UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Plataforma de Seguridad para Centro de Datos

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Daniel Contreras Murillo

ASESOR DE INFORME

M. en C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., noviembre 2016

Plataforma de Seguridad para Centro de Datos

1 Índice General

Agradecimientos

A mis padres María Concepción Murillo Ramírez y Gerardo Contreras Domínguez, por su apoyo incondicional en todo lo que me propongo, por sus esfuerzos para llegar hasta donde hoy me encuentro y por darme confianza para superarme.

A mis hermanos Diego y Gerardo, quienes han estado siempre para apoyarme y por todos esos ratos que pasamos divertidos jugando con videojuegos lo que me ayuda a olvidarme del estrés de la vida cotidiana.

A mis abuelos Sergio Daniel Contreras Revilla y Eva Celia Domínguez Ríos, por acompañarme día con día para asistir a la universidad, escucharme cuando más lo necesito y apoyarme en todo lo que está dentro de sus posibilidades.

A Cinthia Estephania Yañez Cintora, por estar siempre conmigo y ayudarme cuando más lo necesito, por darme el valor para no dejarme rendir y ayudarme a ver las cosas desde otros puntos de vista.

A Eduardo, Dan, Víctor, Raymundo, Carlos, Oscar y Omar; por brindarme su amistad y compañía durante todo el tiempo que cursé la Universidad y hacer de ese tiempo algo muy divertido e inolvidable.

A la M.C. Ma. Jaquelina López Barrientos, por ser una gran profesora quien nunca desiste para transmitir su gran conocimiento y apoyo y hacer de nosotros sus alumnos mejores profesionistas, por brindar esos consejos no solamente profesionales sino también personales ojala existieran más maestros así, y sobre todo muchas gracias por brindarme su apoyo para salir por la puerta grande.

Y por último a la Universidad Nacional Autónoma de México y en especial a la Facultad de Ingeniería por la formación de calidad, diversidad cultural, formación de principios y de su gran riqueza de conocimientos.

Introducción

Introducción

En la actualidad existe una gran necesidad, no solamente en México sino a nivel mundial, de establecer políticas de Seguridad de la Información sin importar el sector industrial del que se hable, es decir, en la actualidad existe una gran demanda en cuanto a servicios de protección de la información para empresas sin importar el rubro al cual se dediquen.

Es aquí donde cobra importancia una correcta preparación como Ingeniero en Computación para afrontar, de manera adecuada, los retos que se presentan al asegurar los activos informáticos de una empresa, ya que debemos de conocer las técnicas empleadas.

Cabe mencionar que hoy en día los ciber-criminales buscan obtener accesos de manera ilícita hacia las empresas y extraer datos o información, incluso sin que los administradores de la red informática tengan conocimiento de ello hasta meses después de extraída la información.

Por lo cual, con base en mi experiencia puedo decir que la Universidad Nacional Autónoma de México en particular con la Facultad de Ingeniería en la carrera de Ingeniería en Computación se lleva a cabo una gran labor al preparar adecuadamente a los alumnos que hemos pasado por sus aulas, a través de un plan de estudios completo y adecuado a las necesidades laborales que vemos hoy en día, ya que, la Universidad no prepara a sus estudiantes para que los egresados tengan la capacidad de administrar y configurar alguna herramienta de comunicación y/o seguridad de la red en particular, sino que más bien nos da las bases de cómo se comportan este tipo de herramientas con lo que podemos llegar a deducir la forma en la cual se emplean las distintas marcas de fabricantes de seguridad.

Con lo anterior, como Ingeniero y en mi caso en particular como consultor de Seguridad Informática, al egresar de la Facultad de Ingeniería salí con los conocimientos necesarios para conocer y deducir la manera en la cual esta clase de dispositivos actúan al interior de una empresa, sin conocer necesariamente, alguna marca o herramienta en particular, y de esta manera puedo dar recomendaciones con mayor aportación hacia las empresas que contratan los servicios de la empresa donde laboro y donde los que como yo son consultores de Seguridad Informática sin necesidad de dar recomendaciones con una marca de fabricantes en particular.

Además, al enfrentarse al mundo laboral, los conocimientos de una rama en particular como lo es la seguridad informática de la computación, se quedan cortos, porque es necesario conocer de otras áreas como el diseño de sistemas, programación de aplicaciones, bases de datos, entre otras; para con esto tener una visión más amplia y ejecutar un plan de acción más adecuado a las necesidad del cliente, lo cual es abarcado por la Universidad Nacional Autónoma de México en la Facultad de Ingeniería de la carrera en Computación con su plan de estudios.

Capítulo 1
Panorama General Acerca de mí

1.1 Trayectoria Estudiantil

Desde muy temprana edad recuerdo sentirme atraído hacia la tecnología, ya que soy de la época de finales de los 80´s recuerdo ver como la vida cotidiana fue cambiando con grandes hallazgos y aportaciones del campo científico y tecnológico. Y esta atracción se vio aumentada cuando por primera vez tuve oportunidad de utilizar una computadora, la cual era de mi papá, claro está que no con fines de aprendizaje o de trabajo sino más bien para jugar un videojuego, pero este primer acercamiento a la computación me dejó marcado y día con día se vio impulsado ya que mi papá trabaja en este campo de la computación.

Así, una vez terminada mi preparatoria obtuve el pase directo a la Facultad de Ingeniería en la carrera de Ingeniero en Computación.

Durante los primeros meses en la carrera de Ingeniero en Computación, tal vez durante todo el primer semestre, me fue difícil ya que los primeros meses son muy exigentes y es tanto el conocimiento que muchas veces no es fácil asimilarlo todo y es necesario dedicarle unas horas extras de estudio, a lo cual yo no estaba acostumbrado, pero tuve la suerte de conocer a grandes personas las cuales siguen siendo grandes amigos y quienes muchas veces me ayudaron a comprender temas los cuales me resultaban confusos.

Así, transcurrieron meses, años y con ellos los semestres; aprendí a convivir con muchos tipos de personas, con gustos diferentes, colaborar y trabajar en equipo, en otras ocasiones ser líder y en otras seguir a un líder, es decir, aprendí a convivir con muchas más personas y ahora veo que esto es útil para lograr buenas relaciones laborales, ya que no todos contamos con el mismo perfil de personalidad.

1.2 Transición estudiantil a laboral (conclusión de créditos)

Entré a la carrera de Ingeniería en Computación en agosto de 2007 y terminé el total de créditos a finales de mayo de 2013 con un total de 408 créditos, entre materias obligatorias y optativas y promedio general de 8.50.

Una vez obtenido el total de créditos, trabajé en mi currículum Vitae y lo subí en varias plataformas de bolsa de trabajo en línea, obtuve respuesta de una dependencia de gobierno y de dos consultoras, después del proceso de entrevistas en la dependencia de gobierno y con ambas consultoras, una de ellas me ofreció contrato inmediatamente después de terminar la entrevista, por lo cual acepté en ese momento.

Así me incorporé al campo laboral a principios de febrero de 2014 como becario en la consultora de nombre BuróMC Seguridad Informática con perfil de consultor de seguridad, donde empecé a ver temas de Ingeniería de preventa y post-venta, después de un mes de laborar ahí y debido a

diversas circunstancias, entre ellas de tipo económico, me vi obligado a aceptar la propuesta económica que me ofreció la otra consultora que me entrevistó.

De esta manera comencé a laborar con la consultora OCM-IT Seguridad en Virtualización, a principios de marzo de 2014 donde inicié un proceso para desarrollar mis habilidades como consultor, al cual le dieron por nombre "Plan de desarrollo Consultivo". Este proceso me pareció muy interesante ya que antes de comenzar a asignarme a proyecto, estuve tomando cursos de fabricantes de productos de seguridad con los cuales pude obtener más conocimientos, a los ya alcanzados como estudiante en mi formación profesional, además de realizar exámenes de certificación con lo que he ampliado mi perfil como ingeniero y en particular como consultor de seguridad informática.

1.3 Plan de desarrollo consultivo

Durante los cursos que tomé con el fabricante de seguridad Trend Micro® de sus soluciones de seguridad, pude ver como esta empresa líder global en seguridad en la nube desarrolla sus productos con la visión de "crear un mundo seguro para que las empresas y particulares intercambien información digital".

En esta etapa obtuve una nueva visión de la seguridad, es decir, pude ver cómo las amenazas informáticas actúan en el mundo actual y cómo interactúan las soluciones de seguridad directamente con la estrategia de seguridad de cada organización, por lo que escoger soluciones con la tecnología más avanzada ofrece mayores ventajas, no solamente de administración sino también de detección temprana de amenazas informáticas las cuales han tenido un aumento exponencial en los últimos años al darse cuenta los ciber-criminales de lo rentable que es el mundo del desarrollo de malware.

Además de obtener la visión de cómo los ciber-criminales utilizan herramientas avanzadas de hacking y cracking así como otras técnicas para infiltrarse en infraestructuras de red con la finalidad de obtener un bien económico de manera ilegal, he aprendido a ver cómo las herramientas de seguridad han ido avanzado y cómo se han desarrollado nuevas tecnologías, las cuales permiten asegurar infraestructuras de red de mejor manera desarrollando estrategias de seguridad pensadas en capas y no solamente como productos separados.

Es decir, proteger la organización blindándola con las diferentes soluciones de seguridad que se tengan a la mano, y no solamente dejando que las herramientas como firewall, IPS, IDS, anti-malware, entre otro más, trabajen por separado sino en lugar de ello, llevar a cabo estrategias de seguridad que permitan correlacionar los eventos obtenidos en cada una de las herramientas mencionadas anteriormente.

Ya que actualmente las soluciones de seguridad tradicionales como anti-malware por sí mismas no son capaces de proteger la información y los recursos de todas las amenazas que se encuentran en el mundo actual, como el caso de los ataques dirigidos y las amenazas avanzadas persistentes, los cuales son más difíciles de detectar antes de que causen un daño dentro de la infraestructura de red que se desea proteger, llegando incluso a robo de información sensible, pérdidas económicas, situaciones legales y/o pérdida de reputación de la organización.

Es por ello que es muy importante observar las nuevas tendencias como la tecnología de nube, en la que los datos se encuentran vinculados a un servidor o incluso a grupos de servidores en los que un gran número de dispositivos acceden a ellos una gran cantidad de veces al día o el caso de BYOD (Bring Your Own Device) las cuales son tendencias actuales que no es posible asegurar con las estrategias tradicionales. Llegando al punto en el cual los planes de seguridad diseñados anteriormente no protegen de manera adecuada, por lo que, las más avanzadas soluciones de seguridad diseñadas por los líderes de productos de seguridad deben de modificar sus modelos de desarrollo de soluciones de seguridad y adaptarse a los cambios que presenta el mundo de hoy en día y las tendencias modernas de comunicación.

1.4 Conocimientos adquiridos durante la etapa escolar para desarrollo laboral

Gracias a la Universidad Autónoma de México a través de su Facultad de Ingeniería con su plan de estudios 1192 de la carrera de Ingeniero en Computación adquirí conocimientos de los cuales estoy muy orgulloso y que agradeceré todo el tiempo ya que me han permitido desarrollarme en mi vida laboral de manera exitosa. Al día de hoy puedo mencionar que la FI me proporcionó las bases para superarme y que ahora aplico día a día en cada uno de los servicios profesionales otorgados a diferentes clientes de distintos sectores.

La consultoría entregada por OCM-IT exige una amplia gama de conocimientos en distintas áreas de la computación principalmente en las áreas de redes de computadoras y seguridad en redes informáticas, así como conocimientos de bases de datos, programación y desarrollo de software; los cuales son temas que la FI exige para que todo ingeniero en computación que pase por sus aulas debe de cursar para lograr obtener conocimientos de dichas áreas mencionadas anteriormente y de esta manera lograr obtener el título de Ingeniero

A continuación se enlistan las asignaturas más importantes en mi desarrollo como ingeniero en computación y que me han sido de gran apoyo en mi labor como Consultor de Seguridad:

a) **Administración de proyectos de Software**
b) **Administración de redes**
c) **Arquitecturas cliente/servidor**
d) **Arquitectura de computadoras**

e) **Bases de Datos**
f) **Criptografía**
g) **Estructura y programación de computadoras**
h) **Ingeniería de software**
i) **Redes de datos**
j) **Seguridad informática I**
k) **Seguridad informática II**
l) **Sistemas operativos**

Capítulo 2
Principales proyectos laborales

OCM-IT® es una empresa fundada en el año 2005, dedicada a la implementación de soluciones tecnológicas a la medida de cualquier tipo de negocio que requiera disminuir y controlar problemas y riesgos durante la operación de su empresa, desarrollando de manera conjunta con diversos negocios y clientes estrategias de negocio, dando como resultado nuevas herramientas y recursos tecnológicos. Gracias a sus plataformas, recursos y socios tecnológicos garantiza la continuidad de cualquier negocio a través de la implementación de Hardware, Software y Servicios de Tecnología.

2.1.1 Misión

La misión de la organización es lograr la efectividad y rentabilidad en la inversión de cada uno de nuestros clientes a través de maximizar los recursos de cada proyecto con precios competitivos, servicio personalizado y valores agregados sin costo adicional.

2.1.2 Visión

Ser la empresa líder en brindar soluciones de tecnología que favorezcan el cuidado del ambiente, empleando equipos que utilicen menos recursos no renovables y empresas de software socialmente responsables que aporten dinero a causas para mejorar el medio ambiente.

2.1.3 Valores

Compromiso, Integridad, Respeto, Confianza e Innovación, permiten cumplir la promesa de brindar soluciones a la medida de cada cliente, satisfaciendo sus necesidades.

2.1.4 Servicios

- Health Check: le permite estar al tanto de la situación actual de algún aplicativo en particular en cuanto a arquitectura, distribución de roles, configuración y errores.
- Assesment de diferentes tecnologías: este reporte le permite conocer el resultado de un análisis detallado de la configuración y operación de la herramienta implementada, validando que la herramienta esté funcionando bajo mejores prácticas del fabricante.

- Capacity Planner & Sizing Microsoft: este análisis le permite conocer el ciclo de operación de la infraestructura de servidores durante un periodo de 30 días, recomendado para conocer el consumo de recursos relacionado al porcentaje de uso de CPU, memoria RAM, entradas a disco y red de cada uno de los servidores monitoreados. El objetivo es entregar un reporte que contenga la consolidación de servidores a utilizar en un ambiente virtual considerando alta disponibilidad, tolerancia a fallas, replicación y respaldo.
- Evaluación tecnológica (diferentes soluciones): esta es una prueba de concepto que permite realizar la instalación de cada una de las herramientas en la infraestructura de laboratorio, desarrollo y/o producción de clientes con el objetivo de mostrar las funcionalidades técnicas y beneficios al negocio.

2.1.5 Ofertas estratégicas

OCM-IT® ha generado un grupo de ofertas estratégicas las cuales consisten en:

- Virtualización:
    - Virtualización para centros de datos.
    - Virtualización de escritorios de usuario final.
    - Virtualización de aplicaciones.

- Seguridad.
    - Continuidad del negocio.
    - Disminución de riesgos de seguridad.
    - Cumplimiento de niveles de servicio.
    - Seguridad de la información para ambientes físicos, virtuales y en la nube.
    - Seguridad para ambientes Vmware sin agentes.

- Infraestructura tecnológica.
    - Servicios administrados.
    - Plataformas de correo electrónico (Office 365 y Microsoft Exchange).
    - Monitoreo de infraestructura con System Center, Trend Micro y software del fabricante Dell.
    - Aseguramiento de tecnología (pólizas de soporte, pago por evento).
    - Respaldos de base de datos con Ultrabac, Veeam y Software del fabricante Dell.

2.1.6 Cobertura

Estratégicamente OCM-IT® tiene su oficina central en la ciudad de México y desde ella da servicios hacia el interior del país con una cobertura en:

- Ciudad de México y Área Conurbada.
- Querétaro.
- Puebla.
- Monterrey.

2.1.7 Organigrama

OCM-IT® está constituida por diversos departamentos los cuales en conjunto se dedican a entregar soluciones de cómputo como seguridad de redes de datos, virtualización de aplicaciones y de equipo de cómputo final, así como servicios administrados e infraestructura tecnológica; cuenta con 20 trabajadores entre consultores, directores, recursos administrados en infraestructura de clientes, entre otros más.

En la Figura 2.1 se muestra el organigrama de la consultora OCM-IT®:

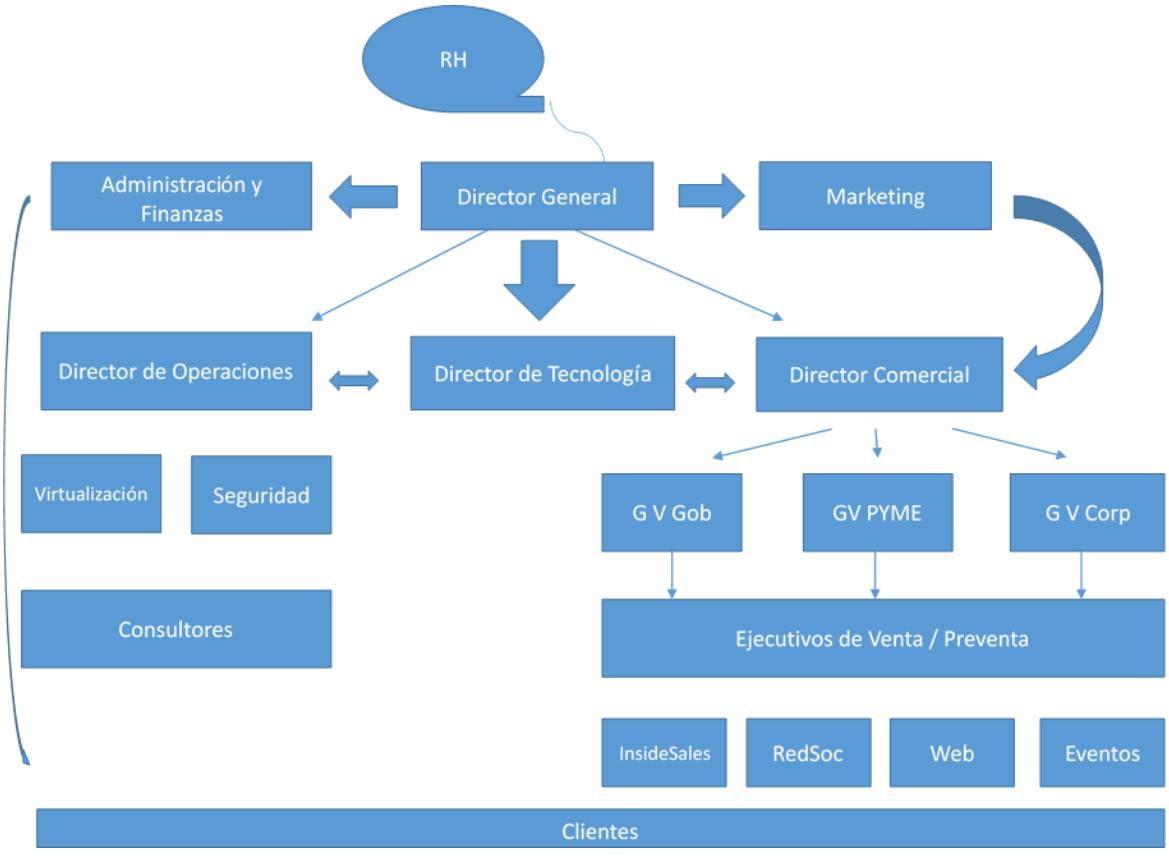


Figura 2.1 Organigrama OCM-IT®

Actualmente desempeño mis labores en el área de seguridad como Consultor de Seguridad debido a la estructura del organigrama de OCM-IT® este departamento está integrado por las siguientes personas:

- Director General - Tonatiuh Botello Alarcón
- Director Operaciones - Ing. Alejandro Piña Herrera
- Gerente del área de Seguridad - Ing. Oswaldo Rodríguez Morales
- Consultor de Seguridad - Ing. Rafael Mendoza
- Consultor de Seguridad - Ing. Omar Ochoa Herrera
- Consultor de Seguridad – Ing. Ricardo Salazar Garduño
- **Consultor de Seguridad - Daniel Contreras Murillo**

2.2 Proyecto 1: Implementación de herramienta de monitoreo de red en tiempo-real

Este primer proyecto se lleva a cabo en una empresa privada dedicada a la educación a nivel universitario fundada en el año de 1940, se encuentra catalogada como una Institución de Nivel VI en la Southern Association of Colleges and Schools (SACAS). Actualmente es reconocida como una de las principales instituciones de educación superior en México y goza de reconocimiento internacional entre los que destacan:

- Las Mejores Universidades.
- Las Mejores Escuelas de Negocios de América Latina.
- QS World University Rankings 2013.

Objetivos

- Tener visibilidad de los eventos que pueden impactar en la operación ya que en la red de la Empresa 1 no es posible administrar dispositivos propiedad de los alumnos y con Trend Micro™ Deep Discovery Inspector™ podrán saber el riesgo al que están expuestos en tiempo real.
- Identificar los dispositivos que se encuentran dentro de su red y sobre todo, conocer si tienen un comportamiento malicioso sin la necesidad de tener que instalar un agente en cada uno de los dispositivos conectados a la red de Empresa 1.
- Contar con la tranquilidad de tener la visión de lo sucedido en una red tan compleja y distribuida para tener la inteligencia necesaria y contar con la información correcta y oportuna para poder tomar mejores decisiones y en menor tiempo antes de que se genere un incidente que impacte en la continuidad de la operación de la Empresa 1.

Desarrollo

La implementación de la herramienta Trend Micro® Deep Discovery Inspector® en el centro de datos de la Empresa 1 se llevó a cabo en un día el 29 de septiembre de 2014, debido a que la herramienta no es intrusiva lo que permite realizar la implementación de manera rápida, los ajustes de configuración se realizaron el mismo día, ya que los parámetros son mínimos los cuales se listan en los siguientes puntos:

- Segmentos de confianza de la infraestructura de red.
- Servicios válidos dentro de la red de la empresa 1.
- Dominios con los cuales cuenta la empresa1.

