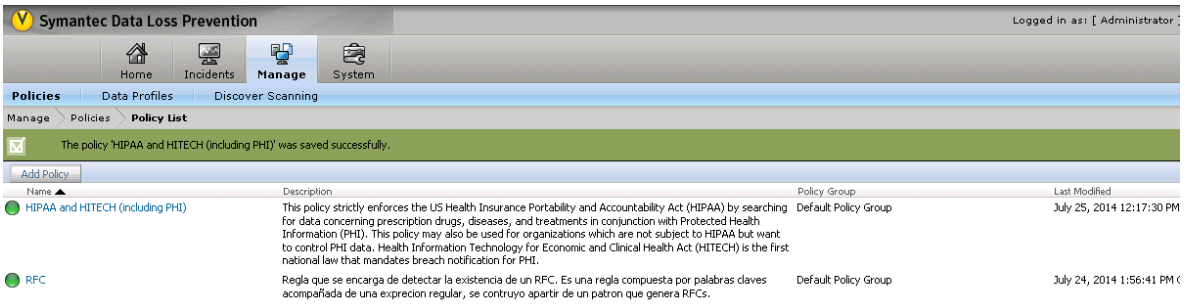


Figura 176 Actualizamos las políticas.

Configurar reglas.

Content Matches Keyword.

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

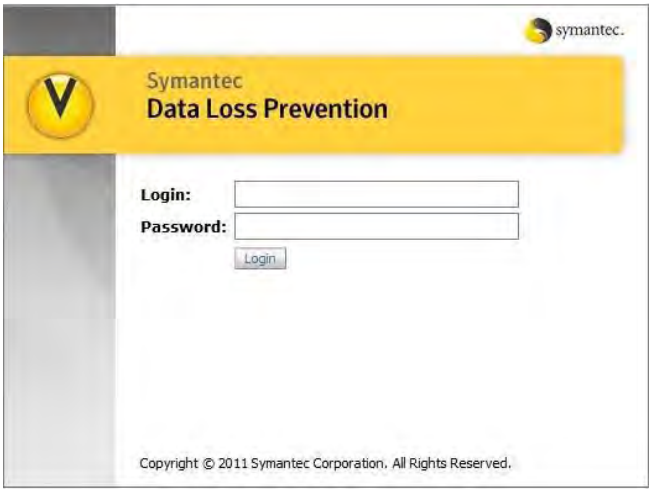


Figura 177 Configuración de Reglas.

Nos dirigimos a la siguiente ruta Manager>Policies>policies policy list> Configure policy

Seleccionamos una política y agregamos una regla en Add Rule.

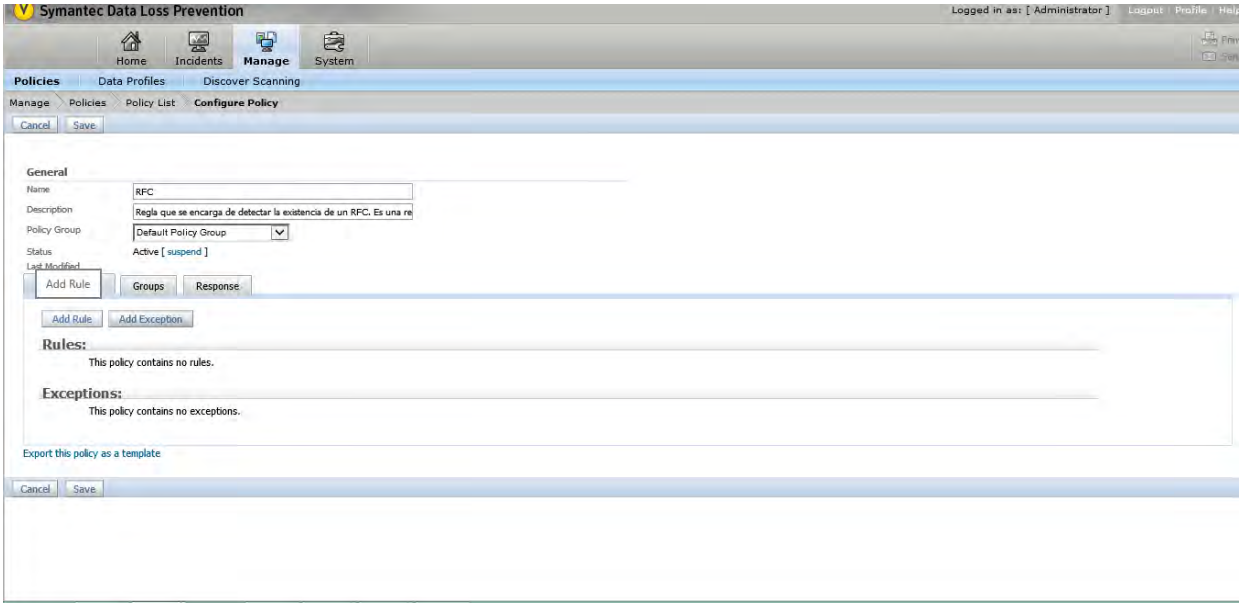


Figura 178 Agregar Reglas.

Seleccionar Content Matches Regular Expression.