Una vez implementada la herramienta Deep Discovery Inspector® se realizó el monitoreo de los eventos detectados como maliciosos en la infraestructura de red del cliente en tiempo real, así como también se extraían dichos eventos de manera mensual y se llevó a cabo una análisis de los mismos detectando amenazas.

Una vez detectados todos los eventos en periodos mensuales, partiendo de octubre como primer mes, se realizaron Planes de Mitigación, en los cuales se recomienda al cliente como puede protegerse de las distintas amenazas detectadas durante el tiempo monitoreado. Asimismo se llevó un seguimiento en la cantidad de eventos durante un periodo trimestral (octubre-noviembre-diciembre) en los cuales se pudo observar que implementando los procesos de mitigación, la red del cliente se vio beneficiada, no solamente detectando menor cantidad de amenazas, sino que además el ancho de banda del cliente se vio beneficiado, debido a la reducción de amenazas de red que consumían el ancho de banda.

Por último, se apoyó a la Empresa 1 con una campaña de limpieza de equipos de cómputo, en la cual se notificó a los alumnos en los que se detectó que tenían dispositivos infectados con algún tipo de malware y se realizaron los procedimientos de limpieza en cada uno de los dispositivos de los alumnos que asistieron a dicha campaña, esto con la finalidad de limpiar los equipos que no pertenecen a la Empresa 1.

Principales logros

La Empresa 1 al implementar la solución de monitoreo en tiempo real que ofrece visibilidad y detección contra amenazas avanzadas y ataques dirigidos obtuvo los siguientes logros:

- Visibilidad y detección en tiempo real contra todo tipo de amenazas de red.
- Disminución de los equipos comprometidos con alguna familia de malware.
- Mejora en el rendimiento de ancho de banda.

- Disminución de eventos en los cuales los usuarios descargaban contenido malicioso.
- Incremento en la detección de amenazas en tiempo real que impactan a la red.

El logro general y que permitió ser exitoso fue la administración y coordinación correcta del proyecto sobre todo el control y contacto con todo el personal involucrado.

2.2.1 Proyecto 2: Visibilidad y detección de malware

Se trata de una empresa líder en el sector financiero con más de 100 años de servicio y formada en Monterrey, cotiza en la Bolsa de Valores de México (BVM), además de cotizar en las bolsas de España y Estados Unidos. Actualmente ofrece una gran variedad de productos, así como de servicios a través de su casa de bolsa, las compañías de pensiones y seguros, Afore, sociedades de inversión, empresas de arrendamiento y factoraje, y almacenadora.

Debido al gran flujo de efectivo que maneja la Empresa 2 es de vital importancia implementar y administrar herramientas de seguridad que nos permitan asegurar de la mejor manera toda la infraestructura de red con la que ellos cuentan.

Objetivos

- Integración de una solución de detección de brechas de seguridad en tiempo real que evaden la seguridad tradicional a través de la integración de la herramienta Trend Micro® Deep Discovery Inspector® en 6 localidades distintas en el interior de la República Mexicana.
- Creación de un reporte ejecutivo, en el cual contendrá la información necesaria para la generación de planes de mitigación, de acuerdo a la naturaleza de los hallazgos detectados
- Tener mayor protección en el área perimetral contra ataques de negación de servicio y alertando ante la detección de cualquier actividad sospechosa y vulnerabilidades.
- Instalación de 6 servidores Trend Micro® Deep Discovery Inspector® en 6 localidades de Empresa 2.

Desarrollo

La implementación de la herramienta Trend Micro® Deep Discovery Inspector® en las 6 distintas localidades se llevaron a cabo a lo largo de un periodo de 5 meses (de noviembre de 2014 a Marzo del 2015) de los cuales, dos meses se emplearon en las actividades referentes a la instalación de tres plataformas de Deep Discovery Inspector® en la ciudad de México y tres en Monterrey, debido a la localización de las diversas instalaciones del cliente a mí solamente me tocó implementar la plataforma de monitoreo en tiempo real en las localidades de la ciudad de México.

Debido a la naturaleza no intrusiva de la herramienta la configuración de los parámetros se realizó después de colocar la herramienta de monitoreo Trend Micro® Deep Discovery Inspector® en sitio esto es, en las 6 localidades que abarcó esta implementación, a través de la consola de administración web de cada una de las plataformas, realizando la conexión por medio de la infraestructura de red del cliente.

Una vez configurados los parámetros de monitoreo de Deep Discovery Inspector® en las 6 localidades, se trabajó en conjunto con personal del cliente para crear un sandbox personalizado con las características de una de las principales imágenes de equipo de cómputo final del cliente, sistema operativo y aplicativos, el cual le permitió al cliente analizar muestras de archivos sospechosos en un ambiente lo más cercano posible a los equipos de punto final que se tienen en su infraestructura.

El último punto de configuración de las 6 plataformas de monitoreo fue sincronizarlas con la herramienta de Trend Micro® Control Manager® la cual en palabras del fabricante, “es la consola de consolas”, es decir, se sincronizaron las 6 plataformas Deep Discovery Inspector® con Control manager® para que los administradores del área de red tuvieran visibilidad de las 6 consolas sin necesidad de tener que entrar a cada una de ellas, facilitando de esta manera la detección y análisis de eventos de red que impactan en la infraestructura del cliente.

Por último, impartí un curso denominado por OCM-IT como “Transferencia de conocimientos” el cual tuvo una duración de 21 horas y que se llevó a cabo con la asistencia de 6 personas que son las que quedaron a cargo del monitoreo de la herramienta Deep Discovery Inspector®, en dicho curso les transferí los conceptos generales que les permiten manipular configuraciones básicas de la herramienta así como también observar y llevar a cabo el análisis de los eventos de red que se encuentran impactando en la red del cliente, generar reportes, así como gráficas de los eventos encontrados y análisis de malware en equipos comprometidos.

Principales logros

La Empresa 2 al implementar la solución de monitoreo en tiempo real Trend Micro® Deep Discovery Inspector® obtuvo los siguientes logros:

- Visibilidad y detección en tiempo real contra todo tipo de amenazas de red.

- Disminución de los equipos comprometidos con alguna familia de malware.
- Mejora en el rendimiento de ancho de banda.
- Disminución de eventos en los cuales los usuarios descargaban contenido malicioso.
- Incremento en la detección de amenazas en tiempo real que impactan a la red.
- Mejora en el tiempo de respuesta contra incidentes que impactan en la operación.

2.2.2 Proyecto 3: Implementación de anti-virus Trend Micro OfficeScan®

Es un proyecto de implementación en una dependencia del Poder Ejecutivo Federal, tiene a su cargo el desempeño de las atribuciones y facultades que le encomiendan la Ley Orgánica de la Administración Pública Federal, la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y demás ordenamientos legales aplicables en la materia:

- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- Ley de Obras Públicas y Servicios Relacionados con las Mismas.
- Ley General de Bienes Nacionales.
- Ley del Servicio Profesional de Carrera en la Administración Pública Federal.
- Ley Federal de Presupuesto y Responsabilidad Hacendaria.
- Otras leyes, reglamentos, decretos, acuerdos y órdenes del Presidente de la República.

Por lo anterior, es importante contar con una solución anti-malware que permita a los administradores de seguridad proteger escritorios virtuales y físicos en contra de la evolución del panorama de las amenazas que se observa hoy en día, esta herramienta de seguridad para Endpoint proporciona varios niveles de protección contra amenazas y seguridad de datos para proteger a los usuarios y su información corporativa contenida en sus equipos de cómputo.

Objetivos

Protección de 1 500 equipos de usuarios finales con los módulos de protección con la cual cuenta la plataforma de Seguridad para equipos de cómputo final los cuales se listan a continuación:

- Reputación Web (Anti-malware).
- Reputación de archivos (Anti-malware).
- Detección de amenazas (Anti-malware).
- Detección y escaneo de vulnerabilidades (Vulnerability Protection).
- Prevención de pérdida de datos (DLP).

- Monitoreo de modificaciones inusuales (Behavior Monitoring).
- Controlar el acceso a los dispositivos de almacenamiento externos y recursos de red (Device Control).

Desarrollo

La implementación de la herramienta de protección anti-malware Trend Micro® OfficeScan® en el sitio del cliente para 1 500 equipos se llevó en un tiempo de alrededor de 4 meses (de mediados de Junio de 2015 a mediados de Octubre de 2015), desde la implementación de una plataforma virtual provisional de anti-malware hasta el despliegue de todos los agentes en los equipos de cómputo final y su registro en la plataforma definitiva.

Las actividades que realicé son las siguientes:

- Instalación y configuración inicial de una consola de anti-malware Trend Micro® OfficeScan® en un ambiente virtual, ya que la licencia del anti-malware anterior se terminó y el servidor físico para la instalación de la plataforma de OfficeScan no se tenía, debido a tiempos de entrega del fabricante, se optó por realizar una instalación provisional de la plataforma en un servidor virtual mientras se hacía la entrega del servidor físico y para no dejar desprotegidos los equipos de cómputo.
- Una vez que se recibió el servidor físico la gente de infraestructura del cliente instaló un sistema operativo Windows Server 2012 R2 y lo actualizaron con todos los parches necesarios de sistema operativo.
- Instalé los requerimientos web necesarios para la implementación de la consola de administración de Trend Micro® OfficeScan® y continúe con la instalación de la plataforma de seguridad.
- Debido a que los agentes se reportaban con la consola del primer servidor (servidor Virtual) fue necesario realizar un procedimiento de migración a la consola web de administración de OfficeScan® en el servidor físico, durante esta actividad se tuvieron un par de inconvenientes por lo que tuve que levantar casos de soporte con el fabricante de seguridad Trend Micro® y llevar un seguimiento para darle solución a los mismos.
- Una vez que todos los agentes se reportaron a la nueva consola de anti-malware en el servidor físico fue necesario tener sesiones con la gente de infraestructura del cliente para poder afinar las configuraciones de la herramienta de acuerdo con las características de su red y el nivel de protección deseado.

Principales logros

La Empresa 3 al implementar la solución de Seguridad para equipos de cómputo final físicos y virtuales Trend Micro® OfficeScan® obtuvo los siguientes logros:

- Protección de datos en equipos de cómputo físicos y virtuales desde una plataforma de administración central.
- Reducción en la carga de actualizaciones del cliente.
- Reducción de footprint en los equipos de cómputo físicos y virtuales.
- Disminución en el impacto del rendimiento de los equipos de usuario final.
- Evitar que los programas o usuarios desactiven la protección anti-malware.
- Asegurar equipos de usuario con la más amplia gama de protección contra malware como virus, troyanos, gusanos, spyware, ransomware, amenazas persistentes avanzadas y nuevas variantes emergentes.
- Protección de usuarios y equipos de punto final de acceso hacia contenido web malintencionado sin depender de las actualizaciones para asegurar la protección de día cero.
- Identifica y bloquea botnet y ataques dirigidos de comunicaciones de servidores de comando y control (C&C).
- Protección del buzón de correo electrónico de usuarios finales mediante el escaneo de carpetas de correo electrónico POP3 y Outlook en busca de amenazas.
- Reducción en la asistencia y los costes de TI al simplificar el aprovisionamiento y gestión de dispositivos.
- Permitir al área de TI para restringir el uso de unidades USB, grabadores de CD/DVD y otros medios extraíbles.
- Centralizar la gestión a través de Trend Micro® Control Manager®, para mayor visibilidad y un mayor control.

Capítulo 3
Caso de Estudio

3.1 Cliente

Es una Institución con más de 70 años de experiencia, se especializa en el desarrollo y la formación universitaria de hombres y mujeres de los cuales una gran cantidad de ellos se han llegado a convertir en grandes líderes de nuestra nación, por lo que se ha ganado el título de ser una de las mejores instituciones de educación superior privada en México y en el extranjero, a la cual se le denominará en el presente documento como *"la universidad".*

Así, *la universidad* ofrece más de 30 programas de licenciaturas y posgrados, diez doctorados, más de 20 maestrías y cuentan con programas de especialidades académicas, así como también ofrece una gran cantidad de cursos y diplomados a través de diversos portales.

3.2 Antecedentes

En la actualidad *la universidad* se encuentra en un proceso de valoración/conocimiento de una herramienta que le permita tener un mayor control y administración de seguridad interna sobre los servidores críticos y para ello está contemplando la adopción de una tecnología que le permita mejorar la seguridad dentro del Centro de Datos, así como, el control de accesos a servidores productivos.

La universidad está consciente que los módulos que integra la Tecnología de Trend Micro® Deep Security® 9.5, le permitirán aplicar diferentes niveles de protección hacia sus servidores y las aplicaciones que se encuentren dentro de los mismos, así como tener el control total sobre dichos servidores ya sea en entornos físicos y/o virtuales.

La herramienta de Deep Security® 9.5 le permitirá a *la universidad* que los Sistemas a integrar dispongan de auto blindaje por medio de Parcheo Virtual para evitar vulnerabilidades de Sistema Operativo y de Aplicativos, dándole a *la universidad* el tiempo suficiente para cubrir dichos equipos con las actualizaciones pertinentes.

3.3 Problemática

A raíz de la presentación de la Estrategia de Seguridad para Centros de Datos que ofrece la consultoría de OCM-IT®, en conjunto con Trend Micro®, *la universidad* desea implementar una solución tecnológica de seguridad para centros de datos para 15 servidores virtuales que le permita aplicar los siguientes puntos:

a) Integración y habilitación de módulo de Antimalware.

b) Revisión y/o monitoreo de puertos abiertos y cerrados.
c) Monitorear las actividades de conexión remotas hacia los servidores.
d) Escanear y Mostrar las vulnerabilidades que puedan existir para cada ambiente.
e) Saber los cambios realizados sobre archivos específicos en los servidores a contemplar.
f) Asegurar 15 servidores con Sistemas Operativos Windows y Linux.

Análisis y requerimientos

- Para la implementación de la solución de seguridad para Centros de Datos se acotó a solamente 15 servidores de un total de 38, del ambiente de *la universidad*, debido a negociaciones con el cliente, esto con la finalidad de instalar y configurar la solución para los ambientes con Sistemas Operativos Windows y Linux que nos indique *la Universidad*.

- Los Servidores estarán protegidos con el Agente anti-malware de Deep Security® y se busca protegerlos en diferentes vertientes, ya que actualmente se encuentran desprotegidos y las aplicaciones que se encuentran montadas en ellos son de carácter crítico, por lo cual se buscó mantenerlos asegurados y que sus servicios se encuentren disponibles, las vertientes de protección se muestran a continuación:

    1. Escaneo y revisión de reglas recomendadas que muestran las vulnerabilidades de sistema y aplicaciones a las cuales están expuestos los sistemas.
    2. Revisión y monitoreo de puertos abiertos en cada sistema.
    3. Escaneo de Monitoreo de integridad sobre los sistemas definidos.
    4. Protección de sistemas con Antimalware, evitar las tormentas de antivirus que suelen experimentarse en las exploraciones completas del sistema y las actualizaciones de patrones.
    5. Protección contra URL´s maliciosas y amenazas web.

Objetivos

El objetivo planteado por *la universidad* considera que se debe cumplir con lo siguiente:

> El proyecto de Protección Antimalware e Integridad de Archivos busca dar mayor protección a los servidores que están de alguna forma expuestos a peticiones provenientes de Internet. Evitar mediante un anti Malware la infección de software dañino o la contención del mismo. Asegurar la integridad de los archivos mediante la

creación de un “base line” que nos permita controlar las modificaciones que pudieran surgir en los servidores. Así como también, blindar los servidores y aplicaciones en los mismos mediante el uso de parcheo virtual (RFP - Proyecto de Protección Antimalware e Integridad de Archivos, noviembre, 2013).

Metodología

En la actualidad la mayoría de los proyectos de desarrollo e implementación de software, están basados en el proceso para el desarrollo de software, conocido por algunos autores como ciclo de vida del desarrollo de software. El cual está basado en cuatro etapas principales las cuales se muestran a continuación:

1) Planificación: proporciona un marco de trabajo que permite al administrador del proyecto hacer estimaciones razonables de recursos costos y planificación temporal. Estas estimaciones se hacen dentro de un marco de tiempo limitado al comienzo de la definición de un proyecto de software, y normalmente se actualización a medida que progresa el proyecto.
2) Análisis del Sistema: en este proceso el Analista se reúne con el cliente (un representante institucional, departamental o cliente particular), e identifican las metas globales, se analizan las perspectivas del cliente, sus necesidades y requerimientos, sobre la planeación temporal y presupuestal, líneas de mercadeo y otros puntos que puedan ayudar a la identificación y desarrollo del proyecto.
3) Diseño del Sistema: es un conjunto de pasos repetitivos que permiten al diseñador describir todos los aspectos del Sistema a construir. A lo largo del diseño se evalúa la calidad del desarrollo del proyecto con un conjunto de revisiones técnicas. El diseño debe implementar todos los requisitos explícitos contenidos en el modelo de análisis y debe acumular todos los requisitos implícitos que desea el cliente
4) Implementación: es la última fase del desarrollo de Sistemas, es el proceso de instalar equipos o Software nuevo, como resultado de un análisis y diseño previo como resultado de la sustitución o mejoramiento de la forma de llevar a cabo un proceso automatizado. Al Implantar un Sistema de Información lo primero que debemos hacer es asegurarnos que el Sistema sea operacional o sea que funcione de acuerdo a los requerimientos del análisis y permitir que los usuarios puedan operarlo
5) Pruebas: consiste en la ejecución de actividades en donde se debe verificar que la funcionalidad total de un sistema fue implementada de acuerdo a los documentos

de especificación definidos en el proyecto. Consisten en la comprobación de que elementos del software que interactúan entre sí, funcionan de manera correcta.

De los diferentes modelos que existen para llevar a cabo el proceso de desarrollo de software, OCM-IT Seguridad en Virtualización como parte de sus políticas de trabajo utiliza el modelo Microsoft Solution Frameworks.

Modelo Microsoft Solution Frameworks (MSF)

Microsoft Solution Frameworks también conocido como MSF es un enfoque personalizable utilizado por la consultoría OCM-IT ® para entregar con éxito soluciones tecnológicas de manera más rápida, con menos recursos humanos y menor riesgo, pero con resultados de calidad.

MSF ayuda a los equipos a enfrentarse directamente a las causas más habituales de fracaso de los proyectos tecnológicos y mejorar así las tasas de éxito, la calidad de las soluciones y el impacto comercial.

MSF se centra en los siguientes puntos:

- Alinear los objetivos de negocio y de tecnología.
- Establecer de manera clara los objetivos, los roles y las responsabilidades a lo largo del proyecto.
- Implementar un proceso iterativo controlado por hitos o puntos de control.
- Gestionar los riesgos de manera proactiva.
- Responder con eficacia ante los cambios.

Implementación de la plataforma de seguridad para Centros de Datos

A continuación se describen las etapas del Proceso para desarrollo de Software utilizando como metodología Microsoft Solution Frameworks, el cual, como se mencionó anteriormente es utilizado por la consultoría OCM-IT® durante la implementación de los servicios contratados por clientes y fue utilizado para la implementación de la solución de seguridad para Centros de Datos Trend Micro® Deep Security® en su versión 9.5 para *la universidad* utilizando los documentos entregables que se generaron para cada una de las etapas que componen este proceso.

Notas: debido a que la información de *la universidad* es confidencial muchos datos utilizados a lo largo de la implementación serán omitido y/o reemplazados por caracteres “X”. Los documentos que se muestran a continuación fueron desarrollados por mí y revisados por mis superiores en

ellos se muestran las actividades que realice durante la implementación del proyecto desde la planeación hasta la liberación del mismo

Etapa 1: Planeación

Para cumplir con la implementación de la herramienta de seguridad Trend Micro® Deep Security®, se planeó realizar las siguientes actividades primarias:

- Preparar la infraestructura necesaria para la implementación de la solución Trend Micro® Deep Security 9.5®, contemplando las mejores prácticas recomendadas por el fabricante.
- Optimizar la administración de la seguridad para centros de datos a través de la consola de administración central Deep Security Manager®.
- Aumentar el nivel de seguridad de la infraestructura del centro de datos actual de *la Universidad* brindando una capa más de protección.

Durante la etapa de planeación OCM-IT con base en el Proceso para desarrollo de Software y siguiendo la metodología MSF se hizo entrega de la siguiente documentación la cual fue realizada por mí y revisada por mi superior del área de seguridad:

- Plan de trabajo

A continuación se muestra el plan de trabajo seguido para la implementación de la solución Trend Micro ® Deep Security® 9.5 en las instalaciones de *la Universidad:*

a) Objetivos del documento

Este documento tiene los siguientes objetivos primarios planificación de:

- Implementación de la solución de seguridad Trend Micro® Deep Security® 9.5 en la localidad de XXXX[1] con dirección en XXXX[2].
- Instalación de 15 agentes de seguridad Deep Security® Agent´s en servidores pertenecientes a la infraestructura de *la Universidad*.
- Descubrimiento y configuración de los 15 agentes de seguridad en la consola de administración central Deep Security Manager®.

b) Objetivos en la implementación

[1] Datos omitidos por confidencialidad con el cliente.
[2] Datos omitidos por confidencialidad con el cliente.

Esta estrategia incluye las consideraciones que deben hacerse para minimizar el impacto del proceso de implementación tanto para los administradores, como para los procesos operativos actuales de la infraestructura de red.

Una vez implementada la plataforma de seguridad Deep Security® 9.5 en el servidor virtual designado para la solución, así como la instalación de la base de datos SQL Server necesaria por la plataforma de seguridad y de los agentes de seguridad en la misma organización, se utilizará la consola de administración central para realizar la configuración y administración de los mismos.

Los servidores asegurados con el agente de Deep Security® deberán de ser capaces de comunicarse ya sea con el FQDN o la dirección IP (según sea el caso) del servidor virtual dónde se implementará la plataforma de seguridad.

c) Localidad

Para realizar la implementación la solución de seguridad Trend Micro® Deep Security® 9.5 se realizó físicamente desde las instalaciones de *la Universidad* ubicadas en XXXX[3] con dirección en XXXX[4].

d) Componentes de Hardware

De acuerdo a la propuesta presentada por OCM - IT a *la Universidad,* se requirió de 1 servidor virtual con las siguientes características necesarias para soportar la funcionalidad de la plataforma de seguridad Trend Micro® Deep Security® de manera adecuada:

- Procesador Quad Core 3GHz x64.
- 8-12 GB de RAM.
- 1 NIC de 1 Gb.
- Almacenamiento, 120 GB en raid 1.
- Microsoft Windows Server 2012 R2 Standard.

e) Componentes de Software

Deep Security® trabaja a partir de componentes de software, estos son utilizados para definir una correcta arquitectura de la propia plataforma, así como también hace uso de los recursos de la infraestructura de red, a continuación en la tabla 3.1 se describen los componentes que integran una arquitectura de Deep Security® 9.5:

[3] Datos omitidos por confidencialidad con el cliente.
[4] Datos omitidos por confidencialidad con el cliente.

Tabla 3.1 Componentes de una arquitectura Deep Security

Componentes	Función
Deep Security Manager	Es la consola de administración central la cual utilizan los administradores de la solución para configurar políticas de seguridad y desplegar protección a los siguientes componentes: • Deep Security Virtual Appliance • Deep Security Agents
Deep Security Virtual Appliance	Es una máquina virtual segura diseñada para ambientes VMware vSphere la cual proporciona: • Protección Anti-malware. • Prevención de intrusos. • Monitoreo de integridad. • Protección de aplicaciones web. • Protección de control de aplicaciones. • Firewall.
Deep Security Agents	Es un agente de seguridad desplegado directamente en el equipo a proteger el cual nos provee: • Prevención de intrusos. • Firewall. • Protección de aplicaciones web. • Control de aplicaciones. • Monitoreo de integridad. • Inspección de registros.
Deep Security Relay	Este módulo distribuye actualizaciones hacia otros agentes y Virtual Appliances. En esta versión de Deep Security (9.5) agentes Windows y Linux cuentan con una función de Relay.
Deep Security Notifier	Es una aplicación Windows System Tray el cual comunica el estado de los agentes de Deep Security, así como del Relay.

f) Requerimientos de Software:

Los requerimientos de software que a continuación se listan son necesarios para llevar a cabo la implementación de la plataforma de seguridad para centros de datos Trend Micro® Deep Security®:

- Instalación previa de un servidor de base de datos SQL Server.
- Licenciamiento Deep Security® 9.5 para 15 servidores.
- Medias de instalación.

g) Rol del componente Deep Security Manager

Este servidor se encarga de lo siguiente:

- Centralizar la administración de la plataforma de seguridad.
- Crear y administrar políticas de seguridad.
- Detectar amenazas y tomar acciones preventivas en respuesta a ellas.
- Implementar protección con los diferentes módulos que conforman la plataforma de seguridad a los componentes de la herramienta:
    - Deep Security Virtual appliance.
    - Deep Security Agent.

h) Arquitectura

La consola de administración se montó sobre un ambiente virtual VMware sobre el cual se instaló un sistema operativo Windows Server 2012 R2. A continuación se muestra un diagrama con la arquitectura de la solución con agentes (véase la figura 3.1):

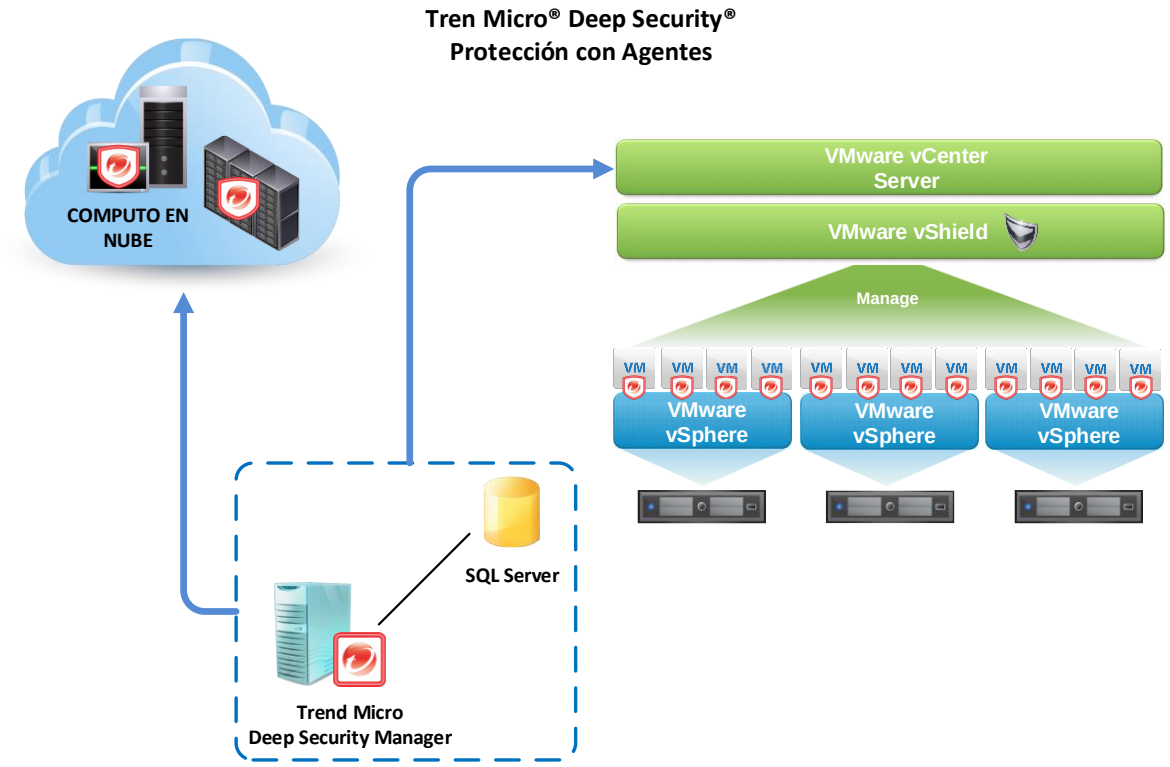


Figura 3.1. Arquitectura Deep Security® protección con agente

i) Agenda de Implementación

La agenda de implementación contempla las configuraciones necesarias en la consola de administración central para la creación de las políticas y configuración de los perfiles de seguridad de las mismas para el despliegue a los servidores a proteger con Deep Security®.

A continuación en la tabla 3.2 se enlista la agenda de implementación del proyecto Implementación de plataforma de seguridad para Centro de Datos:

Tabla 3.2 Agenda de implementación

Nombre de tarea	Duración
Implementación de Plataforma de Seguridad para Centros de Datos (Deep Security)	**82.35 días**
Etapa I. Análisis	**4.85 días**
Análisis de requerimientos de infraestructura actual	0.6 días
Creación de documento de Situación Actual	4 días
Entrega de documento de Situación Actual	0.25 días
Etapa II. Diseño de arquitectura	**4.5 días**
Validación de cumplimiento de requerimientos.	1 día
Creación de Diseño Lógico y Físico	3 días
Entrega de Diseño Lógico y Físico	0.5 días

Etapa III. Implementación	**55 días**
Instalación de Deep Security Manager (DSM)	**1 día**
Instalación de consola Deep Security Manager (DSM)	0.5 días
Configuración de consola Deep Security Manager (DSM)	0.5 días
Creación de perfil de seguridad	**54 días**
Instalación de Agente Deep Security para 15 servidores	2 días
Definición de perfiles de acuerdo a tipo de Sistema Operativo y aplicaciones	3 días
Aplicación de perfil	0.5 días
Módulo de Antimalware y Web Reputation	**9.5 días**
Habilitar modulo	0.5 días
Definición de listas de exclusiones por tipos de escaneos	3 días
Configuración de tipos de escaneo (En tiempo real, Manual y Calendarizados)	2 días
Configuración de acciones por tipo de malware	1 día
Validar escaneos en tiempo real	1 día
Prueba de consumo de recursos	1 día
Análisis de métricas de consumo	1 día
Módulo Intrusion Prevent	**12.5 días**
Escaneo de recomendaciones (virtual patch)	2 días
Revisión de reglas recomendadas	2 días
Validar con personal de *la Universidad* reglas a aplicar	4 días
Aplicación de recomendaciones (virtual patch)	1 día
Validación de reglas aplicadas	1.5 días
Análisis de comportamiento de servidores protegidos	1 día
Configuración de alertas	1 día
Módulo de File Integrity Monitoring	**6.5 días**
Habilitar Modulo de FIM	0.5 días
Ejecutar escaneo de recomendaciones	1.5 días
Creación de Baseline (si no existe)	0.5 días
Aplicar reglas recomendadas	1 día
Creación de reglas personalizadas	3 días
Módulo de Log Inspection	**7 días**
Habilitar Modulo de LI	0.5 días
Ejecutar escaneo de recomendaciones	1 día
Aplicar reglas recomendadas	1 día
Creación de etiquetas por eventos específicos para cada ambiente	3.5 días
Configuración de alertas	1 día
Módulo Firewall	**13 días**
Ejecutar escaneo de puertos	2 días
Generación de lista de puertos	1 día
Generación de reglas de firewall	8.5 días
Habilitar Modulo de Firewall	0.5 días
Configuración de alertas	1 día
Etapa IV. Validación	**17 días**
Monitoreo de desempeño de consola de administración DS	2 días
Creación de memoria de configuración.	15 días
Etapa V. Entrega	**1 día**

Entrega de documentación final	0.5 días
Cierre de proyecto	0.5 días

j) Recursos de implementación

En la tabla 3.3 se indican los recursos que fueron asignados para la implementación de Deep Security® que se dividen las siguientes áreas:

Tabla 3.3 Recursos asignados para la implementación

Recursos	Actividades
Ing. del Área de Seguridad De *la Universidad*	Personal a cargo de proyecto asignado por Institución "X", se encargará de proveer la coordinación con las áreas involucradas según su estructura departamental para realizar las diligencias necesarias para la realización de las tareas y aprovisionar los requerimientos y recursos físicos para la implementación, además de supervisar el proceso en todas sus etapas.
Daniel Contreras Murillo OCM-IT	Desarrolla la implementación y coordina la puesta en operación del proyecto junto con el personal de Institución "X".

k) Asistencia Técnica

El soporte Técnico de segundo nivel es proporcionado por OCM-IT® a través de una Póliza de Soporte sobre la Plataforma de Deep Security® 9.5 durante un periodo de 12 meses después de liberar la herramienta a producción. Adicionalmente, soporte de tercer nivel será proporcionado por Trend Micro® en conjunto con OCM-IT®.

El soporte técnico del hardware o software de los servidores físicos y/o virtuales donde se implementara la herramienta de Deep Security® es responsabilidad de *la Universidad*.

No hay soporte a infraestructura de telecomunicaciones, los cambios y/o configuraciones serán realizados por parte de personal designado por *la Universidad*.

l) Preparación

OCM-IT® en conjunto con *la Universidad* definió las configuraciones más adecuadas para cada uno de los módulos que integran la plataforma de seguridad para centros de datos y con ello se crearon los Perfiles de Seguridad de acuerdo a los distintos roles o aplicativos que pueda contener cada uno de los servidores como entrega de servicios de tipo DNS, FTP, SMTP, Active Directory, de bases de datos, de entrega de servicios web, de autenticación, entre otros; en la infraestructura de red de *la Universidad* que se consideran a proteger a lo largo de la duración de este proyecto.

m) Validación

Se asumió que para el inicio de la implementación, los servidores a proteger por la plataforma Deep Security® estarían disponibles para instalarles el agente de seguridad e iniciar el proceso de configuración de los distintos módulos que componen la plataforma de seguridad para centros de datos.

n) Consideraciones de la implementación

Para realizar la implementación de la plataforma de seguridad Deep Security® 9.5 es necesario que el proceso de instalación de la base de datos ya esté finalizado con éxito, para este caso se definió una base de tipo SQL.

La instalación del software para la solución está determinada por las siguientes actividades:

- Instalación previa de la base de datos a utilizar por la plataforma de seguridad Deep Security.
- Implementación y configuración de Deep Security Manager.
- Instalación de agentes sobre servidores a proteger.
- Creación y aplicación de perfiles de seguridad para servidores a proteger.
- Monitoreo de ambientes protegidos.

o) Encuesta de Satisfacción

La satisfacción de *la Universidad* se vio reflejada cuando se cumplan los criterios enlistados a continuación:

- Ambiente Deep Security® estable y operando adecuadamente, de acuerdo a los alcances establecidos.
- 15 Servidores protegidos y funcionando correctamente.
- Plan de Implementación conforme a los lineamientos detallados en el Plan de Trabajo.
- Revisión de Arquitectura Deep Security® aprobada y aceptada por personal de Infraestructura de *la Universidad*.

p) Responsabilidades

Se consideró que la responsabilidad sea compartida entre *la Universidad* y OCM-IT® para la administración, operación y mejora continua de las reglas definidas para los 15 servidores que se contemplaron.

En el desarrollo de la implementación de la plataforma de Deep Security® se consideró la entrega de los siguientes documentos:

Etapa I Análisis

- Documento de Requerimientos Técnicos
- Documento de Situación Actual.

Etapa II Diseño

- Documento de Diseño Físico.
- Documento de Diseño Lógico.

Etapa III Implementación

- Creación de memoria de Instalación.

Etapa IV Validación

- Ejecución de documento de Plan de Pruebas y Validación del mismo.

Etapa V Entrega

- Entrega de Memoria de Instalación Deep Security®.
- Entrega de concentrado de demás documentos.

Nota: Los documentos son proporcionados conforme el avance de las etapas del proyecto.

A continuación se muestra el diagrama de Gantt en dónde se muestra el inicio y fin de cada una de las etapas que componen el proyecto se seguridad para Centros de Datos de *la Universidad,* (véase la figura 3.2):

Nota: las fechas mostradas a continuación no corresponden en su totalidad con las fechas de implementación debido a que *la Universidad* decidió adelantar algunas de las fechas para asegurar sus servidores lo más pronto posible.

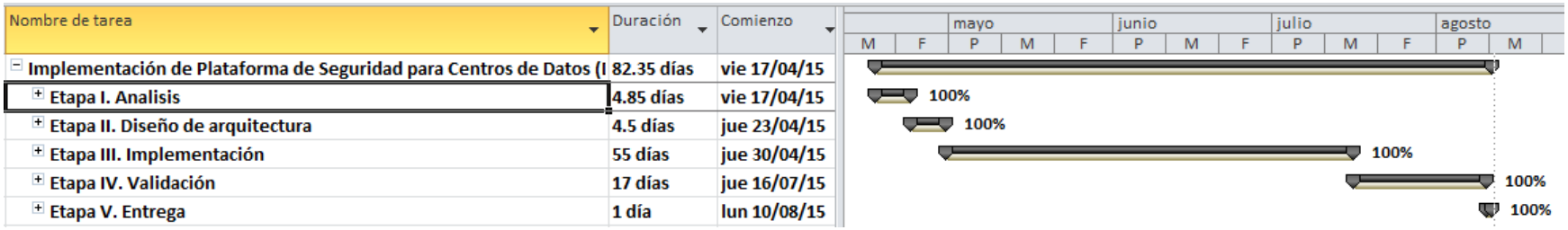


Figura 3.2. Diagrama de Gantt

q) Registro de Cambios

El registro de cambios fue llevado y registrado conforme al avance del proyecto y/o requerimientos. Estos fueron adicionados en la carpeta de la memoria técnica que se entregó a *la Universidad* al finalizar el proyecto. Entre los principales cambios se encuentran los siguientes:

- Se cambió la fecha de algunas de las actividades como escaneos de recomendaciones.
- Se solicitó adelantar algunas de las configuraciones, ya que no se vieron afectados los servidores en cuanto a recursos.
- Debido a problemas de compatibilidad, se requirió de hacer un cambio en la lista inicial de servidores a proteger cambiando algunos de ellos por otros.

Cabe mencionar que todos los cambios fueron solicitados por el área de Seguridad de la información de *la Universidad.*

Etapa 2: Análisis

Durante la etapa de análisis del proyecto implementación de plataforma de seguridad para centros de datos, OCM-IT con base en Proceso para desarrollo de Software se hizo entrega de la siguiente documentación:

- Documento de Requerimientos Técnicos.
- Documento de Situación Actual.

Documento de Requerimientos Técnicos

a) Resumen Ejecutivo

En este documento se especifican los objetivos y necesidades para la implementación de Trend Micro® Deep Security® en la infraestructura actual de *la Universidad*. Esta implementación nos permitió proteger las aplicaciones y los datos empresariales de filtraciones e interrupciones empresariales sin tener que aplicar costosos parches de urgencia.

Esto ayudó a *la Universidad* a simplificar sus actividades de seguridad y garantizar el cumplimiento de normativas en sus ambientes virtuales y computación en la nube.

b) Requerimientos de Hardware

En la tabla 3.4 se coloca como referencia el requerimiento de Hardware de los diferentes componentes de la arquitectura de Deep Security®:

Tabla 3.4 Requerimientos de Hardware de los componentes de Deep Security

Software	Descripción	Proporcionado	Cumple (Si/No)
Deep Security Manager	**Memoria RAM:** 8 GB **Disco Duro:** 5 GB recomendado **Sistema Operativo:** cualquiera de los que se muestran a continuación • Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit) • Windows Server 2008 (64-bit), Windows Server 2008 R2 (64-bit)	**Servidor:** SrvDeepSec **Memoria RAM:** 12GB **Disco Duro:** 100 GB recomendado **Sistema Operativo:**	**Si**

	• Windows 2003 Server SP2 (64-bit), Windows 2003 Server R2 (64-bit) • Red Hat Linux 5/6 (64-bit) **Nota: este equipo será proporcionado por *la Universidad*.**	Windows Server 2012 R2 (64-bit)	
Deep Security Data Base	**Memoria RAM:** 8 GB como mínimo **Versión:** cualquiera de las que se presentan a continuación • Oracle Database 11g, Oracle Database 11g Express • Oracle Database 10g, Oracle Database 10g Express • Microsoft SQL Server 2014, Microsoft SQL Server 2014 Express • Microsoft SQL Server 2012, Microsoft SQL Server 2012 Express • Microsoft SQL Server 2008, Microsoft SQL Server 2008 Express • Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008 R2 Express **Nota: la base de datos será proporcionada por *la Universidad*.**	**Servidor:** SrvDB **Memoria RAM:** 12 GB **Versión:** Microsoft SQL Server 2008	**Si**
Deep Security Agents	**Memoria RAM:** 512 MB **Disco Duro:** 1 GB recomendado **Sistema Operativo:** cualquiera de los que se muestran a continuación **Windows:** • Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 7 (32-bit and 64-bit) • Windows Server 2008 (32-bit and 64-bit)	**1.Servidor:** Srv01 192.XX.XX.XX **Memoria RAM:** 6 GB **Disco Duro:** 15.7 GB **Sistema Operativo:** Windows Server 2008 R2 Enterprise (64-bit)	**Si**

• Windows Server 2008 R2 (64-bit) • Windows Vista (32-bit and 64-bit) • Windows Server 2003 SP1 (32-bit and 64-bit) with patch "Windows Server 2003 Scalable Networking Pack" • Windows Server 2003 SP2 (32-bit and 64-bit) • Windows Server 2003 R2 SP2 (32-bit and 64-bit) • Windows XP (32-bit and 64-bit) • Hyper-V en Windows 2012 R2, 2012, 8, 8.1 and 2008 R2 **Linux:** • Red Hat 5 (32-bit and 64-bit) • Red Hat 6 (32-bit and 64-bit) • Red Hat 7 (64-bit) • Oracle Linux 5 (32-bit and 64-bit) • Oracle Linux 6 (32-bit and 64-bit) • CentOS 5 (32-bit and 64-bit) • CentOS 6 (32-bit and 64-bit) • CentOS 7 (64-bit) • SUSE 10 SP3 and SP4 (32-bit and 64-bit) • SUSE 11 SP1, SP2, and SP3 (32-bit and 64-bit) • CloudLinux 5 (32-bit and 64-bit) • CloudLinux 6 (32-bit and 64-bit) • Oracle Linux 5 (64-bit) Unbreakable Kernel • Oracle Linux 6 (64-bit) Unbreakable Kernel • Amazon AMI Linux EC2 (32-bit and 64-bit) • Ubuntu 10.04 LTS (64-bit) • Ubuntu 12.04 LTS (64-bit) • Ubuntu 14.04 LTS (64-bit)	**2.Servidor:** Srv02 192.XX.XX.XX **Memoria RAM:** 8 GB **Disco Duro:** 16.2 GB **Sistema Operativo:** Windows Server 2008 R2 Enterprise (64-bit)	**Si**
	3.Servidor: Srv03 192.XX.XX.XX **Memoria RAM:** 8 GB **Disco Duro:** 7.23 GB **Sistema Operativo:** Windows Server 2008 R2 Enterprise (64-bit)	**Si**
	4.Servidor: Srv04 172.XX.XX.XX **Memoria RAM:** 8 GB **Disco Duro:** 37.1 GB **Sistema Operativo:** Windows Server 2008 R2	**Si**

	Enterprise (64-bit)	
	5. Servidor: Srv05 192.XX.XX.XX **Memoria RAM:** 64 GB **Disco Duro:** 38.2 GB **Sistema Operativo:** Windows Server 2008 R2 Datacenter (64-bit)	**Si**
	6. Servidor: Srv06 192.XX.XX.XX **Memoria RAM:** 64 GB **Disco Duro:** 39.2 GB **Sistema Operativo:** Windows Server 2008 R2 Datacenter (64-bit)	**Si**
	7.Servidor: Srv07 192.XX.XX.XX **Memoria RAM:** 16 GB **Disco Duro:** 43.6 GB **Sistema Operativo:** Windows	**Si**

	Server 2008 R2 Enterprise (64-bit)	
	8.Servidor: Srv08 172.XX.XX.XX **Memoria RAM:** 96 GB **Disco Duro:** 97.3 GB **Sistema Operativo:** Windows Server 2008 R2 Enterprise (64-bit)	**Si**
	9.Servidor: Srv09 172.XX.XX.XX **Memoria RAM:** 4 GB **Disco Duro:** 3.54 GB **Sistema Operativo:** Windows Server 2003 SP 2 (32-bit)	**Si**
	10. Servidor: Srv10 192.XX.XX.XX **Memoria RAM:** 32 GB **Disco Duro:** 27 GB **Sistema Operativo:**	**Si**

	Linux Red Hat Enterprise Server 5.4 (64-bit)	
	11. Servidor: Srv11 172.XX.XX.XX **Memoria RAM:** 8GB **Disco Duro:** 27 GB **Sistema Operativo:** Linux Red Hat Enterprise Server 6.5 (64-bit)	**Si**
	12. Servidor: Srv12 172.XX.XX.XX **Memoria RAM:** 12GB **Disco Duro:** 27 GB **Sistema Operativo:** Linux Red Hat Enterprise Server 6.0 (64-bit)	**Si**
	13. Servidor: Srv13 192.XX.XX.XX **Memoria RAM:** 6 GB **Disco Duro:**	**Si**

	1.6 GB **Sistema Operativo:** Linux Red Hat Enterprise Server 5.4 (64-bit)	
	14. Servidor: Srv14 192.XX.XX.XX **Memoria RAM:** 2GB **Disco Duro:** 19 GB **Sistema Operativo:** Windows Server 2008 R2 Enterprise (32-bit)	**Si**
	15. Servidor: Srv15 192.XX.XX.XX **Memoria RAM:** 6GB **Disco Duro:** 15 GB **Sistema Operativo:** Windows Server 2012 Standard (64-bit)	**Si**
	Nota: los equipos en los cuales se instalarán los agentes serán proporcionados por *la Universidad.*	

c) Requerimientos Adicionales

A continuación en la tabla 3.5 se muestran requerimientos adicionales necesarios para tener acceso a la consola de administración web Deep Security Manager®:

Tabla 3.5 Requerimientos adicionales

Requerimientos Adicionales para consola de Administración Deep Security
• **Navegador web:** Firefox 24+, Internet Explorer 9.x, Internet Explorer 10.x, Internet Explorer 11.x, Chrome 33+, Safari 6+. Nota: Con Cookie habilitadas
• **Monitor:** con resolución a 1024 x 768 con 256 colores o mayor.
Conexión desde el manager a la base de datos
• La base de datos y el Deep Security Manager deben de encontrarse en la misma red y con una conexión LAN de 1 GB. **Nota:** una latencia de dos milisegundos o mejor es lo recomendado para una conexión del Manager a la base de datos.

d) Requerimientos de red e Internet

La solución Trend Micro® Deep Security® requiere de acceso a servicios de red e Internet para diferentes funciones. En la siguiente tabla 3.6 se enlistan los accesos requeridos.