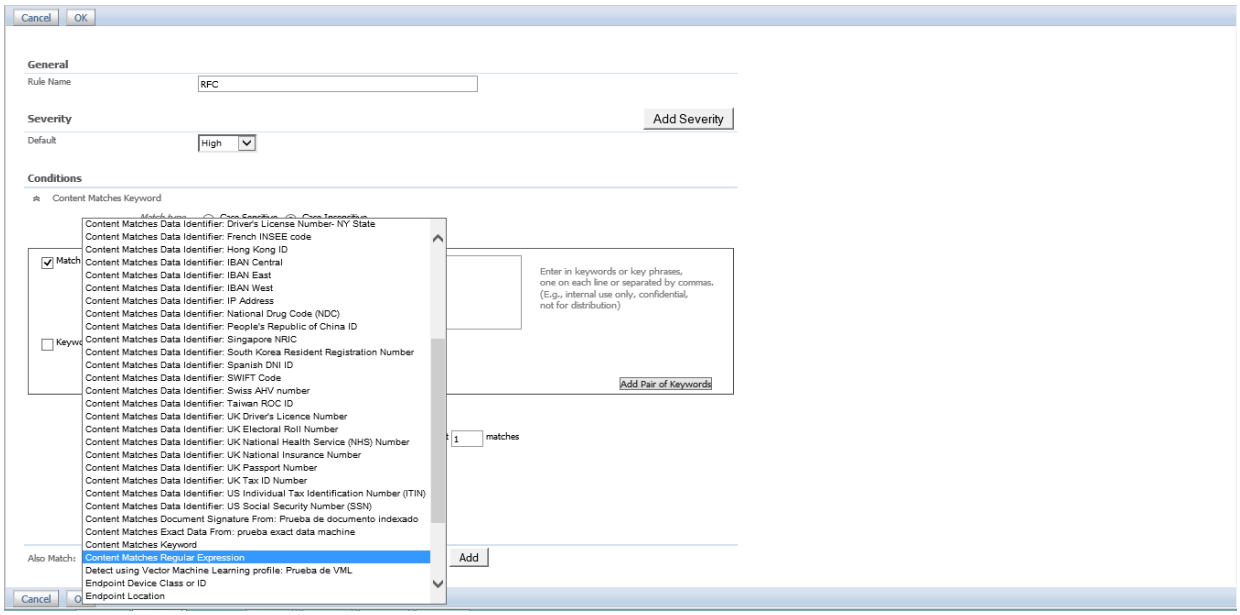


Figura 179 Configuración especializada de Reglas.

En el campo de Match Regular Expression, ingresar la expresión regular para el RFC.
(?i)([a-z][aeiou][a-z]{2}\d{2}((0[13578]|1[02])(0[1-9]|[12]\d|3[0-1])|(0[469]|11)(0[1-9]|[1-2]\d|30)|02(0[1-9]|1\d|2[1-9])))

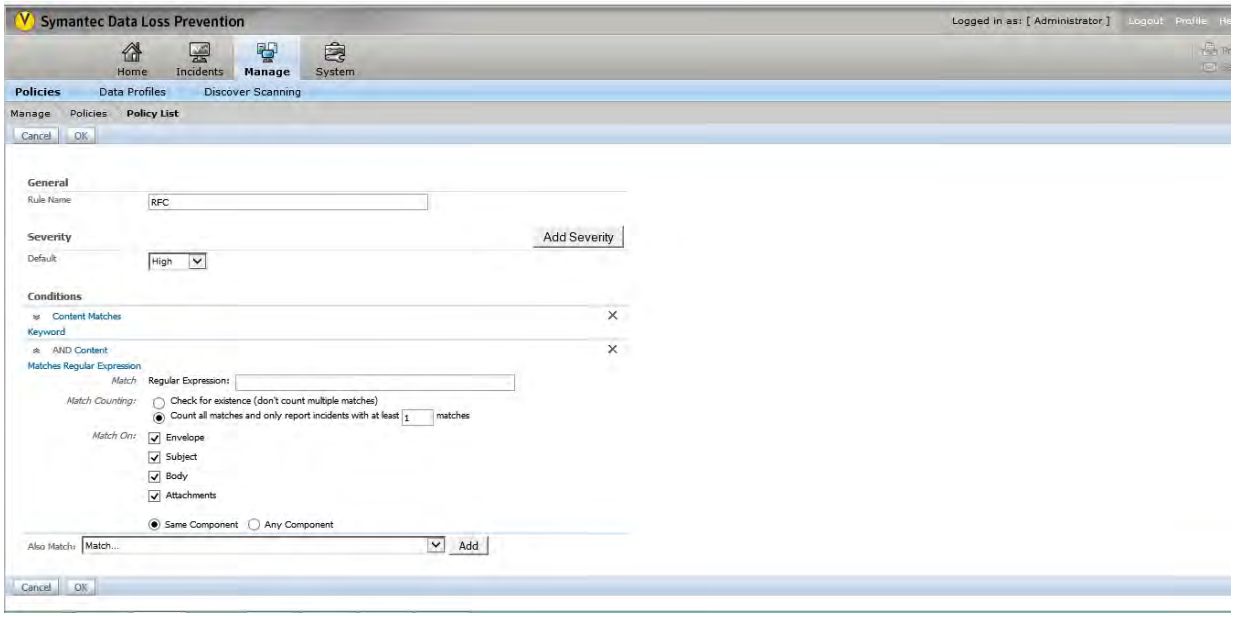


Figura 180 Expresión regular de una configuración de Reglas.

Dar clic en Ok.