Tabla 3.6 Requerimientos de Red y acceso a Internet

En el equipo en dónde se instalará Deep Security Manager		
Puertos:	4120	El puerto de "heartbeat" utilizado por los agentes y appliances de Deep Security® para comunicarse con el Deep Security Manager®.
	4119	Utilizado por el navegador de web para conectarse con Deep Security Manager®. También, es utilizado para la comunicación con el ESXi.
	1521	Puerto bidireccional del servidor de bases de datos Oracle.
	1433 y 1434	Puertos bidireccionales del servidor de bases de datos Microsoft SQL.
	389, 636 y 3268	Conexión con un servidor LDAP para la integración con Active Directory.

	25	Comunicación con un servidor SMTP para enviar correos electrónicos con alertas.
	53	Para DNS Lookup.
	514	Comunicación bidireccional con un servidor Syslog.
	443	Comunicación con cuentas en la nube: VMware vCloud, vCenter, vShield/NSX Manager, Amazon AWS, Microsoft Azure.
En el equipo en dónde se instalará Deep Security Agent, Agents con funciones de Relay y Appliances		
Puertos:	4122	Comunicación del Relay a Agents/Appliances.
	4118	Comunicación del Manager a los Agentes.
	4123	Utilizado para comunicaciones internas. No debe de abrirse hacia el exterior.
	80 y 443	Conexión hacia Trend Micro Update Server y Smart Protection Server.
	514	Comunicación bidireccional con un servidor Syslog.

Documento de Situación Actual

a) Alcance del Proyecto

La visión del alcance del Proyecto desde el punto de vista de la infraestructura actual comprende los siguientes puntos:

a) Definición de los Requerimientos Funcionales: Definir la Infraestructura involucrada en la implementación inicial de Trend Micro® Deep Security® y las herramientas complementarias de la solución en *la Universidad*.
b) Recolección de información de los recursos utilizados actualmente en la infraestructura de servidores de *la Universidad*.
c) Recolección de Información. En esta etapa se recolectó información provista por el cliente acerca de:

- Infraestructura actual de la red.
- Características de la seguridad de la información con las que opera *la Universidad* sobre el Centro de Datos.

d) Recolección de políticas aplicadas a la Infraestructura: En esta etapa se recolectó información provista por el cliente acerca de los lineamientos, reglas o procedimientos vigentes aplicados a la administración de la infraestructura relacionada directamente con la implementación de Trend Micro® Deep Security®, tales como: políticas de seguridad, regulaciones, versiones de S. O., control de accesos, etc.

b) Estatus de Suficiencia de Datos de Equipo (Hardware)

A continuación se lista el Hardware de la infraestructura actual destinada para la instalación de Trend Micro® Deep Security Manager.

En la Tabla 3.7 se indican las características de un Servidor Virtual designado para la instalación de Trend Micro® Deep Security®:

Tabla 3.7 Características Deep Security Manager

Rol del Servidor: Deep Security Manager
Nombre del Servidor: XXXXXXXX
IP del servidor: 172.XX.XX.XX
Memoria RAM: 12 GB
Disco Duro: 100 GB
Procesador: Intel® Xeon® CPU
Sistema Operativo: Windows Server 2012 R2 Standard

c) Site Principal

A continuación se muestra un diagrama de la configuración que corresponde al sistema de seguridad para el Centro de Datos de *la Universidad* (véase figura 3.3):

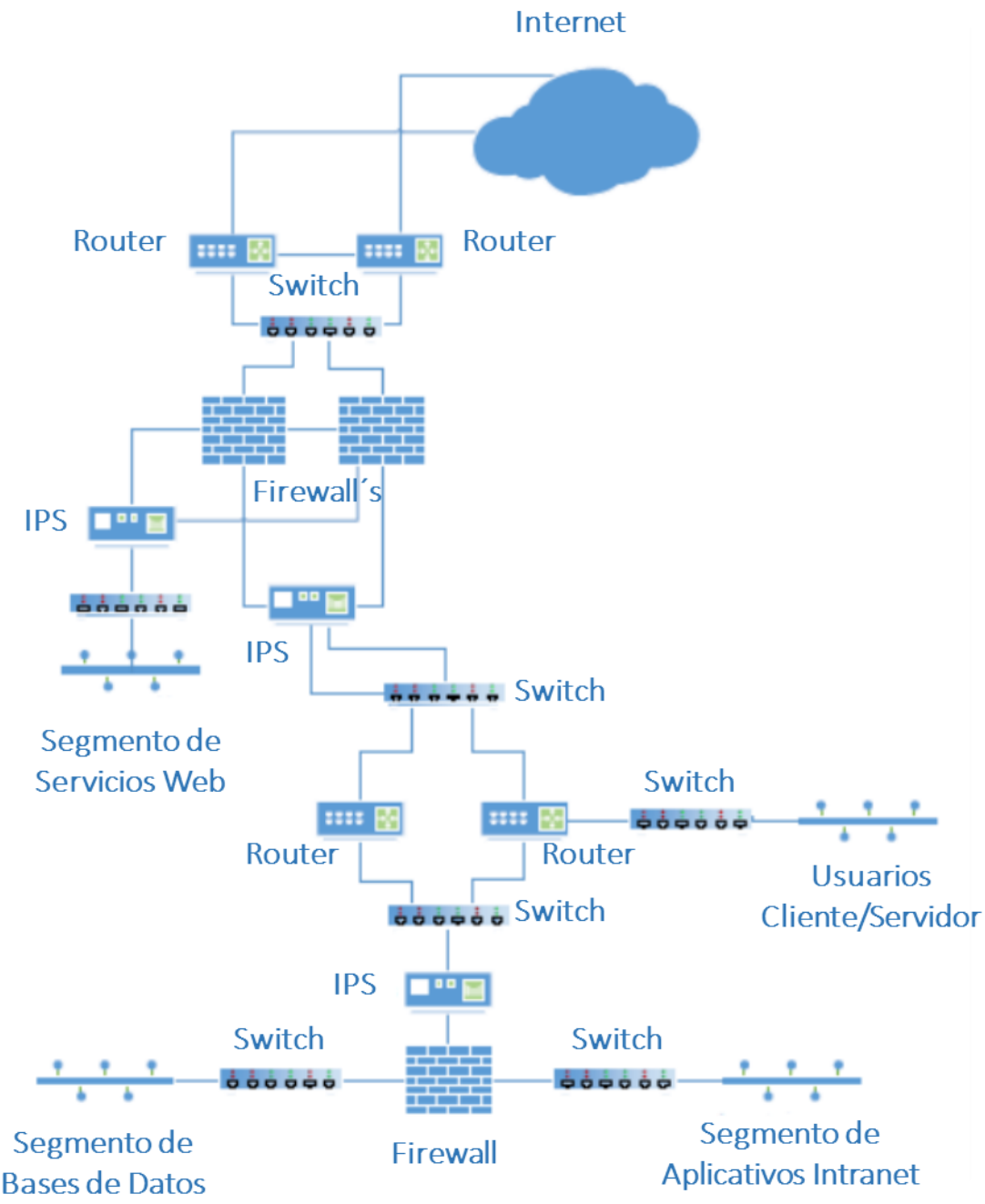


Figura 3.3 Diagrama de configuración Centro de Datos

d) Análisis de Seguridad Situación Actual

- **Seguridad lógica en servidores.** se cuenta con la herramienta de seguridad anti-malware del fabricante Symantec en servidores de entre los cuales se brindan diferentes servicios como AD, Exchange, DNS, entre otros más.

- **Seguridad física y de entorno.** El edificio en donde se encuentra el Site cuenta con personal de seguridad que permiten el paso únicamente a los empleados o personas autorizadas. También existe una chapa con llave que impide el libre acceso a la oficina en donde se encuentra la infraestructura de *la Universidad*.
- **Comunicaciones y administración de operaciones.** Todos los movimientos a la infraestructura de red deben de estar acompañados por la previa autorización de las áreas involucradas por parte de *la Universidad*.
- **Control de acceso.** Todo acceso al centro de datos es con conocimiento y previa autorización del personal de IT de *la Universidad*

e) Criterios de Aceptación

Este proyecto se dio por concluido al finalizar cada una de las actividades descritas en las diferentes etapas en el Plan de Trabajo y con la entrega de los documentos descritos en la sección de entregables, así como también la validación de las pruebas de funcionalidad de la solución.

Nota: Los documentos son proporcionados conforme el avance de las etapas del proyecto.

Etapa 3: Diseño

Durante la etapa de diseño en el proyecto de Implementación de la plataforma de seguridad para centros de datos, OCM-IT con base en el Proceso para desarrollo de Software se hace entrega de la siguiente documentación:

- Diseño Lógico.
- Diseño Físico.

Diseño Lógico

a) Introducción

Trend Micro® Deep Security® ofrece una protección completa avanzada y muy eficiente para los servidores en los centros de datos dinámicos. Deep Security® cuenta con diversos módulos integrados para ampliar la plataforma y garantizar así la seguridad de servidores, las aplicaciones y los datos localizados en servidores físicos, virtuales y/o basados en la nube. Puede elegir una protección con o sin agente que incluya características de antimalware, detección y prevención frente a intrusiones, cortafuegos, protección de aplicaciones web, supervisión de integridad y capacidades de inspección de registros en un único agente de software de gestión centralizada.

Deep Security® protege los datos confidenciales y las aplicaciones básicas para evitar extracción de información y garantizar la continuidad de la actividad empresarial y, al mismo tiempo, permite simplificar las operaciones de seguridad a la par con el cumplimiento de estándares y normas importantes; logrando así una aceleración en el retorno de inversión en proyectos de virtualización y computación en la nube. Gracias a esta solución, las empresas pueden identificar actividades y comportamientos sospechosos y adoptar medidas proactivas o preventivas para garantizar la seguridad de los centros de datos.

Deep Security Agent, Deep Security Manager y el Centro de Seguridad colaboran a la perfección para ofrecer protección dinámica a su centro de datos.

b) Objetivo

Este documento tiene los siguientes objetivos:

- Informar conceptualmente sobre todos los elementos que comprenden la solución propuesta.
- Resumir los requerimientos clave que se utilizarán para el diseño.
- Detallar las suposiciones que se han hecho a fin de progresar en el diseño.
- Proporcionar una vista general de los elementos fundamentales de la solución propuesta.
- Realizar estimaciones de escala, incluyendo número de servidores, hardware requerido y almacenamiento.

c) Supuestos

- Se consideró que *la Universidad* proporcionaría toda la información necesaria (diagramas, topologías, direcciones IP, enlaces, sitios, etc.) la cual fue entregada para la ejecución de la fase de análisis y diseño.
- Se consideró la ejecución de pruebas de funcionalidad del agente de Deep Security en todos los servidores asegurados, las cuales se realizaron en conjunto con el personal que *la Universidad* asigne para esta actividad.

d) Limitantes

Esta sección indica las actividades que no se encuentran dentro de la implementación y desarrollo de este proyecto:

- No se realizará ningún tipo de cambio en los elementos de seguridad (Firewall), red y/o comunicaciones, plataformas de S.O y aplicaciones. Solo nos enfocaremos en la recopilación y análisis de datos.
- No está incluida la solución de servicios, aplicaciones, plataformas de S.O que estén operando de manera incorrecta dentro del dominio de *la Universidad*.
- No se planteó ningún tipo de desarrollo para servicios, aplicaciones y plataformas de S.O. para cumplir con normas de estándares de la empresa.
- La instalación de nuevas versiones de software de aplicaciones y S. O. a proteger, son responsabilidad de *la Universidad*.
- Todo aquello que no sea explícito en este documento no está incluido y deberá ser negociado por las partes involucradas.

e) Conceptos Generales de Deep Security®

Trend Micro® Deep Security® ofrece una protección avanzada, completa y muy eficiente para servidores en los centros de datos dinámicos; ya sean físicos, virtuales o en la nube. Deep Security® cuenta con diversos módulos integrados para ampliar la plataforma y garantizar así la seguridad del servidor, las aplicaciones y los datos localizados en servidores físicos, virtuales y/o basados en la nube, así como escritorios virtuales. Puede elegir una protección con o sin agente que incluya características de antimalware, detección y prevención frente a intrusiones, firewall, protección de aplicaciones web, supervisión de integridad y capacidades de inspección de registros en un único agente de software de gestión centralizada.

Deep Security® protege los datos confidenciales y las aplicaciones básicas para evitar las filtraciones de datos y garantizar la continuidad de la actividad empresarial y, al mismo tiempo, permite simplificar las operaciones de seguridad a la par que lleva al cumplimiento de estándares y normas importantes; logrando así una aceleración en el retorno de inversión en proyectos de virtualización y cómputo en la nube. Gracias a esta solución, las empresas pueden identificar actividades y comportamientos sospechosos y adoptar medidas proactivas o preventivas para garantizar la seguridad de los centros de datos.

Deep Security Agent®, Deep Security Manager® y el Centro de Seguridad colaboran a la perfección para ofrecer protección dinámica a su centro de datos.

f) Módulos de protección

Es posible personalizar Deep Security para que se adapte a la estrategia de seguridad del centro de datos de su empresa por medio de los módulos de protección que a continuación se describen:

1. Antimalware

Se integra en entornos VMware para una protección sin agente y también permite el uso del agente para servidores físicos y equipos virtuales en el modo local.

Integra nuevas API´s de VMware vShield Endpoint con las que ofrece protección antimalware sin agente para los equipos virtuales de VMware sin impacto en el equipo host. Ayuda a evitar las interrupciones de seguridad que suelen experimentarse durante los escaneos de anti-malware completos del sistema y las actualizaciones de patrones. Asimismo, cuenta con protección antimalware basado en agente para proteger servidores físicos, servidores virtuales basados en Hyper-V y XenServer, servidores basados en nube pública y equipos virtuales en el modo local. Coordina la protección con la configuración del modelo con y sin agente para brindar seguridad adaptable que defiende los servidores virtuales durante el tránsito entre el centro de datos y la nube pública.

2. Reputación Web

Protección robusta contra amenazas web para servidores y escritorios virtuales.

Se integra con las capacidades de reputación web de Trend Micro® Smart Protection Network® para salvaguardar usuarios y aplicaciones, bloqueando el acceso a URL´s maliciosas. Provee las mismas capacidades en ambientes en modo sin agente a través del appliance virtual que también entrega tecnologías de seguridad sin agente para mejor protección sin impacto en el equipo host.

3. Monitoreo de integridad

Detecta y reporta cambios maliciosos y no esperados en archivos y registros de sistema en tiempo real.

Provee a los administradores con la habilidad de rastrear ya sea cambios autorizados o no autorizados realizados en la instancia. La habilidad de detectar cambios no autorizados es un componente crítico en la estrategia de seguridad en la nube, ya que proporciona visibilidad en cambios que pueden indicar que se ha comprometido alguna instancia.

4. Inspección de registros

Ofrece visibilidad de los sucesos de seguridad importantes ocultos en los archivos de registro.

Optimiza la identificación de los sucesos de seguridad más importantes que pueden pasar desapercibidos entre múltiples entradas de registro a lo largo del centro de datos. Reenvía los sucesos sospechosos a un sistema SIEM o al servidor de registros centralizado para las tareas de correlación, documentación y archivado. Utiliza y mejora el software de código abierto disponible en OSSEC.

5. **Prevención de intrusos**

Permite la detección y prevención de intrusiones, la protección de aplicaciones Web y el control de aplicaciones.

Detección y prevención de intrusos (parcheo virtual):

Evita el ataque de las vulnerabilidades conocidas desde un sinfín de orígenes (parcheo virtual).

Contribuye a conseguir una protección rápida frente a ataques conocidos y de día cero. Utiliza reglas para blindar las vulnerabilidades conocidas (por ejemplo, aquellas que Microsoft hace públicas mensualmente) frente a una larga lista de explotaciones. Ofrece protección inmediata de vulnerabilidades para más de 100 aplicaciones, incluidas bases de datos, sitios Web, correo electrónico y servidores FTP. Las reglas que protegen las nuevas vulnerabilidades descubiertas se entregan automáticamente en cuestión de horas y pueden enviarse a miles de servidores en unos minutos, sin necesidad de reiniciar el sistema.

Control de aplicaciones Web

Le defiende frente a las vulnerabilidades de las aplicaciones Web.

Permite cumplir el requisito PCI 6.6 (referente al cumplimiento de niveles de seguridad en la forma en la cual se acepta, procesa y transmite información de tarjetas de crédito) para la protección de las aplicaciones Web y los datos que éstas procesan. Protege frente a ataques SQL Injection, secuencias de comandos de sitios cruzados (XSS) y otras vulnerabilidades de las aplicaciones Web. Ofrece un blindaje de las vulnerabilidades hasta que puedan completarse las correcciones del código.

Control de aplicaciones

Identifica software malicioso que accede a la red.

Aumenta la visibilidad y el control de las aplicaciones que acceden a la red. Identifica el software malicioso que accede a la red y reduce la exposición a vulnerabilidades de sus servidores.

6. Firewall

Disminuye la cantidad de ataques hacia servidores físicos y virtuales.

Centraliza la gestión de políticas de firewall para el servidor mediante el uso de un firewall de inspección de estado bidireccional. Admite la creación de zonas de equipos virtuales y previene los ataques de denegación de servicio (DoS). Ofrece una amplia cobertura para todos los protocolos basados en IP y tipos de tramas, así como un filtrado preciso para puertos y direcciones IP y MAC.

g) Resumen diseño lógico Deep Security

Trend Micro® Deep Security®, brinda a *la Universidad* una protección para los servidores del Centro de Datos frente a malware, virus de red, amenazas basadas en web, vulnerabilidades, robo de información, entre otros más.

Como solución integrada, Trend Micro® Deep Security® consta de un agente y/o cliente que reside en el punto final (servidor a proteger) y de un programa servidor (manager) que administra todos los agentes. El agente protege el punto final e informa sobre el estado de su seguridad al servidor. El servidor, a través de la consola de administración basada en Web, simplifica la aplicación de políticas de seguridad coordinada y la implementación de actualizaciones para todos los agentes.

h) Funcionalidad

A continuación se muestra la Arquitectura de Trend Micro® Deep Security® (véase figura 3.4) donde se describe el funcionamiento y el flujo de datos de cada uno de los componentes necesarios para la protección de los Servidores.

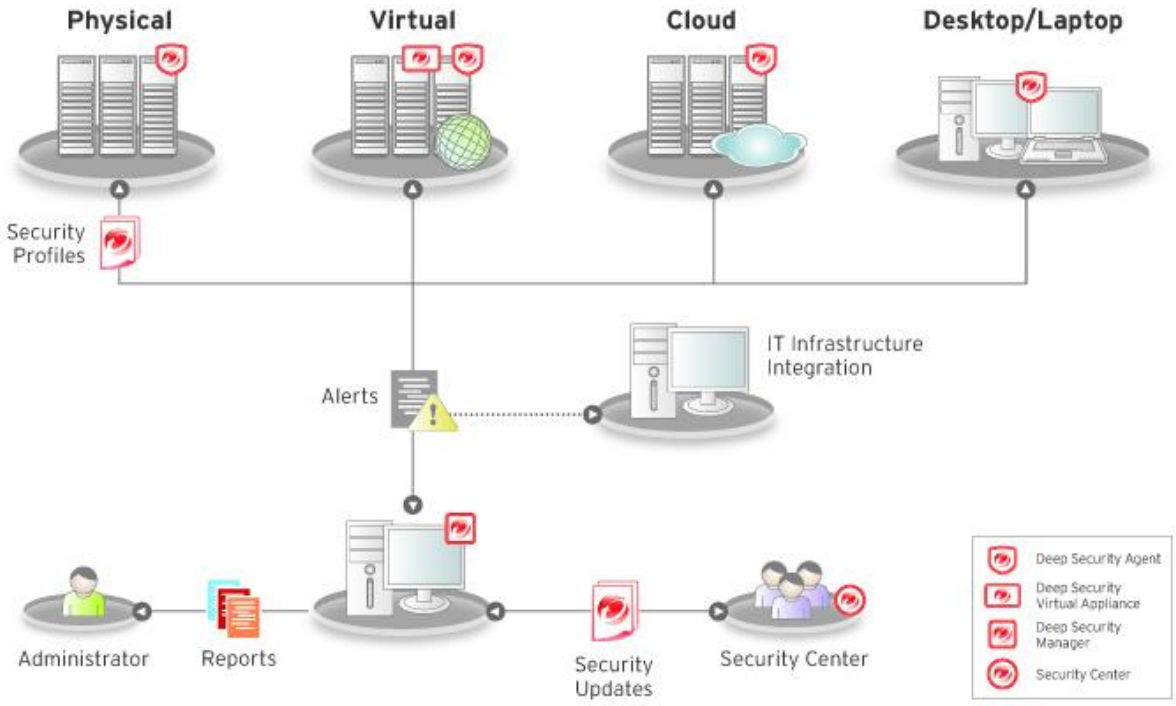


Figura 3.4 Arquitectura Deep Security®

i) Objetos

A continuación se identifican los elementos involucrados en el proceso de definición del diseño lógico de Trend Micro® Deep Security®.

- Instalación de la consola de administración de **Deep Security Manager®**.
- Servidor Virtual con Sistema Operativo Windows Server 2012 R2 Standard actualizado para la instalación de la solución, el cual se agregara a la red actualmente en producción.
- Base de Datos SQL Server 2008 instalada previamente.
- Instalación de los 15 agentes de seguridad para Servidores definidos en producción.
- Reconocimiento de los agentes en la consola de administración web.

j) Acceso

El acceso es a través de los procesos de autenticación de Microsoft Active Directory y/o la cuenta local de administrador para fines de administración, y por medio de cuentas de usuarios de Microsoft Active Directory.

MasterAdmin: Es el administrador que posee todos los atributos de Domain Admin y Local Administrator necesarios para crear, modificar, alterar y eliminar cualquier componente administrable de **Trend Micro® Deep Security®.**

k) Diagrama Lógico de la Arquitectura de Trend Micro® Deep Security® para *la Universidad*

A continuación se muestra el diagrama de diseño lógico presentado para *la Universidad* (véase figura 3.5) en donde se muestra que la plataforma de Trend Micro® Deep Security® consta de un agente y/o cliente que reside en el punto final (servidor a proteger físico o virtual) y de un programa servidor (manager) que administra todos los agentes. El agente protege el punto final e informa sobre el estado de su seguridad al servidor. El servidor, a través de la consola de administración basada en Web, simplifica la aplicación de políticas de seguridad coordinada y la implementación de actualizaciones para todos los agentes:

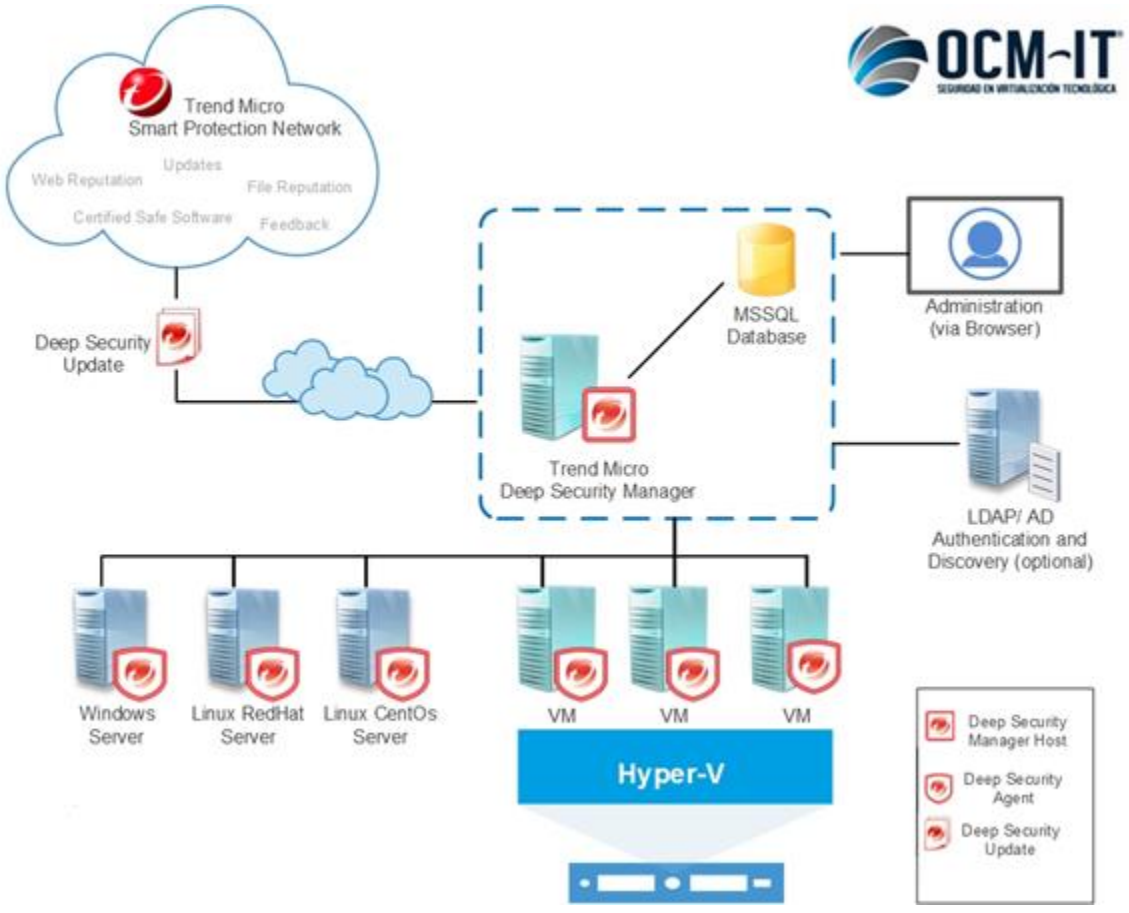


Figura 3.5 Diagrama de diseño Lógico

En la tabla 3.8 se describen las **ca**racterísticas del Rol del Servidor que se utilizará en la implementación de la solución de **Trend Micro® Deep Security®** para *la Universidad***.**

Tabla 3.8 Características Deep Security Manager

Distribución	
Rol del Servidor:	Trend Micro® Deep Security Manager
Nombre del Servidor:	**XXXXXX**
Dirección IP:	172.XX.XX.XX
Procesador:	2 CPU
Memoria RAM:	12 GB
Disco Duro:	100 GB
Producto:	Trend Micro® Deep Security® 9.5

Las características generales del diseño lógico son las siguientes:

- La solución de seguridad para Centros de Datos Trend Micro® Deep Security® se implementó como parte de la propuesta de solución de seguridad de Servidores de acuerdo a las necesidades expresadas por *la Universidad*, y se conforma de las siguientes actividades:

    a) Instalación y configuración de 1 Servidor Virtual que tendrá el Rol de **Trend Micro® Deep Security Manager**.
    b) Implementación de políticas de seguridad de acuerdo al Rol de los Servidores.

l) Criterios de Aceptación

Este proyecto se dio por concluido una vez finalizadas cada una de las actividades en las etapas del proyecto y con la entrega de los documentos descritos en la sección de entregables, así como la validación de las pruebas de funcionalidad de la solución.

Diseño Físico

a) Resumen Diseño Físico

En este documento se proporciona un resumen del ambiente de la solución de Trend Micro® Deep Security®, sus dependencias y arquitectura establecida para *la Universidad*.

Se requiere de una infraestructura capaz de soportar las tareas y servicios de seguridad donde serán implementados según los objetivos del proyecto. Para ello se considera que *la Universidad* ya cuenta con los Servidores Físicos y/o Virtuales en donde se realizará la implementación de Trend Micro® Deep Security®.

b) Diagrama diseño físico Arquitectura de Trend Micro® Deep Security®

A continuación se muestra el diagrama de diseño físico presentado para la Universidad (véase figura 3.6) en donde se muestra un resumen del ambiente de la solución de Trend Micro® Deep Security® sus dependencias y arquitectura establecida para *la Universidad, s*e requiere de una infraestructura capaz de soportar las tareas y servicios de seguridad según los objetivos del proyecto:

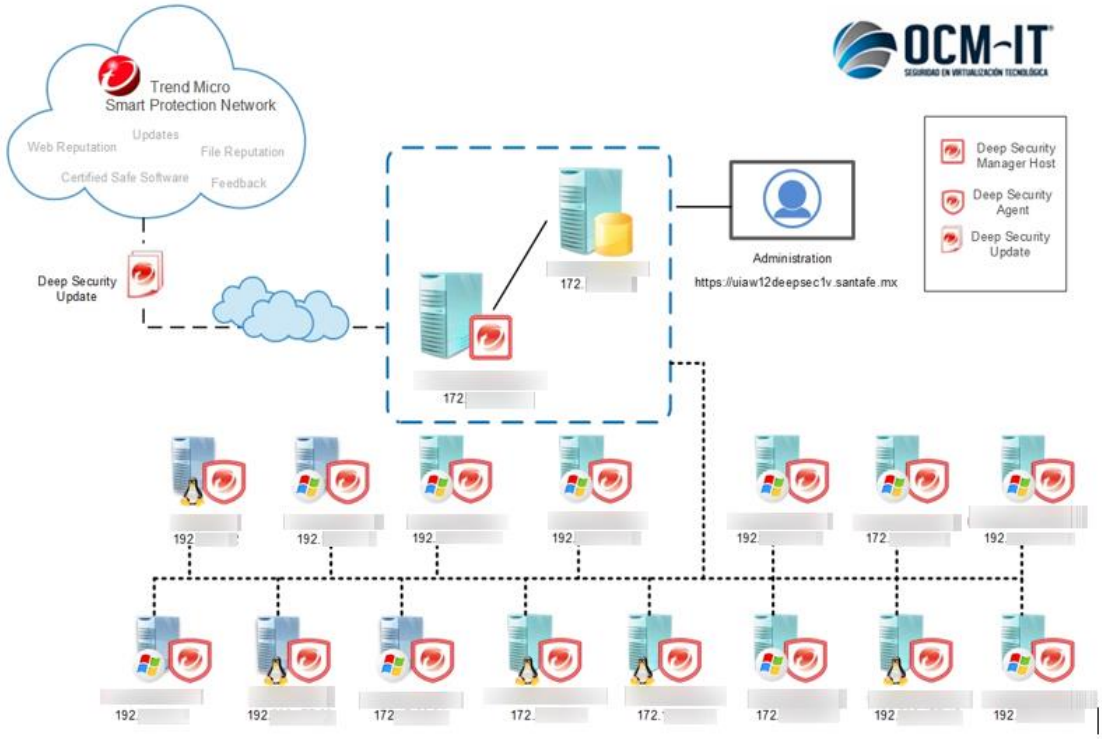


Figura 3.6 Diagrama de diseño físico

c) Restricciones de Ambiente y Premisas del Proyecto

Se muestran algunas condiciones de ambiente y premisas que se deben tomar en cuenta para el éxito de la implementación de la solución de seguridad para centros de datos Trend Micro® Deep Security®:

- Se considera utilizar una máquina virtual con Windows Server 2012 R2 con actualizaciones de seguridad del Sistema Operativo para la instalación del servidor de la solución de seguridad para centros de datos Trend Micro® Deep Security®.
- Denominación de Nombre host del Servidor, el cual será definido por *la Universidad* y previamente ingresado a dominio.
- Se deberá de contar con una dirección IP estática para el Servidor en el que se implementará la tecnología Trend Micro® Deep Security®.
- Se requiere que se permita el tráfico de forma bidireccional por los puertos:
    - 4120: puerto heartbeat, utilizado por los agentes de Deep Security® para comunicarse con Deep Security® Manager.
    - 4119: puerto de administración, es el puerto utilizado por el navegador web para conectarse con Deep Security® Manager.
    - 1433 y 1434: puerto de conexión con la base de datos Microsoft SQL.
    - 389, 636 y 3268: puerto de conexión con servidores LDAP para la integración con Active Directory.
    - 25: puerto de comunicación con servidores SMTP para envió de alertas por correo electrónico.
    - 53: para realizar DNS lookup.
    - 514: puerto de comunicación para la integración con servidores Syslog.
    - 443: puerto de comunicación con VMware, vCloud, vCenter, vShield Manager.
    - 4122: puerto de comunicación del Relay hacia el agente Deep Security®.
    - 4118: puerto de comunicación Manager-Agente Deep Security®.
    - 4123: utilizado por los agentes Deep Security® para comunicación interna.
    - 80 y 443: puerto de comunicación utilizado por los agentes Deep Security® para conectarse con Trend Micro Update Server y Smart Protection Server.

- Se deberá de contar con la correcta resolución de nombres (DNS) para poder invocar por FQDN al Servidor de Trend Micro® Deep Security® Manager.
- Se considera que *la Universidad* ha brindado toda la información necesaria y requerida para identificar todas las posibles restricciones que puedan presentarse por los medios de seguridad y dispositivos con que cuentan.

d) Dependencias del Proyecto

Esta propuesta no contempla la resolución de problemas concernientes a la operación de otras tecnologías que no se contemplen integrar en la presente documentación tales como

administración de software y aplicaciones de los usuarios o equipos que no estén conforme el esquema original, su instalación y configuración por omisión.

Los requerimientos solicitados a *la Universidad* se deben de proveer en el tiempo necesario para no retrasar las actividades del plan de trabajo.

Esta propuesta cubre los alcances expuestos en la sección de Alcances para cada una de las etapas del proyecto. Si como resultado del diseño existiera algún requerimiento adicional a los expuestos en este documento, se tendrá que negociar por ambas partes.

Una vez aceptado el Diseño por parte de *la Universidad* se inicia con la etapa de Implementación, en caso de que se soliciten cambios que impacten al plan de trabajo original en tiempo, será necesario realizar un control de cambios el cual puede impactar en el costo de la solución y se tendrá que negociar por ambas partes (*la Universidad* y OCM-IT Seguridad en Virtualización Tecnológica).

Es necesario que la infraestructura actual de red se mantenga en perfecto estado y funcionando, esto permitirá la correcta implementación de la solución de seguridad para centros de datos Trend Micro® Deep Security® sin contratiempos.

e) Dependencias de Ambiente de Hardware

El hardware que proporcionará *la Universidad* para desarrollar la implementación de Trend Micro® Deep Security® deberá estar debidamente conectado al ambiente de red corporativa.

f) Dependencias de Ambiente de Software

En la tabla 3.9 se listan las dependencias de software que se tienen para la implementación de la herramienta de seguridad para Centros de Datos Deep Security®:

Tabla 3.9 Dependencias de Software

Licenciamiento de:
Microsoft Windows Server 2012 R2
Microsoft SQL Server 2008/2012

Trend Micro® Deep Security®

Controladores, aplicaciones y utilerías requeridas para el equipo descrito en dependencia de hardware y/o lo necesario en todos los equipos involucrados en la implementación. Las restricciones de software pueden consistir en la ejecución y estados de servicios dictados por las políticas de *la Universidad*.

g) Topología de la Solución

A los Servidores que proporcionan el servicio se les denominará Site (Empresa) [Ejemplo: Site *l*a Universidad], para el Site de *la Universidad* se cuenta con una infraestructura que albergará el servicio de Trend Micro® Deep Security®.

Se proporciona almacenamiento necesario para albergar en el disco duro local del Servidor la implementación de Trend Micro® Deep Security®, así como también espacio necesario para el registro de eventos.

h) Servicios

Los servicios y/o aplicaciones que deben estar habilitados y en operación en los servidores a proteger son los siguientes:

- Aplicaciones del fabricante del hardware.
- Servicios de hardware requeridos de los dispositivos que el servidor tenga de fábrica.
- Conexiones de red.
- Acceso remoto desde un equipo cliente desde donde se llevara a cabo la instalación de la solución Trend Micro® Deep Security®, en caso de que la instalación se realice remotamente.
- Direcciones IP (Internet Protocol) asignadas a los equipos a contemplar para la implementación.

i) Direccionamiento

a) Capa de Usuario

Las direcciones IP a nivel de cliente son administradas por el área de sistemas de *la Universidad*. El método de administración de asignación de IP's pertenece a *la Universidad* y es información confidencial.

b) Capa de Servidor

La asignación de dirección IP para el Servidor de Trend Micro® Deep Security® Manager es de tipo fija y es administrada por el departamento de sistemas de *la Universidad*.

Se entiende que la política de asignación de IP's pertenece a *la Universidad* y es información confidencial.

Nota: el direccionamiento es tratado por capas debido a que los clientes normalmente aplican una nomenclatura de direccionamiento IP para equipos de usuario y otra diferente para los servidores.

j) Resolución de Nombres

Configuración DNS: *la Universidad* cuenta con un servidor DNS (Resolución de nombres), el cual se dio por hecho que funciona adecuadamente.

k) Estándares de Nombres

1) Servidores: el nombre del Servidor de Trend Micro® Deep Security® será determinado por políticas de asignación de nombres de servidores pertenecientes a *la Universidad*.

2) Usuarios: el nombre de los usuarios está definido por políticas de asignación de nombres pertenecientes a *la Universidad*.

l) Nombre y descripción de Servidor Deep Security Manager®

En la tabla 3.10 se describe la información tanto de Hardware, Software, red, espacio en disco duro de cada uno de los Servidores que se utilizaran en la implementación de la solución de Trend Micro® Deep Security® para *la Universidad*.

Tabla 3. 10 Nombre y descripción de servidor Deep Security Manager®

Distribución de componentes	
Rol del Servidor:	**Trend Micro® Deep Security® Manager**
Nombre del Servidor:	**XXXXXX**
Dirección IP:	**172.XX.XX.XX**
Procesador:	**2 CPU**
Memoria RAM:	**12 GB**
Disco Duro:	**100 GB**

a) Localización del Servidor

La organización física de la infraestructura en donde se implementara la solución de Trend Micro® Deep Security® consiste en un Site ubicado en las oficinas de *la Universidad*, en México Distrito Federal.

b) Dimensionamiento de Servidores

Los dimensionamientos se realizaron según requerimientos y estos pertenecen a *la Universidad* y es información con trato confidencial.

c) Infraestructura y almacenamiento de información

Los servidores deben tener a su disposición al menos un disco duro local dedicado a la instalación de Trend Micro® Deep Security®.

m) Criterios de Aceptación

Este proyecto se dará por concluido al finalizar cada una de las actividades en las etapas del proyecto y con la entrega de los documentos descritos en la sección de entregables, así como la validación de las pruebas de funcionalidad de la solución.

Etapa 4: Implementación

Durante la etapa de Implementación en el proyecto de Instalación de la plataforma de seguridad para centros de datos, OCM-IT con base en el Proceso para desarrollo de Software y siguiendo la metodología MSF se realizaron las siguientes actividades primarias durante esta etapa:

1) Instalación de Deep Security Manager (DSM):

a. Instalación de consola Deep Security Manager (DSM) en el servidor virtual proporcionado por *la Universidad*.
b. Configuración de consola Deep Security Manager (DSM) de acuerdo a las necesidades presentadas por *la Universidad*.

2) Creación de perfil de seguridad para los servidores a proteger con el agente de Deep Security®:

a. Instalación de Agente Deep Security para 15 servidores, definido durante el contrato.
b. Definición de perfiles de acuerdo a tipo de Sistema Operativo y aplicaciones de los servidores a proteger.
c. Aplicación de perfil de acuerdo a SO y aplicativos de los servidores a proteger de *la Universidad*.

3) Módulo de Antimalware y Web Reputation:

a. Habilitar módulo de protección de Antimalware y Web Reputation en la consola de administración Deep Security® Manager.
b. Definición de listas de exclusiones para los 4 tipos de escaneos con los cuales cuenta la herramienta.
c. Configuración de tipos de escaneo (Real-time Scan, Manual Scan, Scan Now y Scheduled Scan).
d. Configuración de acciones por tipo de malware para cada uno de los escaneos.
e. Validación de procesos de escaneos en tiempo real.
f. Prueba de consumo de recursos en los servidores protegidos con los módulos de Anti-malware y Web Reputation.
g. Análisis de métricas de consumo de recursos.

4) Módulo Intrusion Prevent:

a. Escaneo de recomendaciones en busca de vulnerabilidades (virtual patch) en el SO y aplicativos de los servidores protegidos.
b. Revisión de reglas recomendadas con el personal asignado por parte de *la Universidad*.
c. Validación por parte del personal de *la Universidad* de reglas de recomendación por aplicar a cada uno de los 15 servidores protegidos con el agente de Deep Security®.
d. Aplicación de reglas de recomendación (virtual patch).
e. Análisis de comportamiento de servidores protegidos.
f. Configuración de alertas de las reglas de recomendación aplicadas.

5) Módulo de Integrity Monitoring (IM):

    a. Habilitar Módulo de IM en la consola de administración Deep Security® Manager.
    b. Ejecución de escaneo de recomendaciones en cada uno de los 15 servidores protegidos con el agente de Deep Security.
    c. Creación de Baseline para cada uno de los servidores protegidos.
    d. Validación por parte del personal de *la Universidad* de reglas de recomendación por aplicar a los servidores protegidos.
    e. Aplicación de reglas de recomendación.
    f. Creación de reglas personalizadas (en caso de ser necesario).