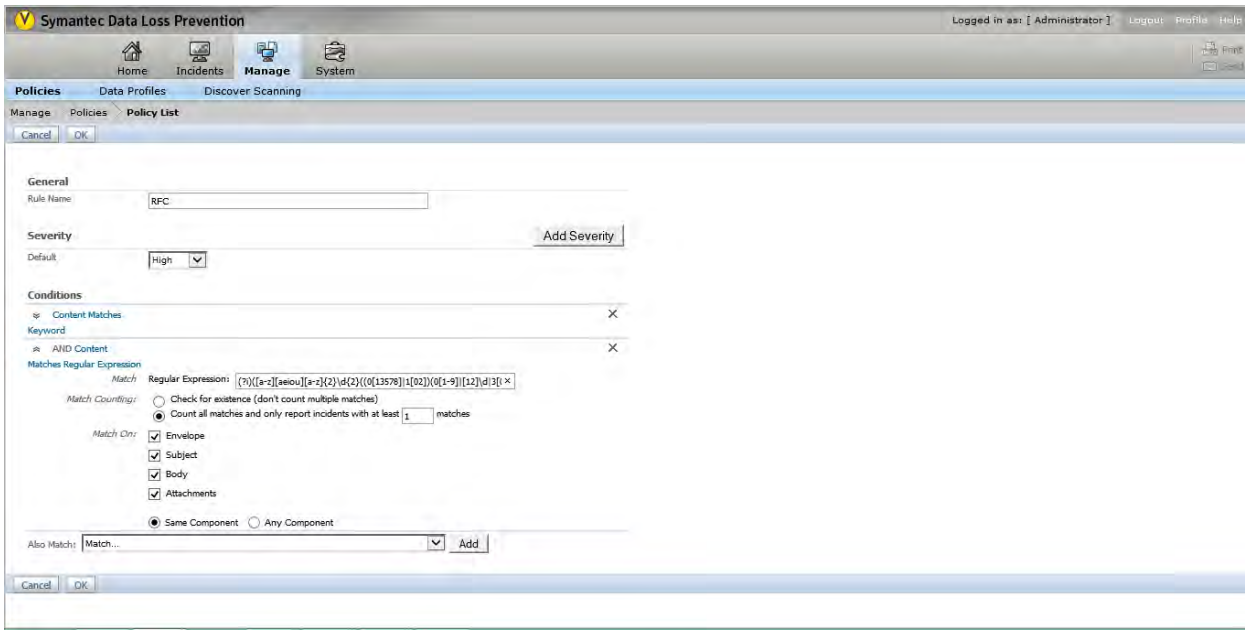


Figura 181 Verificamos la Configuración de Reglas

Dar clic en Save

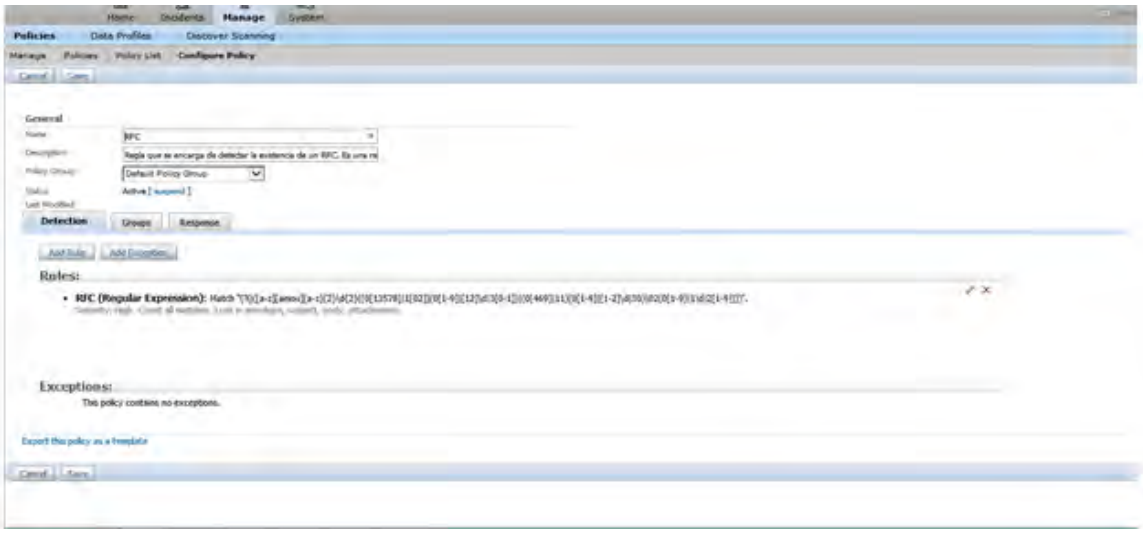


Figura 182 Guardamos Configuración de Reglas.

Para finalizar nos debe de aparecer una ventana en donde se muestra que se guardaron nuestros cambios satisfactoriamente.

Figura 183 Actualizamos la configuración de Reglas.

Reglas de respuesta.

Las acciones de regla de respuesta son los componentes que toman medidas cuando ocurre una infracción de políticas. Las acciones de regla de respuesta son componentes obligatorios de reglas de respuesta. Si crea una regla de respuesta, deberá definir por lo menos una acción para que la regla de respuesta sea válida.

Configurar una Response Rule:

Ingresar a la Consola de DLP con las credenciales válidas proporcionadas al Administrador total.

Figura 184 Reglas de respuesta.

Nos dirigimos a la siguiente ruta Manage>Policies>Response Rules.

Figura 185 Reglas de respuesta.

Seleccionar Add Response Rule.

Figura 186 Reglas de respuesta.

Seleccionar Automated Response y dar click en Next.

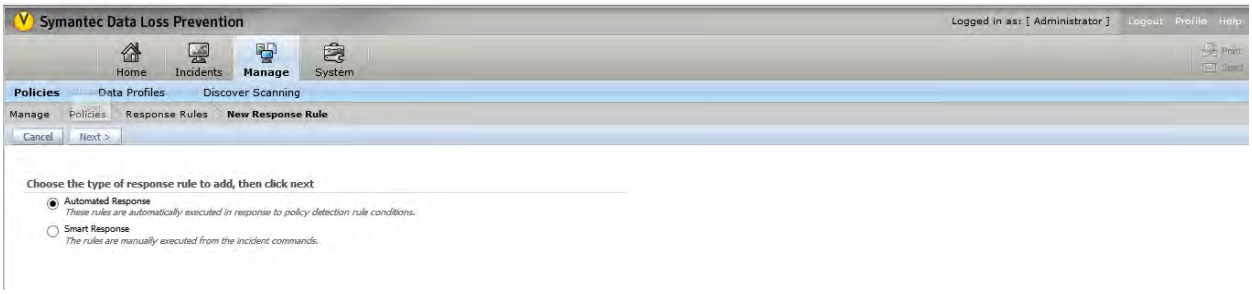


Figura 187 Reglas de respuesta.

Ingresar el campo solicitado de Rule Name y Description.

Nota: para este caso se utilizó la siguiente información.

Name: BLOQUEO SMTP.

Description: En esta regla se impide la salida de correos que violen esta política.

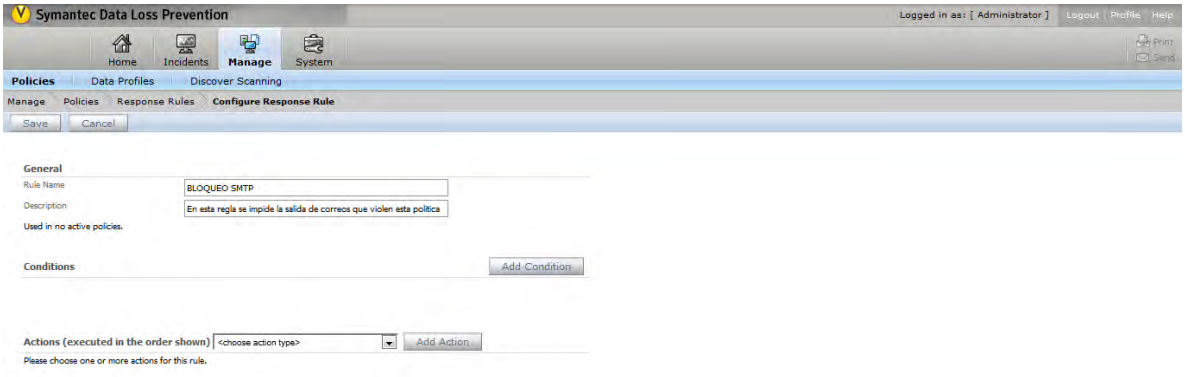


Figura 188 Reglas de respuesta.

Dar clic en Add Condition.

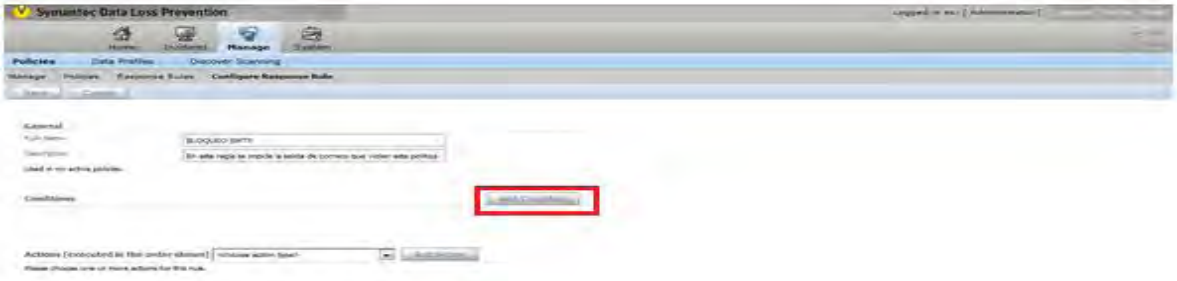


Figura 189 Reglas de respuesta.

Seleccionar Incident Type.

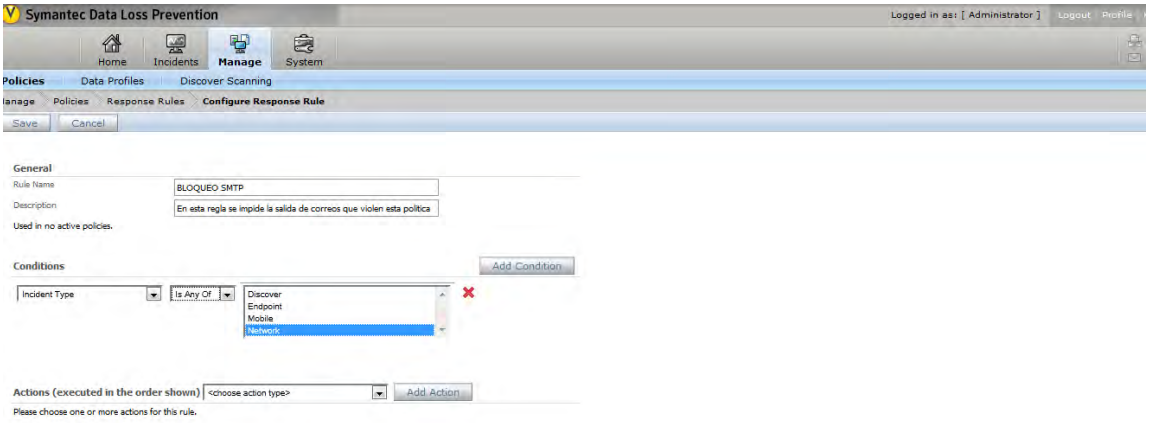


Figura 190 Reglas de respuesta.

Seleccionar Is Any Of de la lista central.

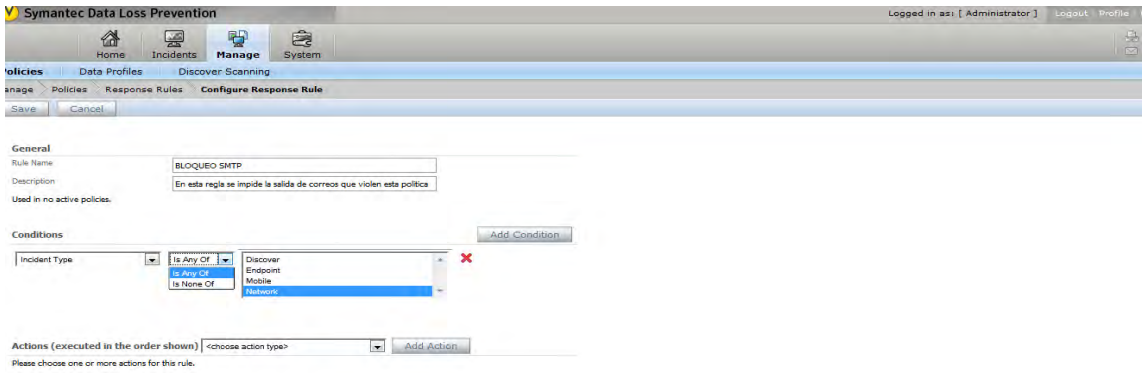


Figura 191 Reglas de respuesta.

Seleccionar Network en la lista de la derecha.