6) Módulo de Log Inspection (LI):

    a. Habilitar Módulo de LI en la consola de administración Deep Security® Manager.
    b. Ejecución de escaneo de recomendaciones en cada uno de los 15 servidores protegidos con el agente de Deep Security.
    c. Validación por parte del personal de *la Universidad* de reglas de recomendación por aplicar a los servidores protegidos.
    d. Aplicación de reglas de recomendación.
    e. Creación de etiquetas por eventos específicos para cada ambiente de servidores.
    f. Configuración de alertas.

7) Módulo de Firewall (FW):

    a. Habilitar Módulo de FW en la consola de administración Deep Security Manager®.
    b. Ejecutar escaneo de puertos en cada uno de los 15 servidores protegidos con el agente de Deep Security®.
    c. Generación de lista de puertos y validación de la misma por parte del personal de *la Universidad*.
    d. Generación de reglas de firewall de acuerdo al perfil de cada uno de los 15 servidores protegidos.
    e. Habilitar Modulo de Firewall en los 15 servidores.
    f. Configuración de alertas.

En la tabla 3.11 se muestran las configuraciones que se implementaron en cada uno de los 15 servidores protegidos durante el proyecto de Implementación de la plataforma de seguridad para centros de datos Trend Micro® Deep Security® 9.5 en la infraestructura de *la Universidad*, así como también la cantidad de reglas aplicadas ya sean personalizadas o recomendadas en los 6 módulos de los cuales se compone la plataforma de seguridad:

Nota: debido a temas de confidencialidad con el cliente en algunos casos no es posible mostrar los datos reales, ya que la información presentada en este documento podría utilizarse por terceros con fines maliciosos, en esos casos se mostrará el mensaje CONFIDENCIAL, indicando que debido a la naturaleza de la información no se mostrará en el presente documento.

Tabla 3.11 Módulos de protección y configuración para los 15 servidores protegidos

Hostname	Servicio	IP	S.O.	Módulos	Anti-malware	Real-time Scan	Scheduled Scan	Manual Scan	Web Reputation	Firewall	Intrusion Prevention	Integrity Monitoring	Log Inspection
Srv01	WebServer	192.XX.XX.XX	Win 2008 R2	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 58 reglas	On - 197 reglas	On - 31 reglas	On - 8 reglas
Srv02	WebServer	192.XX.XX.XX	Win 2008 R2	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 58 reglas	On - 198 reglas	On - 31 reglas	On - 8 reglas
Srv03	WebServer	192.XX.XX.XX	Win 2008 R2	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 58 reglas	On - 233 reglas	On - 31 reglas	On - 8 reglas
Srv04	WebServer	172.XX.XX.XX	Win 2008 R2	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 59 reglas	On - 161 reglas	On - 30 reglas	On - 8 reglas
Srv05	WebServer	192.XX.XX.XX	Suse Enterprise 10	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	NA (No soportado)	On - 71 reglas	On - 101 reglas	On - 30 reglas	On - 6 reglas
Srv06	Base de datos	192.XX.XX.XX	Win 2008 R2	AM, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	OFF	On - 61 reglas	On - 17 reglas	On - 29 reglas	On - 7 reglas
Srv07	Base de datos	192.XX.XX.XX	Win 2008 R2	AM, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	OFF	On - 63 reglas	On - 17 reglas	On - 29 reglas	On - 7 reglas
Srv08	WebServer	192.XX.XX.XX	Linux RedHat 5.4	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 24 reglas	On - 108 reglas	On - 29 reglas	On - 6 reglas
Srv09	WebServer	192.XX.XX.XX	Win 2008 R2	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 71 reglas	On - 164 reglas	On - 30 reglas	On - 9 reglas
Srv10	Exchange	172.XX.XX.XX	Win 2008 R2	AM, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	OFF	On - 91 reglas	On - 229 reglas	On - 30 reglas	On - 9 reglas
Srv11	Base de datos	172.XX.XX.XX	Linux RedHat 6.5	AM, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	OFF	On - 16 reglas	On - 101 reglas	On - 24 reglas	On - 7 reglas
Srv12	WebServer	172.XX.XX.XX	Linux RedHat 5.5	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 15 reglas	On - 145 reglas	On - 26 reglas	On - 7 reglas
Srv13	WebServer	172.XX.XX.XX	Win 2003	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 60 reglas	On - 242 reglas	On - 31 reglas	On - 9 reglas
Srv14	WebServer	192.XX.XX.XX	RedHat 5.4	AM, WR, FW, IDF, LOG, TM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 22 reglas	On - 161 reglas	On - 30 reglas	On - 6 reglas
Srv15	WebServer	192.XX.XX.XX	Win 2008 R2	AM, WR, FW, IDF, LOG, IM	ON	On – Todo el día, todos los días	On - Default	On - Default	On - Alto	On - 35 reglas	On - 233 reglas	On - 30 reglas	On - 11 reglas

Etapa 5: Pruebas

Durante la etapa de pruebas o verificación del proyecto de implementación de plataforma de seguridad para centros de datos se hace entrega de la siguiente documentación:

- Documento de Pruebas de Funcionalidad.
- Memoria Técnica de instalación de Plataforma.
- Memoria Técnica de instalación de Agentes.

Documento de Pruebas de Funcionalidad

a) Introducción

El área de seguridad de *la Universidad* se encontraba implementando una solución para protección de servidores físicos y/o virtuales, que les proporcione visibilidad y protección de la integridad del sistema operativo, servicios, aplicaciones y datos, por medio de una consola de administración centralizada.

Se realizaron pruebas de funcionalidad para comprobar la convivencia de las distintas aplicaciones que se ejecutan en los servidores con resultados satisfactorios.

En el presente documento se comprueba la correcta funcionalidad de la solución Trend Micro® Deep Security® en los 15 servidores de *la Universidad* destinados a la ejecución de las pruebas con los siguientes equipos con nombres de host:

- Srv01
- Srv02
- Srv03
- Srv04
- Srv05
- Srv06
- Srv07
- Srv08
- Srv09
- Srv10
- Srv11
- Srv12
- Srv13
- Srv14
- Srv15

b) Alcances

Las pruebas de funcionalidad contemplan ser ejecutadas en 15 servidores considerando los siguientes módulos:

- Anti-malware

    - Protección de servidores contra virus, troyanos, spyware y otros tipos de software que tiene la intención de dañar el equipo o realizar operaciones sin su consentimiento.
- Web Reputation
    - Protección contra URL´s maliciosas.
- Firewall
    - Disminuye la superficie de ataque de los servidores físicos y virtuales.
- Log Inspection
    - Análisis de bitácoras.
- Integrity Monitoring
    - Protección de información y archivos de sistema.
- Intrusion Prevention
    - Protección contra vulnerabilidades por medio de parcheo virtual.

De acuerdo a lo anterior, el alcance de la evaluación considera llevar a buen término la siguiente estrategia:

- Ejecución de pruebas de funcionalidad.

Al término de las pruebas de funcionalidad de la solución de seguridad Trend Micro® Deep Security®, *la Universidad* obtuvo visibilidad de los siguientes beneficios:

- Los servidores cuentan con una solución de seguridad que protege contra las diferentes formas en que un activo de información puede ser atacado.
- Una consola de administración centralizada, desde la que se tiene gestión de la seguridad que se aplica a los servidores protegidos.
- Una herramienta que permite tener visibilidad de cambios no programados y/o inesperados que se presenten sobre los servidores protegidos en tiempo real.
- El análisis de los eventos o incidentes de seguridad puede ser realizado desde los diferentes módulos de protección, obteniendo una visión global de lo que sucedió o está sucediendo por medio de la misma herramienta de seguridad.
- Costos y complejidad reducidos debido a que la solución está altamente optimizada para que los servidores reduzcan el impacto operativo con una única plataforma para la gestión de políticas y los controles de seguridad.
- Análisis en tiempo real que permite mitigar los riesgos de seguridad soportados por los módulos habilitados, reduciendo la probabilidad de que sucedan interrupciones en los servicios que ofrecen los servidores.
- Incremento de la productividad y reducción de la carga administrativa para el área de TI.

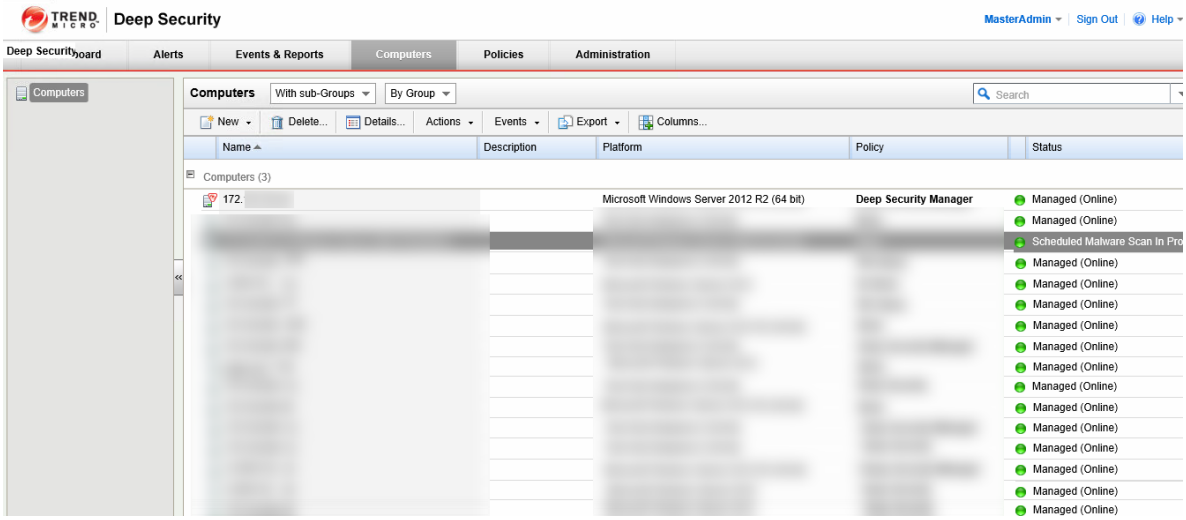
c) Fuera del Alcance

El objetivo de esta sección es dejar claramente establecidas las actividades que no se encuentran comprendidas en esta evaluación.

- No se realizó ningún tipo de cambio en los elementos de red, solo nos enfocamos en la recopilación y análisis de datos.
- Proveer algún componente de SW adicional que no sea requerido para la solución ofrecida.
- Configuración y adecuación adicional a los equipos fuera de los estándares de *la Universidad*.
- La instalación de los Sistemas Operativos tanto del servidor de la consola de administración, así como del servidor de la base de datos fueron responsabilidad de *la Universidad*.
- Respaldos y/o medios de recuperación de las tecnologías a utilizar.
- La capacitación que se proporcionara al personal técnico, no sustituye una certificación ni garantiza un conocimiento completo en la herramienta, por lo que se recomienda tomar los cursos oficiales para tal efecto.
- No se plantea ningún tipo de desarrollo para cumplir normas de estándares de la industria.
- La realización de las actividades de Implementación en una localidad diferente a las instalaciones de *la Universidad* ubicadas en XXXX, D.F., no está contemplada.
- Todo aquello que no sea explícito en este documento no está incluido.

d) Pruebas de funcionalidad

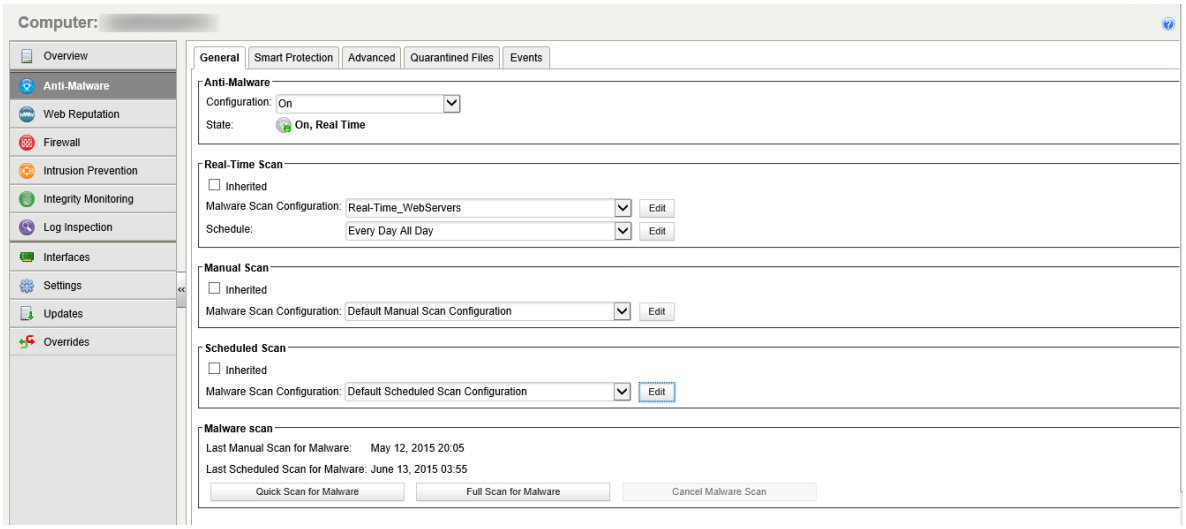
Se realiza la activación de los agentes Deep Security® en los 15 servidores facilitados para la implementación de la solución de seguridad para centros de datos de Trend Micro®.



Nota: debido a que en los 15 servidores se realizaron las mismas pruebas, solamente se mostrarán las del equipo Srv01, ya que el sólo hecho de mostrar los resultados requiere de muchas hojas y en este documento no tiene sentido mostrar la información de los 15 servidores protegidos.

1) Anti-malware

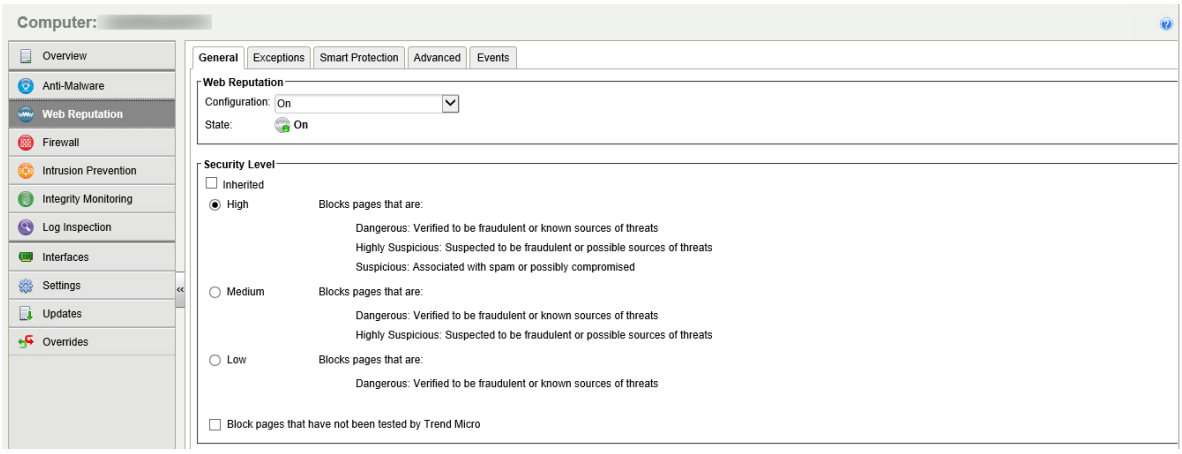
Se activó y se dejó con el escaneo manual y programado con las configuraciones por defecto, para el escaneo en tiempo real se habilitó como todos los días todo el día.



Detecciones del módulo de Anti-Malware: utilizando el archivo de prueba EICAR se comprobó la detección del motor de escaneo de virus de la herramienta.

2) Web Reputation

Se habilitó con un nivel de protección alto y se agregaron excepciones recomendadas por Trend Micro para actualizaciones de Windows, además de algunas URL´s solicitadas por el cliente las cuales son necesarias para que los trabajadores de *la Universidad* puedan desempeñar sus actividades correctamente.

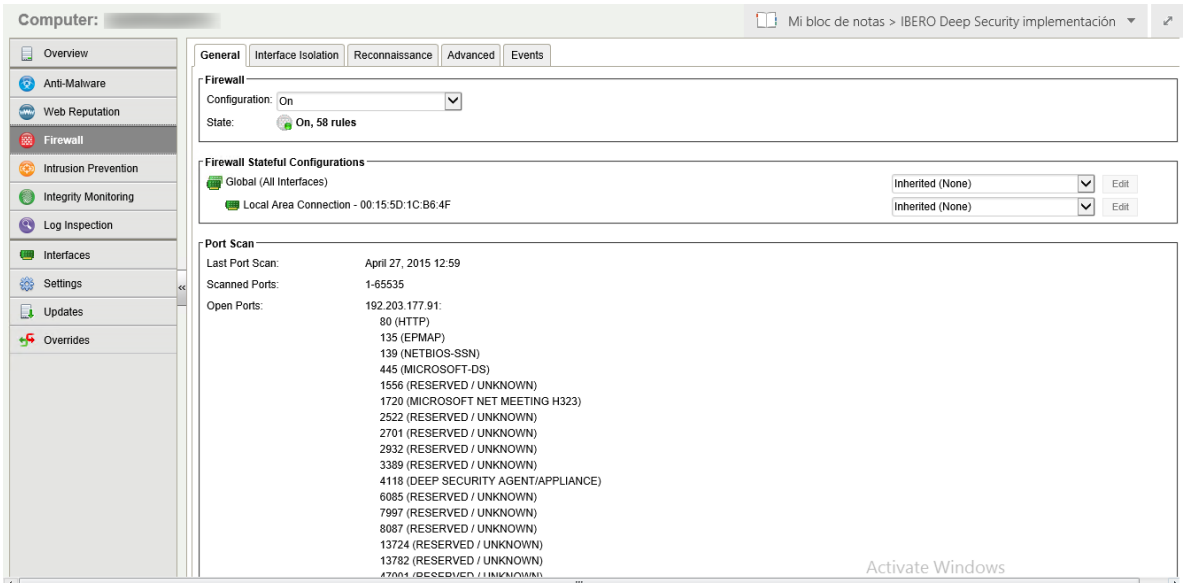


Detecciones del módulo de Web Reputation: se comprobaron las capacidades de detección de URL´s maliciosas con la siguiente URL identificada como maliciosa

www.hothmail.com

3) Firewall

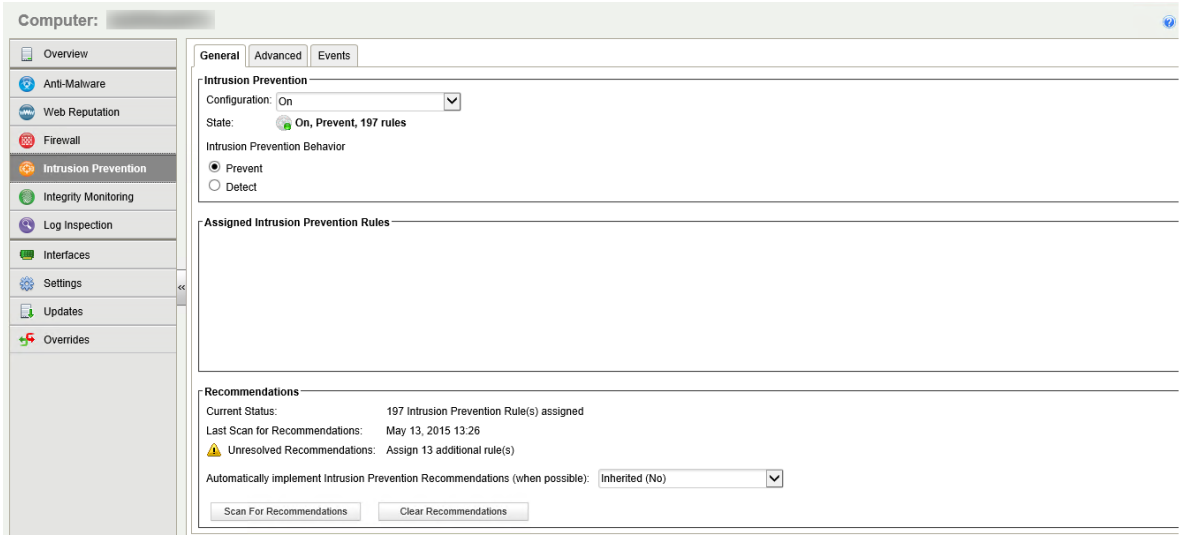
Se realizó el escaneo de puertos abiertos contemplando los 65 535 puertos de red, en los cuales se descubrieron los mismos y se mostraron al personal de *la Universidad*, los cuales nos indicaron las reglas necesarias para que la comunicación sea exitosa y se generaron y aplicaron dichas reglas de comunicación tanto entrante como saliente.



Detecciones del módulo de Firewall: bloqueo de los puertos XX, XX y XXX para los segmentos 172.XX.XX.XX y 172.XX.XX.XX.