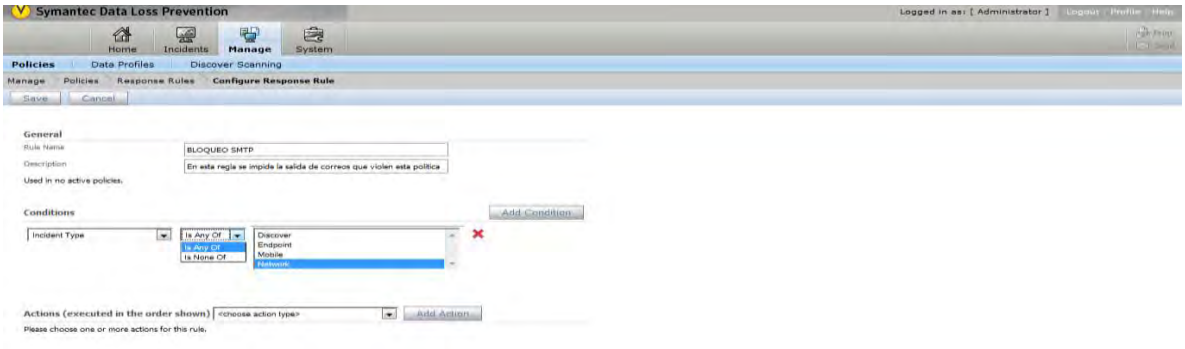


Figura 192 Reglas de respuesta.

En la opción de <choose action type> seleccionar Block SMTP Message.

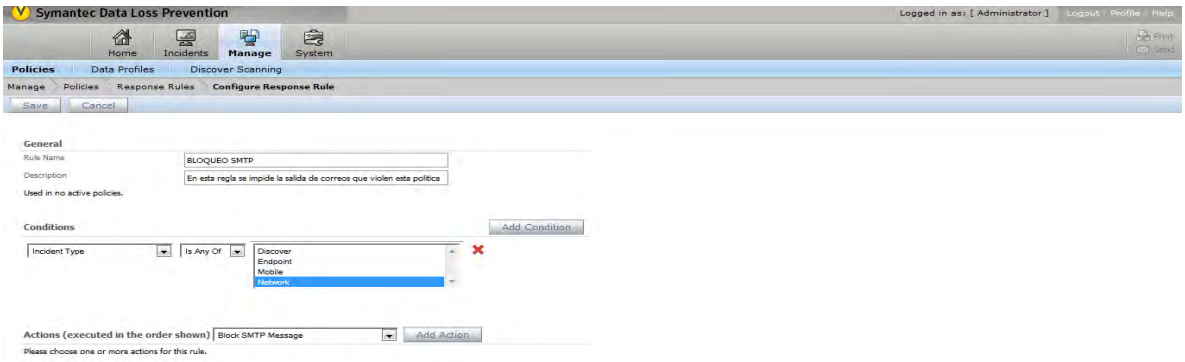


Figura 193 Reglas de respuesta.

Damos clic en la ventana Add Condition.

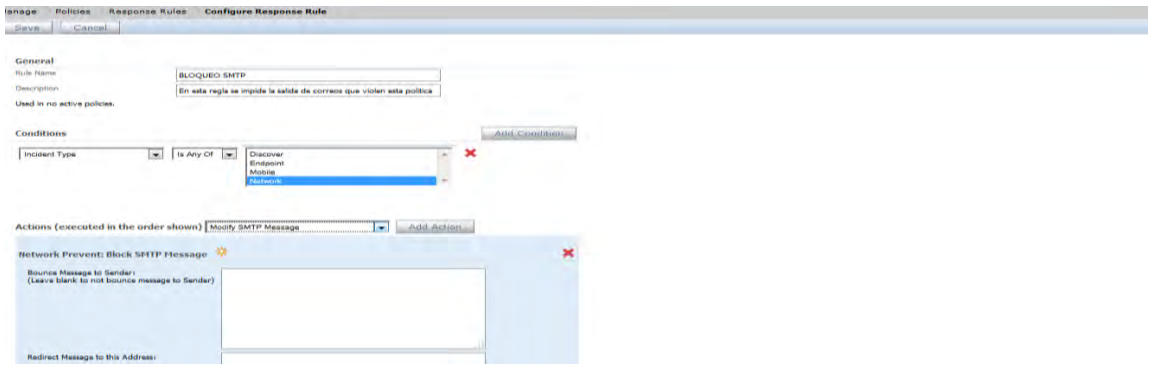


Figura 194 Reglas de respuesta.

En la opción de Bounce Message Sender: Escribir un mensaje para el usuario que trato de sacar información sensible.

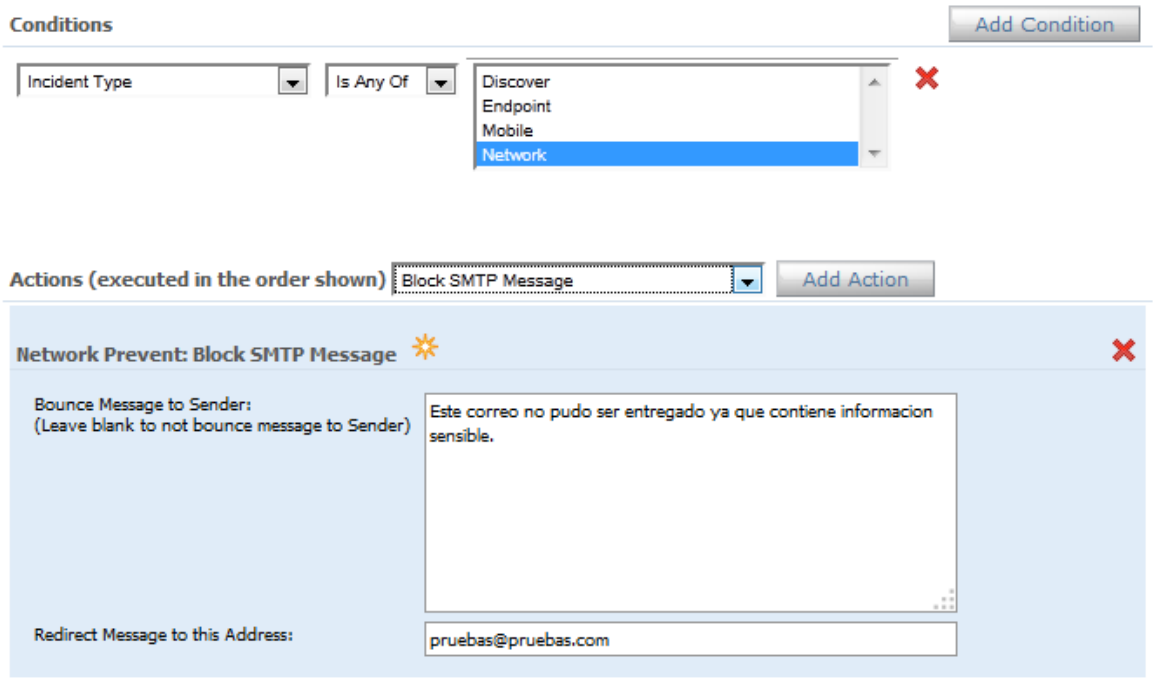


Figura 195 Reglas de respuesta.

En la opción Redirect Message to this Addresss escribimos el correo de la persona a la que queremos re direccionar la notificación anterior.

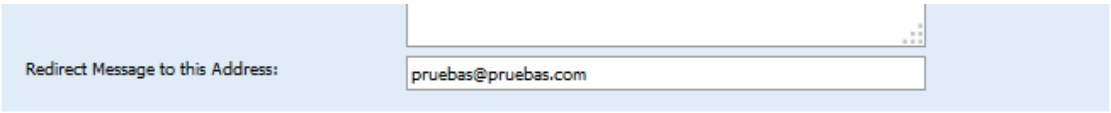


Figura 196 Reglas de respuesta.

Dar clic en Save

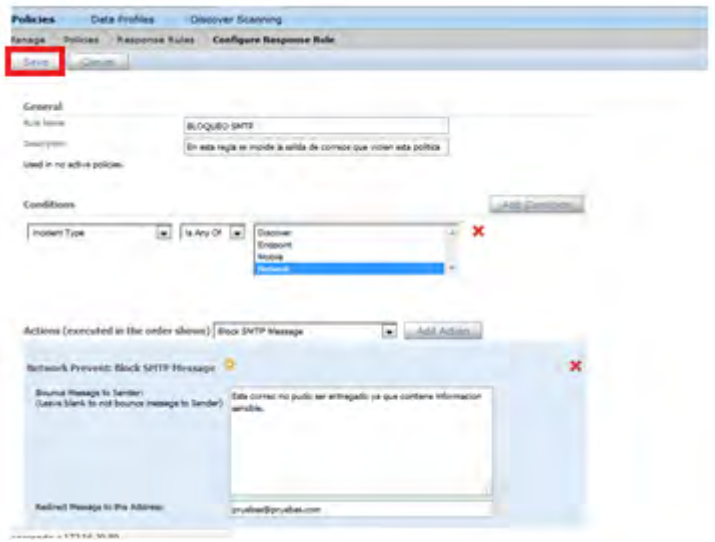


Figura 197 Reglas de respuesta.

Para finalizar nos debe de aparecer una ventana en donde se muestra que se guardaron nuestros cambios satisfactoriamente.

Figura 198 Reglas de respuesta.

CONCLUSIONES.

Alan Daniel Godínez Chávez:

Durante este Trabajo de tesis hemos tenido la posibilidad de valorar los diferentes estudios y criterios sobre la pérdida de datos. Desafortunadamente en las empresas de México y del mundo siempre la fuga o perdida de datos está latente, por lo que las empresas y gobiernos pierden mucho dinero ya que la información es dinero. DLP es un instrumento en su clase la cual nos ayuda con estos problemas que sufren las empresas y gobiernos.

Mediante políticas previamente creadas en la herramienta se puede bloquear la extracción de información por cualquier medio, (CD, pendrive, ftp, correos etc.), dando un índice de seguridad óptima. Permite que en un ambiente con esta herramienta en uso no exista la perdida de información, por lo que es muy importante tenerla tanto como seguridad y como rentable.
Se llevó a cabo un análisis detallado para seleccionar esta herramienta ya que en el ámbito profesional es una de las que mejor da resultado.

En cuanto en el perfil económico es muy rentable implementarla ya que no existe mucho conocimiento por lo que deja una buena ganancia, y en cuestión para las empresas y Gobiernos su retorno de inversión es prácticamente instantáneo ya que en el momento que se implementa ya no hay fugas de información obteniendo nada de pérdida monetaria.

1. El primer paso que se debe de seguir es verificar si la empresa cuenta con información sensible, peligrosa o bien confidencial.
2. Ofrecer DLP, herramienta potencial contra perdida de datos a la empresa.
3. Realizar un levantamiento.
4. Concluir con el proyecto.

De esta manera, se concluye que la herramienta DLP es la mejor opción para asegurar la perdida de Información de cualquier empresa, y al mismo tiempo siguiendo los lineamientos que se plantearon en el capítulo X, esto ahorra tiempo y costos significativos para el cliente final

Iván Olvera Espinoza:

En este proyecto pude aplicar y hacer uso de los conocimientos adquiridos en mi estancia en la facultad de ingeniería uno de los puntos más importantes sobre este proyecto es la Seguridad de la Información ya que es uno de los principales riesgos a los que nos enfrentamos actualmente, hoy en día nos encontramos que la información y los medios por los cuales viaja la información se ven amenazados por una cantidad infinita de factores, la fuga de información es uno de los factores que va en continuo aumento.

En esta investigación pude identificar algunos modelos para la prevención de fuga de información, uno de ellos es el que propone la solución de Symantec DLP, esta solución de divide en 4 vectores para la prevención:

Vector de red. (Monitoreo de la información que viaja en la red).
Vector de puntos finales. (Monitoreo de la información que viaja por medio de puntos finales).
Vector almacenamiento. (Monitoreo de información en repositorios).
Vector en la nube. (Monitoreo de aplicaciones en la nube y correo electrónico con Office365, etc).

Decimos utilizar el vector de puntos finales ya que de los 4 vectores mencionados es el más robusto debido a que podemos monitorear diferentes canales de comunicación (CD/DVD, copias locales, Printer/Fax, Clipboard, HTTPS, HTTP,SMTP, FTP, copias a recursos compartidos, deshabilitar el Print Screen, etc). Todo esto con la finalidad de prevenir fuga de información por estos medios, esta protección la realiza por medio de un agente.

Un punto mi importante es que gracias a las reglas de respuesta que se pueden configurar en el Symantec DLP podemos apoyar a cualquier organización para que los usuarios comprendan que la seguridad de la información es responsabilidad de todos y no sólo del departamento de Seguridad Informática, además de que contiene mecanismos de medición de la efectividad de las políticas de detección generadas en la solución.

La mayoría de la fuga de información en las empresas es porque los usuarios no tienen conocimientos de protección de fuga de información, al contar con una herramienta de prevención de fuga de información podríamos hacer conciencia a los usuarios para el uso de información y tener una herramienta de protección para usuarios malintencionados.

GLOSARIO

DLP: Es una estrategia para asegurarse de que los usuarios finales no envían información sensible o crítica fuera de la red corporativa. El término también se utiliza para describir productos de software que ayudan a un administrador de red a controlar qué datos pueden transferir los usuarios finales.

USB: Un puerto USB funciona como dispositivo que facilita la conexión de periféricos y accesorios a una computadora, permitiendo el fácil intercambio de datos y la ejecución de operaciones.

TI: Tecnologías de la información o simplemente TI, es un amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información.

Amenaza: Se refiere a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

La Vulnerabilidad: Es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Nube: Se trata de un servicio que funciona a través de internet que permite a los usuarios guardar información cualquier tipo: música, videos, en General y poderlos tener alojados en servidores dedicados, es decir en equipos que siempre permanecen encendido las 24 horas del día y los 365 días del año.

PII: La información de identificación personal (PII) es cualquier dato que podría identificar potencialmente a un individuo específico. Cualquier información que puede ser utilizada para distinguir una persona de otra, y que puede ser usada para quitarle el anonimato a los datos anónimos puede ser considerada PII.

Carbonite: Un servicio de copias de seguridad remota, en línea o gestionado es un servicio que proporciona a la computadora de un usuario conexiones online con un sistema remoto para copiar y almacenar los ficheros de su computadora. Los proveedores de copias de seguridad gestionado son empresas que suministran este tipo de servicios.

Mozy: Las opciones por defecto traen una configuración según la cual se programa una copia dos veces al día, aunque tenemos acceso a los ajustes para modificar los períodos y la cantidad de copias. Su función principal es la de permitirnos restaurar nuestro archivo perdido.

Dropbox: Es un servicio gratuito de hasta 2 gigas para almacenamiento de archivos. Para más espacio existen tarifas diferentes.

Wikileaks: Es una organización mediática internacional sin ánimo de lucro, que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

IP: IP Es la sigla de Internet Protocol o, en nuestro idioma, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados. El IP no cuenta con la posibilidad de confirmar si un paquete de datos llegó a su destino.

SMTP: Es la sigla que corresponde a la expresión de la lengua inglesa Simple Mail Transfer Protocol. En nuestro idioma, dicho concepto puede traducirse como Protocolo para la Transferencia Simple de Correo. El SMTP es un protocolo de red que se emplea para enviar y recibir correos electrónicos (emails).

HTTP: El http son las siglas de “Hypertext Transfer Protocol” es un protocolo de transferencia donde se utiliza un sistema mediante el cual se permite la transferencia de información entre diferentes servicios y los clientes que utilizan páginas web.

HTTPS: Hypertext Transfer Protocol Secure (ó HTTPS) es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la WWW, generalmente para transacciones de pagos o cada vez que se intercambie información sensible (por ejemplo, claves) en internet.

FTP: Este protocolo de red llamado Protocolo de Transferencia de Archivos es como su nombre lo indica una de las formas en la cual podemos enviar archivos hacia una Red TCP (siglas en inglés de Transmission Control Protocol) en la que utilizaremos la clásica arquitectura de Cliente - Servidor para dicha transferencia. De este modo, tenemos desde nuestra computadora que oficiará como Cliente la posibilidad de poder establecer un vínculo con un Servidor remoto para poder o bien descargar archivos desde esta dirección de destino.

Telnet: Es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente.

Nodo: En las Redes de computadoras de área local, es un dispositivo que se encuentra conectado a las Conexiones de red con la capacidad de poder comunicarse con los diferentes dispositivos que se encuentren en la misma.

Hotmail: Es el nombre de un proveedor de cuenta de correo electrónico gratuito y de pago fundado en 1995 por Jack Smith y Sabeer Bhatia en 1995. Fue el primer sistema tipo webmail.

Gmail: Es un servicio gratuito del buscador Google que nos permite crearnos una cuenta de correo electrónico accesible desde cualquier lugar del mundo con acceso a Internet (webmail).

Apple: Es una empresa multinacional estadounidense que diseña y produce equipos electrónicos y software, con sede en Cupertino (California, Estados Unidos) y otra pequeña en Dublín (Irlanda).

IBM: Es empresa de tecnología y consultoría más grande del mundo, con sede en Armonk, Nueva York, Estados Unidos. Sus productos incluyen hardware y software para la línea de servidores empresariales, productos de almacenamiento, microchips diseñados a la medida y software de aplicación.

ADSL: Es una clase de tecnología que permite la conexión a Internet mediante el uso de la línea telefónica tradicional, transmitiendo la información digital de modo analógico a través del cable de pares simétricos de cobre.

Pentium: Es una gama de microprocesadores de arquitectura x86 desarrollados por Intel. Posee versiones de un único núcleo y de multinúcleo.

FDDI (interfaz de datos distribuidos por fibra): Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida (WAN) o de área local (LAN), mediante cables de fibra óptica.

FireWire: Es una tecnología para la entrada/salida de datos en serie a alta velocidad y la conexión de dispositivos digitales como videocámaras o cámaras fotográficas digitales y computadoras portátiles o de sobremesa.

IrDA: Asociación de Datos Infra-rojos", define un estándar físico en la forma de transmisión y recepción de datos por rayos infrarrojos. IrDA se creó en 1993, entre: HP, IBM, Sharp y otros. Esta tecnología está basada en rayos luminosos que se mueven en el espectro infrarrojo.

Broadcast: Es el acto más frecuente de transmitir ondas y/o señales de audio y video en diversos formatos a un público que puede ser local, regional, nacional, internacional y con distintas características.

Routers: es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes. Este enrutamiento se realiza de acuerdo a un conjunto de reglas que forman la tabla de enrutamiento. Es un dispositivo que opera en la capa 3 del modelo OSI y no debe ser confundido con un conmutador (capa 2).

Switch: Es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos.

OSI: Siglas que significan Open Systems Interconnection o Interconexión de Sistemas Abiertos. Es un modelo o referente creado por la ISO para la interconexión en un contexto de sistemas abiertos. Se trata de un modelo de comunicaciones estándar entre los diferentes terminales y host.

Driver: Es un programa que facilita la comunicación entre un sistema operativo y un periférico.
En informática se le llama controlador de dispositivo, driver, o simplemente controlador al software que se encarga de permitir que un sistema interactúe con un periférico.

Workstation: Una Workstation (estación de trabajo) es una microcomputadora de alta gama diseñada para aplicaciones científicas y técnicas.

Supercomputadoras: fueron introducidas en la década de 1970 y fueron diseñadas principalmente por Seymour Cray en la compañía Control Data Corporation (CDC), la cual dominó el mercado durante esa época, hasta que Cray dejó CDC para formar su propia empresa, Cray Research.

UNIX: es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969, por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Dennis Ritchie, Ken Thompson y Douglas McIlroy.

NDS: En redes donde se ejecuta Novell NetWare 4.0, base de datos distribuida que mantiene información acerca de cada recurso de la red y que proporciona acceso a dichos recursos.

CGI: Es una norma para establecer comunicación entre un servidor web (web server) y un programa, de tal modo que este último pueda interactuar con Internet. También se usa la palabra CGI para referirse al programa mismo, aunque lo correcto debería ser script.

PHP: Es un lenguaje de scripts diseñado para el rápido desarrollo de sitios web dinámicos y que ha tomado muchas de las mejores cualidades de lenguajes como: la versatilidad del C, los objetos de Java y la facilidad y potencia del parser de Perl.

ASP: Modelo de negocio que surgió a finales de los 90 basado en ofrecer aplicaciones online, bien a través de un navegador web (browser), bien mediante el uso de clientes ligeros.

SQL: Es un lenguaje estándar que se usa en cualquier motor para manipular la información que se encuentra almacenada en una base de datos relacional.

Web Apache: Es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual.

MySQL: Es un sistema de gestión de base de datos relacional (RDBMS) de código abierto, basado en lenguaje de consulta estructurado (SQL).

Firewalls: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Backup: se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos. La forma verbal es hacer copias de seguridad en dos palabras, mientras que el nombre es copia de seguridad.

VoIP: es un acrónimo de Voz sobre Protocolo de Internet (Voice Over Internet Protocol), el cual por sí mismo significa voz a través de internet. Es una tecnología que proporciona la comunicación de voz y sesiones multimedia (tales como vídeo) sobre Protocolo de Internet (IP).

VPN: es una sigla que puede hacer mención a diferentes cuestiones de acuerdo al contexto. Uno de sus usos más frecuentes se encuentra en la tecnología, dondeVPN alude a la expresión del idioma inglés Virtual Private Network, que puede traducirse como Red Virtual Privada.

QoS: es la sigla de Quality of Service (Calidad de servicio) que podemos definir como el conjunto de tecnologías que garantiza la transmisión de cierta cantidad de información en un tiempo determinado a uno o varios dispositivos.

Streaming: Es la distribución digital de multimedia a través de una red de computadoras, de manera que el usuario consume el producto (generalmente archivo de vídeo o audio) en paralelo mientras.

Sockets: Es una dirección de Internet, combinando una dirección IP (la dirección numérica única de cuatro partes que identifica a una computadora particular en Internet) y un número de puerto (el número que identifica una aplicación de Internet particular, como FTP, WWW, etc).

REFERENCIAS

[1] (Beaver, s.f.)

[2] (INTECO, 2012)
[3] (GITS, 2013)
[4] (Mogull, s.f.)
[5] Trabajo Nº8 Tecnologías de la Información y Comunicación Yessenia Naranjo Polo
[6] Definición.de/internet
[7] universidad de castilla la mancha,
https://www.uclm.es/profesorado/ricardo/webnntt/bloque%202/internet.htm#62
[8] http //es.ccm.net/content/213-intranet-i-extranet.html
[9] Cisco Networking Academy http://ecovi.uagro.mx/ccna1/
[10] http://www.netronycs.com/cuantos_tipos_de_redes_hay.html
[11] https://hubslide.com/a/catiik-lozano
[12] www.tiposde.org
[13] http://platea.pntic.mec.es/jdelucas/sistemasoperativos.htm Javier de Lucas
[14] estadisitica
[15] IDC
[16] E-ducativa repositorio 1000 sistemas operativos de red
[17] http://profesores.fi-b.unam.mx/sun/Downloads/Solaris/DavidGalan/1.historia.pdf
[18] www.adinformaticasmr.wikispaces.com
[19] http://www.cert.org.mx/index.html
[20] Serot.com.mx/consejospymes04.html
[21] http://revista.seguridad.unam.mx/numero-16/normatividad-en-las-organizaciones-pol%C3%ADticas-de-seguridad-de-la-informaci%C3%B3n-parte-i
[22]
https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/SOLUTIONS/222000/TECH222445/en_US/Symantec_DLP_12.5_Admin_Guide.pdf?__gda__=1462037821_890e2410f5bec1ddc901c79570243909
[23]
https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/SOLUTIONS/221000/TECH221192/en_US/Symantec_DLP_12.5_System_Requirements_Guide.pdf?__gda__=1462046874_cf5babcc7cf4ad138d6b9aee4413d5d0
[24]
https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/SOLUTIONS/219000/TECH219406/en_US/Symantec_DLP_12.0_Oracle_11g_Installation_Upgrade_Guide.pdf?__gda__=1462059239_df874d12c1d3d8ff9a10731b9e9b7065

Índice de Figuras

Descripción Página