4) Intrusion prevention

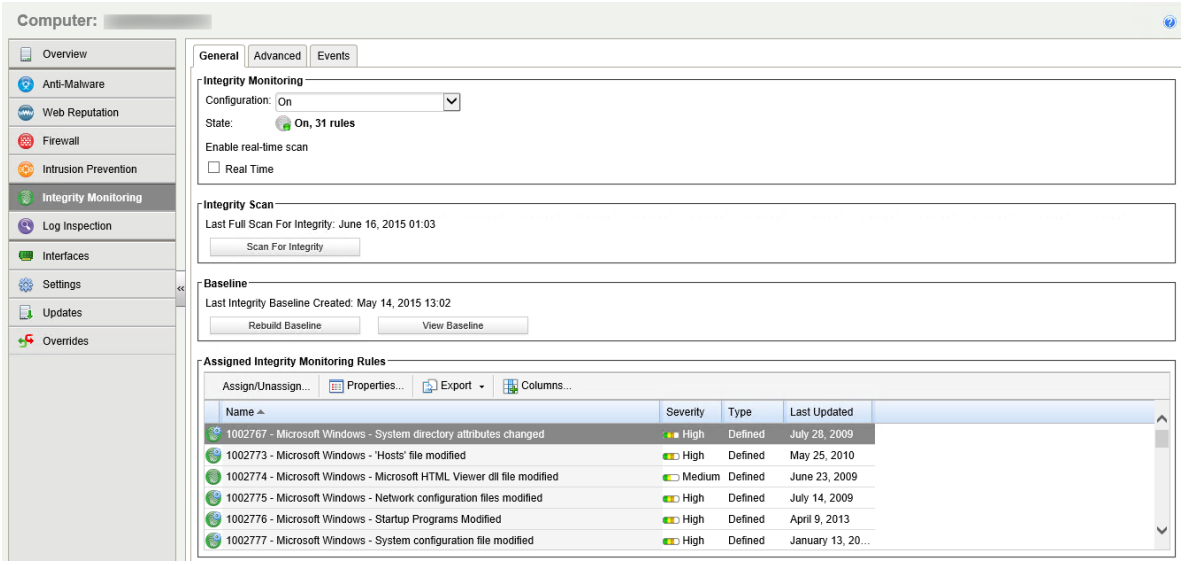
Se realizó un escaneo de recomendaciones encontrando reglas para prevención contra vulnerabilidades (Virtual Patching), se mostraron al personal de *la Universidad* quienes nos ayudaron a validar las reglas se deben de aplicar y se aplicaron las mismas.



Detecciones del módulo de Intrusion Prevention: detección de intentó de explotación de la vulnerabilidad CVE – xxxxxx.

5) Integrity Monitoring

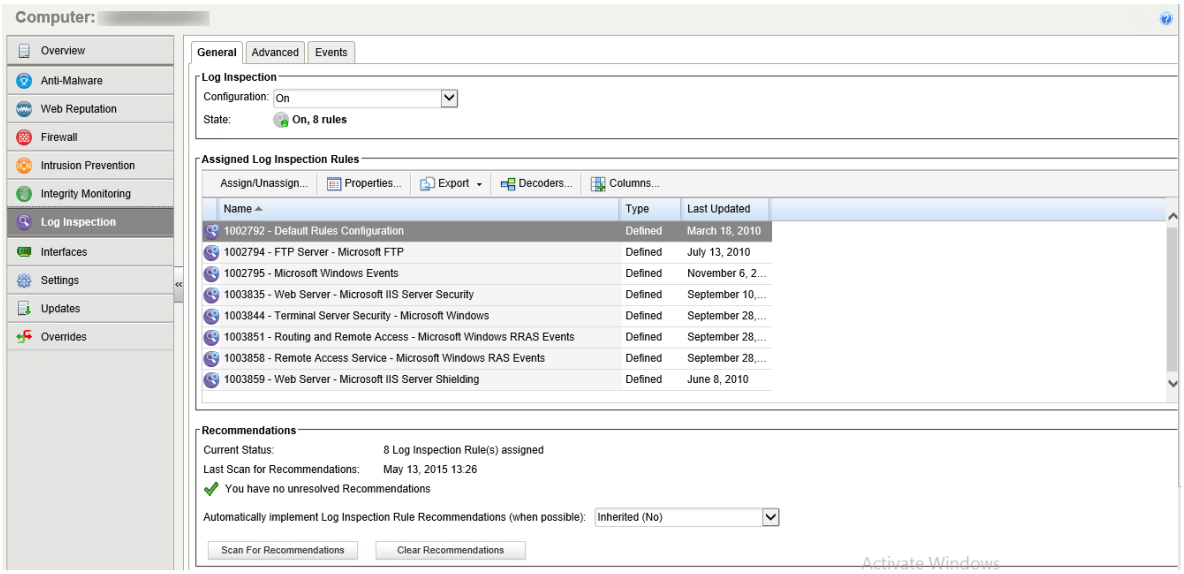
Se habilitó el monitoreo de integridad en tiempo real y se ejecutó un escaneo de integridad en donde se detectó la necesidad de aplicar reglas de protección, se validaron en conjunto con el personal de *la Universidad* y se aplicaron las reglas.



Detecciones del módulo Integrity Monitoring: detección de reinicio y modificación de atributos de servicios.

6) Log Inspection

Se efectuó un escaneo de recomendaciones detectándose reglas para obtener las bitácoras de eventos de acuerdo al tipo de sistema operativo, se validaron en conjunto con el personal de *la Universidad* y se aplicaron las reglas.



Una vez terminada la configuración de los módulos que componen la herramienta Deep Security® y teniendo resultados satisfactorios en las pruebas realizadas, se monitoreó a los servidores protegidos en cuanto a recursos de CPU y memoria RAM obteniendo resultados satisfactorios en la funcionalidad de los 15 servidores protegidos con el agente de Deep Security®.

Conclusiones del proyecto

De acuerdo al alcance planteado por el cliente *la Universidad* en conjunto con OCM–IT® y con base en los procedimientos realizados desde la etapa de planeación hasta la etapa de pruebas, la implementación de la solución de seguridad para centros de datos Trend Micro® Deep Security® se llevó a cabo de manera exitosa, y una vez concluida proporciona el nivel de seguridad adecuado, esperado de acuerdo a los niveles de seguridad requeridos para su infraestructura de red y en particular para el segmento de servidores de su Centro de Datos.

Además de dar mayor protección a los servidores que están expuestos a peticiones provenientes de Internet, con lo que se lograron los objetivos siguientes:

- Evitar mediante el módulo de anti Malware, la infección de software dañino (malware) o la contención del mismo.
- Asegurar la integridad de los archivos mediante la creación de un "base line" que nos permita controlar las modificaciones que pudieran surgir en los servidores.
- Blindar los servidores y aplicaciones en los mismos mediante el uso de parcheo virtual.

Se cumplió con los objetivos planteados al contar con una metodología adecuada que me permitió implementar la solución de seguridad de manera correcta y en tiempo, y a mí me dio la oportunidad de conocer todo el proceso de implementación de una solución de seguridad desde el inicio del proyecto en la etapa de análisis hasta el cierre del mismo, de esta manera, aportando conocimientos a los ya obtenidos anteriormente a lo largo de mi educación profesional dando satisfacción para el cliente, donde fue posible evaluar los controles de seguridad y realizar recomendaciones finales para mejorar ese ambiente de control.

Además me pude dar cuenta de que la Facultad de Ingeniería particularmente en la carrera de Computación se nos prepara de muy buena manera con conocimientos sólidos en las distintas ramas que se compone el área de Computación, permitiéndome de esta manera afrontar y superar los retos que se me han presentado desde el comienzo de mi carrera profesional, por lo cual me siento muy orgulloso de ser egresado de una Universidad tan prestigiosa a nivel nacional e internacional como lo es la Universidad Nacional Autónoma de México.

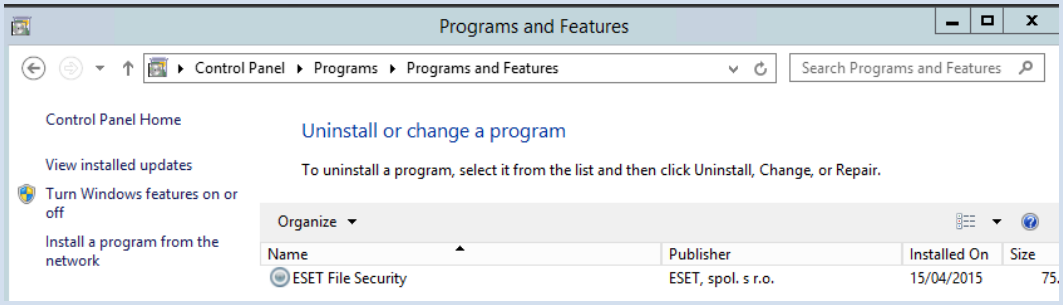
Anexos

Anexo 1. Memorias Técnicas

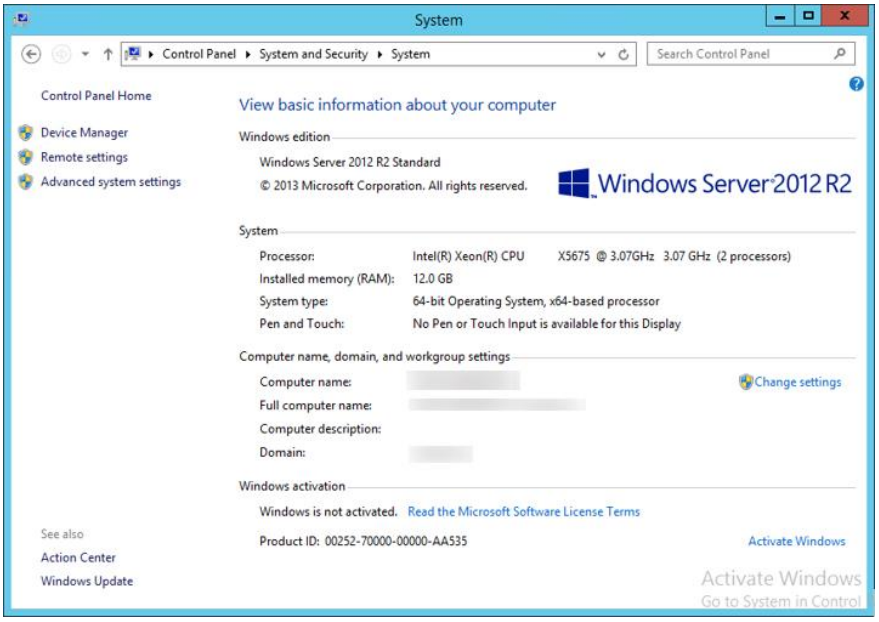
Memoria Técnica de instalación plataforma Trend Micro® Deep Security® 9.5

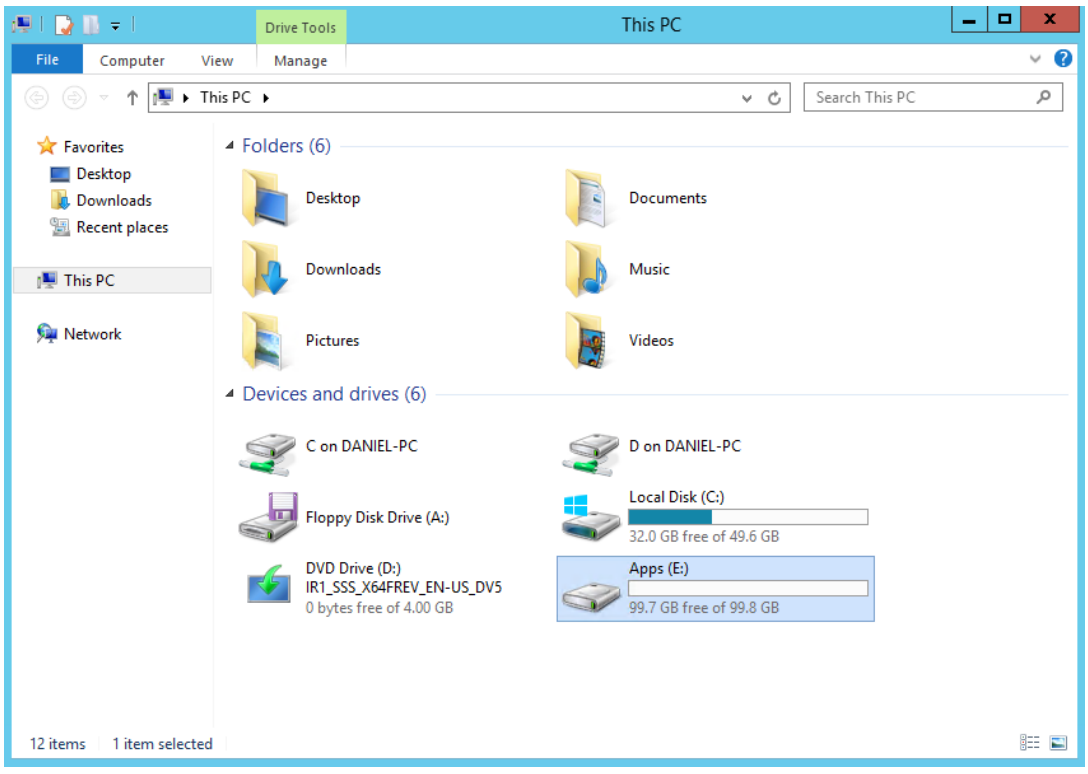
a) Instalación y configuración de equipo para Deep Security® Manager

1. Validar que no se cuenta con alguna herramienta de antivirus, esto lo podemos hacer dirigiéndonos a Panel de Control > Programas > Programas y Características > Desinstalar Programas. En caso de que no se cuente con ninguna herramienta de antivirus pasar al Paso En caso contrario, desinstalar la herramienta de antivirus manualmente.

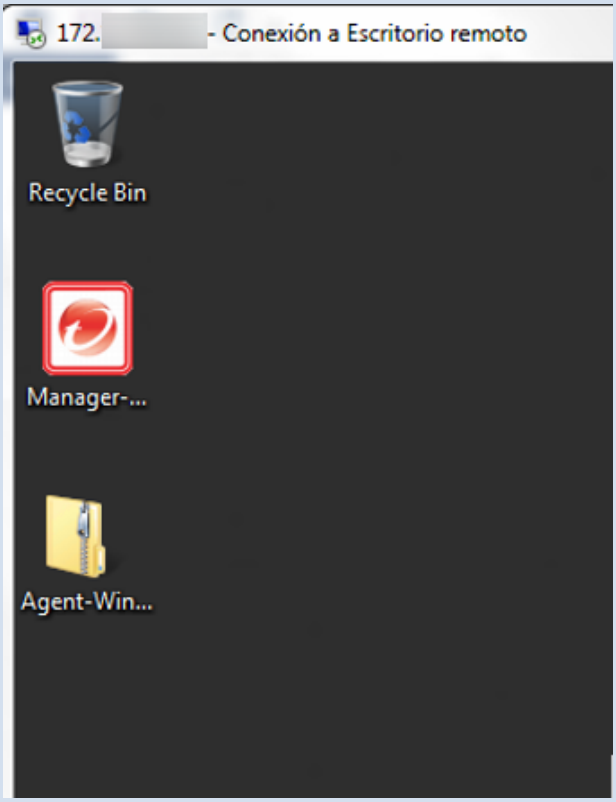


2. Confirmar que el servidor 172.XX.XX.XX cuente con los requerimientos necesarios tanto de sistema, como de espacio en disco para la instalación del programa Deep Security Manager.

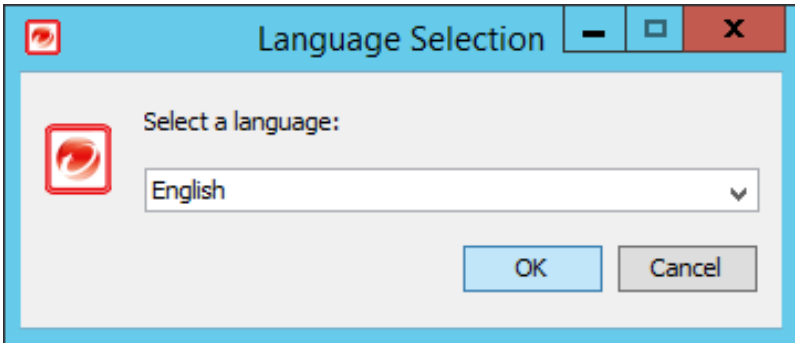




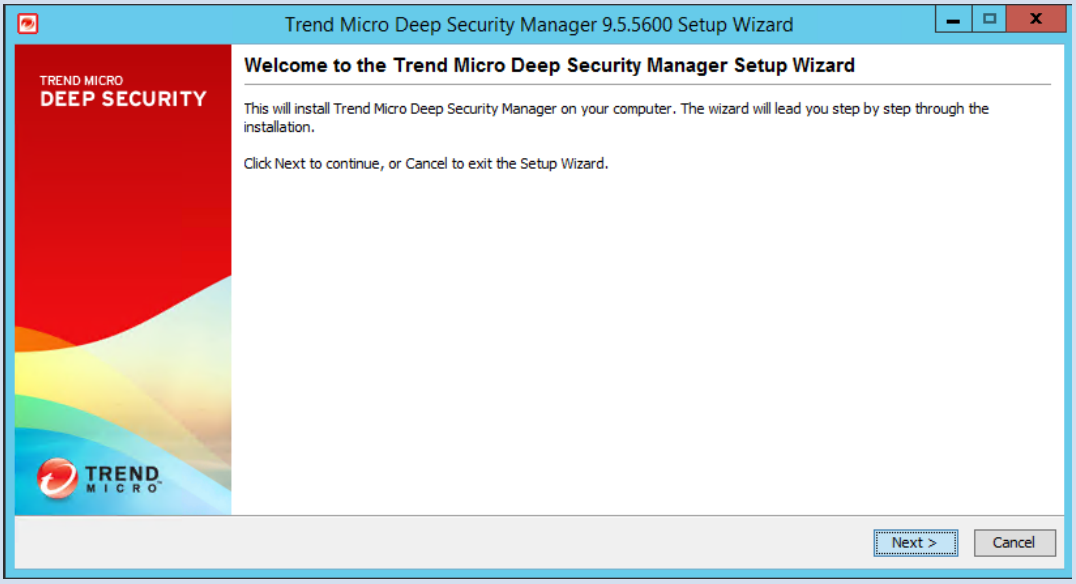
3. Copiar el paquete de instalación de Deep Security Manager® al equipo destino. En nuestro caso es el equipo con Hostname SrvDeepSec:



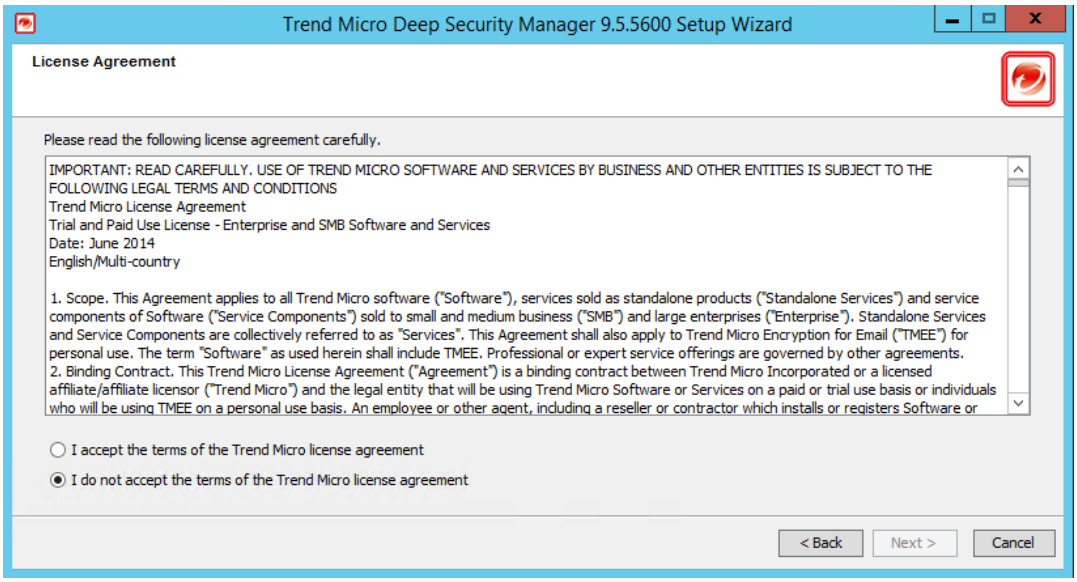
4. Iniciar el paquete de instalación de Deep Security Manager® dándole doble clic. A continuación seleccionar el lenguaje de instalación y darle clic en **OK**:



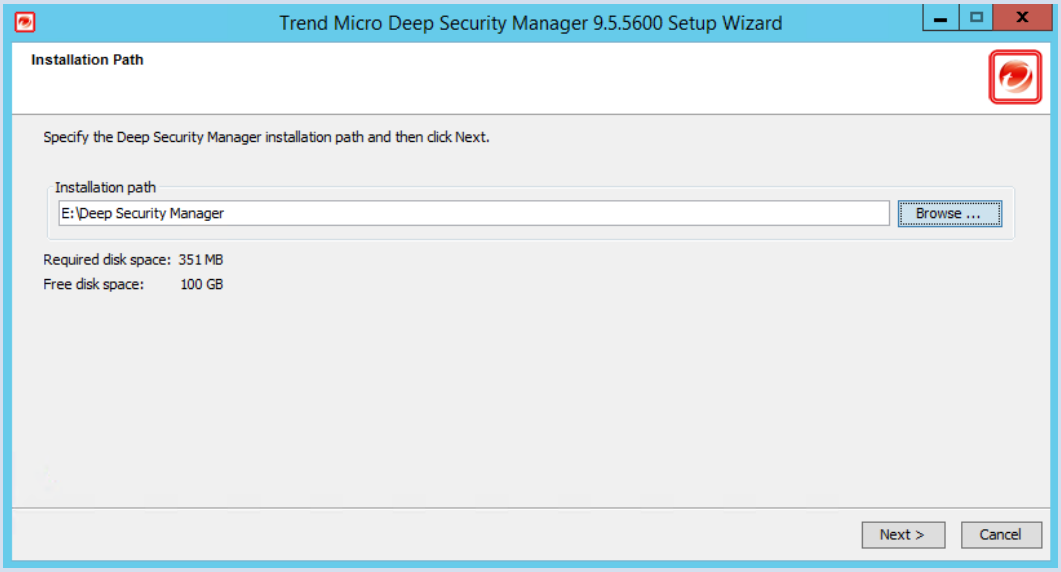
5. A continuación se nos presentará una pantalla en donde se nos menciona que el wizard de instalación nos ayudará paso a paso en la instalación, para continuar damos clic en **Next**:



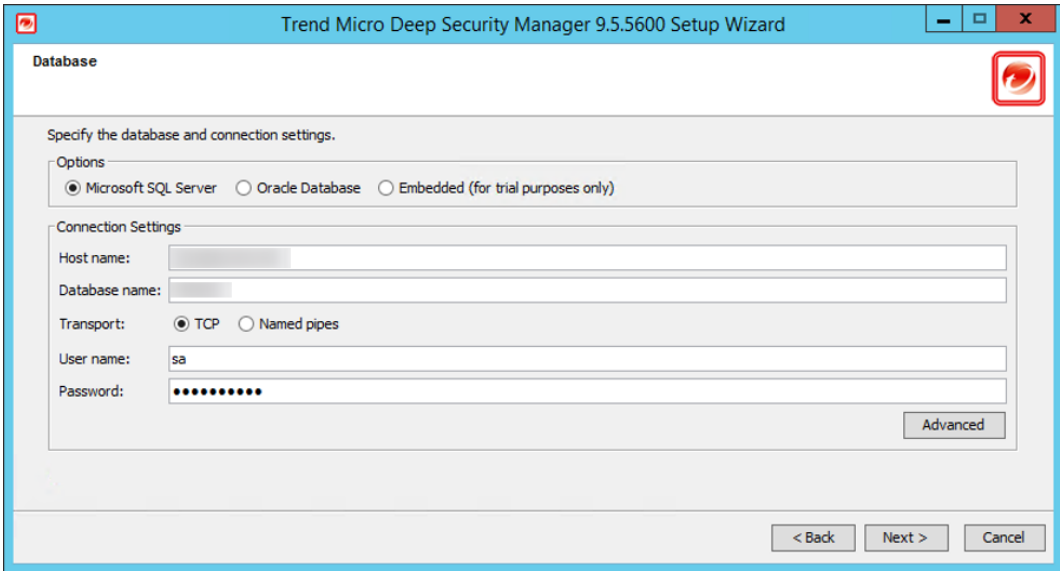
6. Acuerdo De Licencia: Si está de acuerdo con los términos del contrato de licencia, seleccione **I accept de agreement** y haga clic en **Next**:



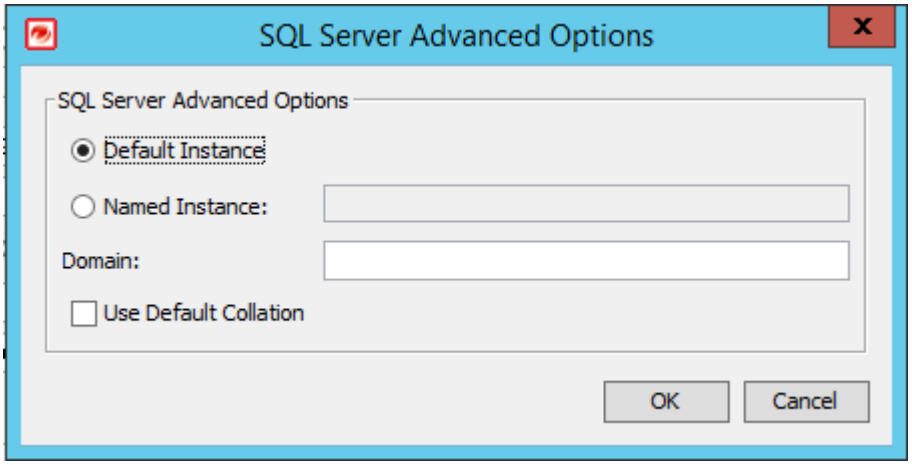
7. Ruta de instalación: Especifique la carpeta donde desea que se instale Deep Security Manager® y haga clic en **Next**:



8. Base de Datos: Especifique el tipo de base de datos que desea utilizar (instalada previamente).

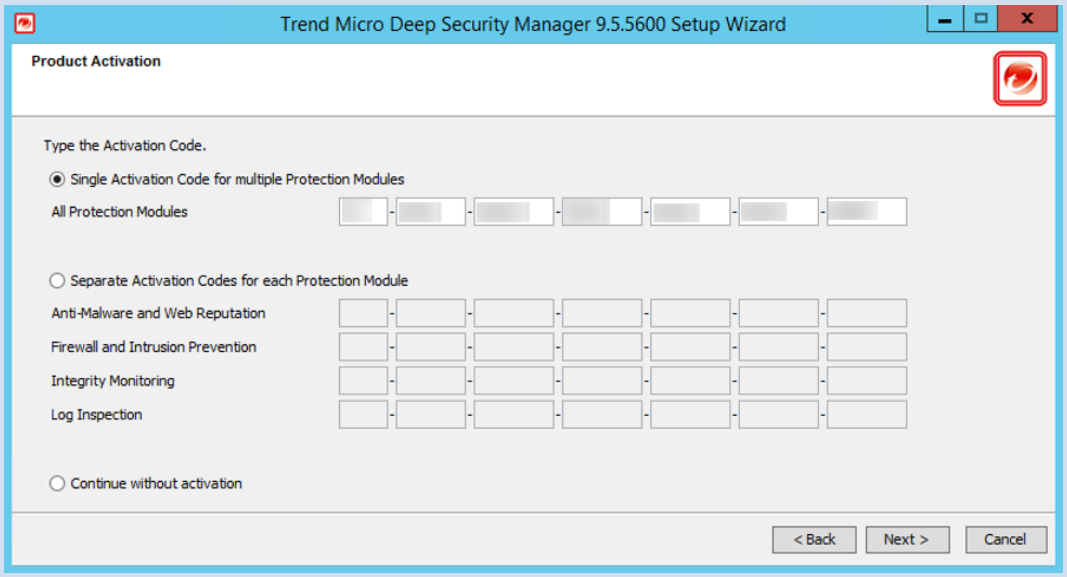


Agregamos la información necesaria:
Hostname: SQLDB
Database name: DSXXXX
Transport: TCP
User name: sa
Password: XXXXXXX

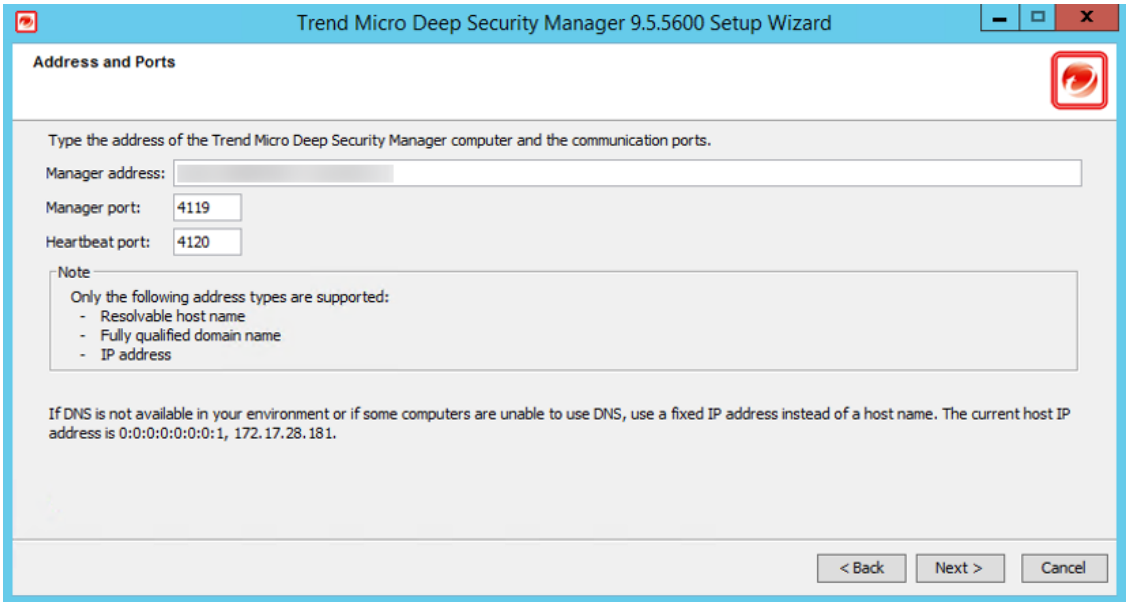


Dando clic en **Advanced** podemos seleccionar si queremos la instancia por default o alguna en específico en este caso dejamos por default, y dejamos sin seleccionar el checkbox de **Coallition**.

9. Activación del Producto: Ingrese su código(s) de activación. Introduzca el código para todos los módulos de Protección o los códigos de los módulos individuales para las que usted ha adquirido una licencia:

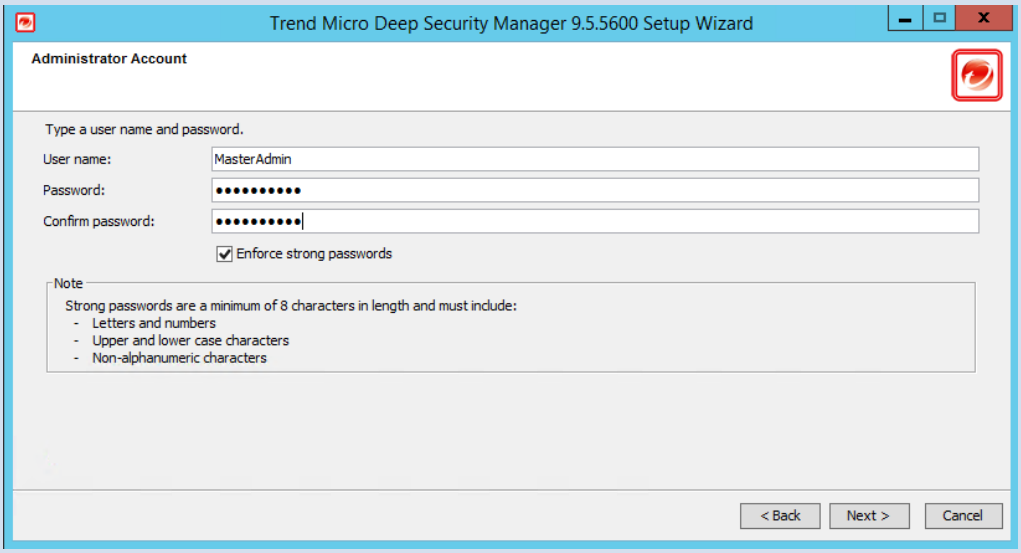


10. Dirección y Puertos: Ingrese un hostname, URL, o dirección IP de la computadora de Deep Security Manager. La dirección del Manager debe de ser ya sea, un hostname, FQDN o dirección IP que puedan resolver los agentes. El “Management Port” es el puerto en el cual la consola de administración web es accesible a través de HTTPS. El "Heartbeat Port" es el puerto por el cual el Manager escucha la comunicación proveniente de los agentes/appliances.

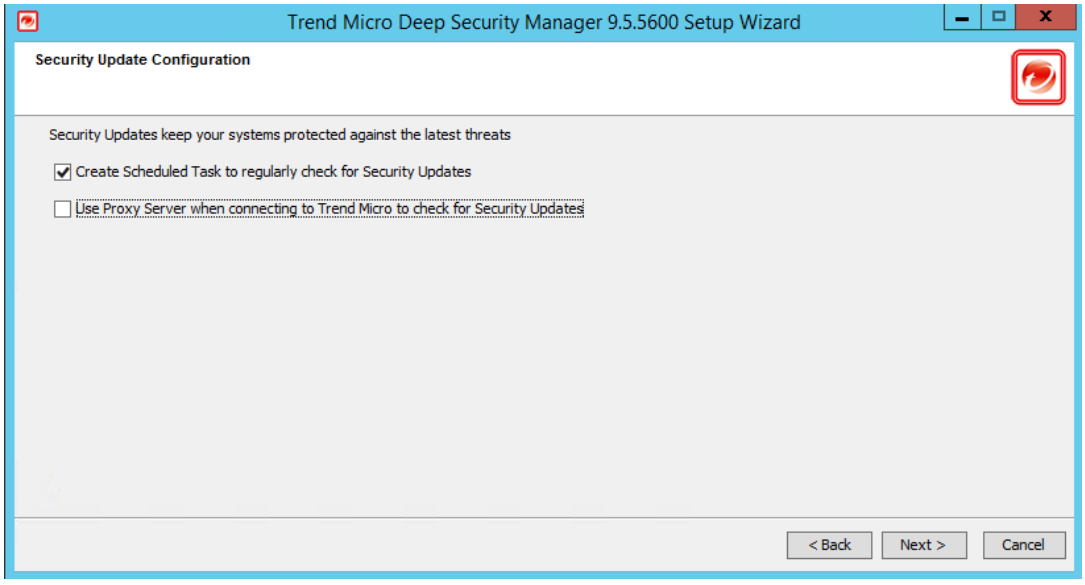


11. Cuenta de administrador: Introduzca un nombre de usuario y una contraseña para la cuenta de administrador principal. Seleccionando **Enforce strong passwords** (recomendado) exige que las contraseñas sean fuertes y deberán de incluir letras mayúsculas y minúsculas, caracteres no alfanuméricos, y los números, y exigir un mínimo de 8 caracteres. Haga clic en Next:

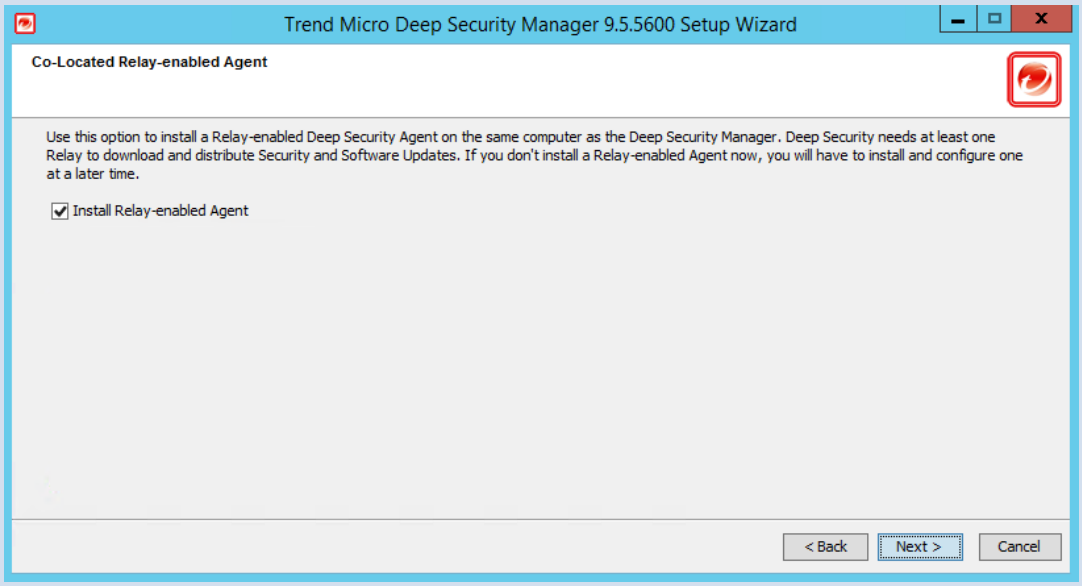
    User name: MasterAdmin
    Password: XXXXXX



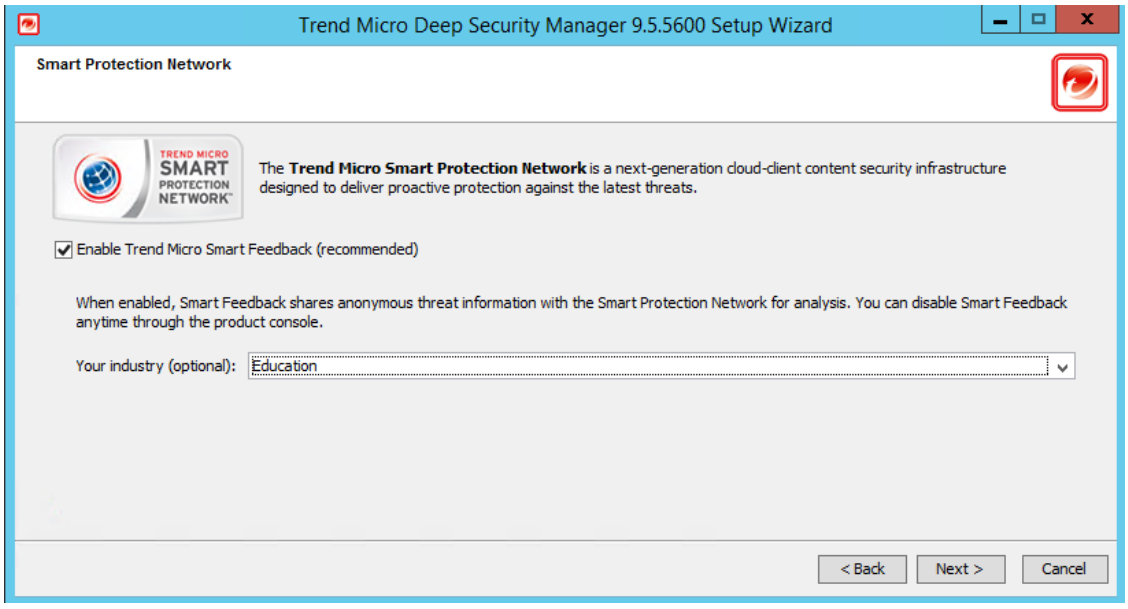
12. Configuración de actualizaciones de Software: Seleccione **Automatically Update Components**, sí se selecciona, Deep Security Manager recuperará automáticamente los últimos Componentes o detectará el nuevo software. En este caso no se cuenta con Proxy por lo que no seleccionamos la casilla de Use Proxy Server when connecting to Trend Micro to Security Updates Haga clic en **Next**.



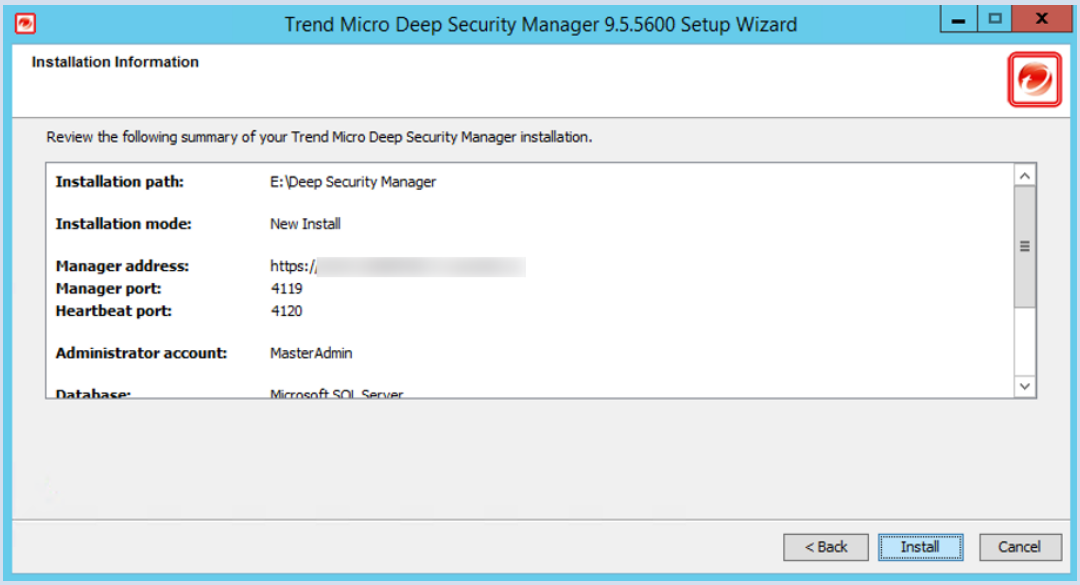
13. Agente de retransmisión: Seleccione si desea instalar Deep Security Relay® en el mismo equipo. (Si usted no tiene el paquete de instalación de Deep Security Relay® en la misma ubicación que el instalador de Deep Security se omitirá este paso). Seleccione **Install Relay – enabled agent**, dar clic en **Next**:



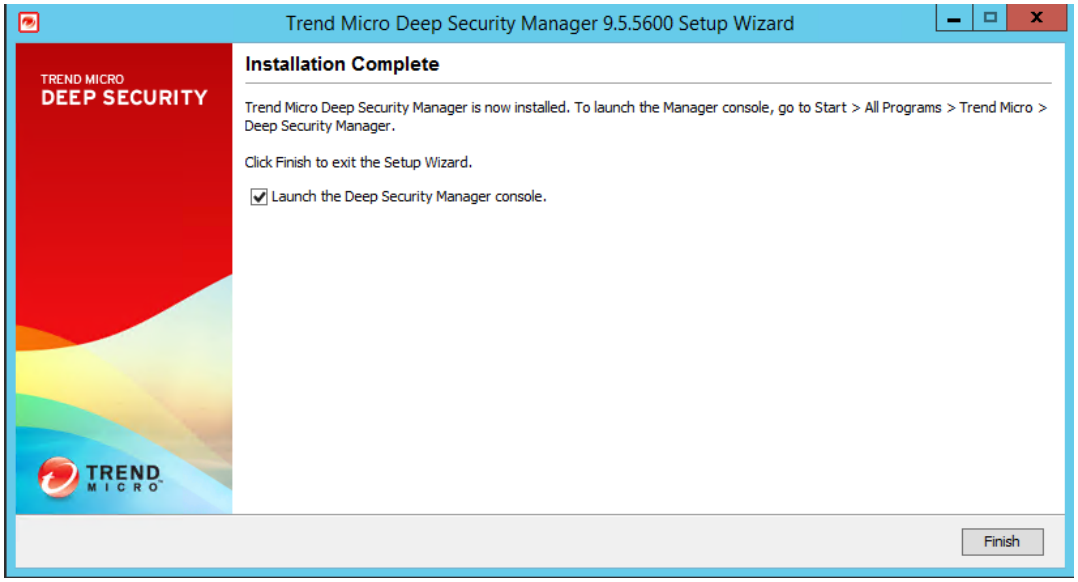
14. Smart Protection Network: Seleccione la casilla de **Enable Trend Micro Smart Feedback** para subir información a la nube de Trend Micro. Además ingrese su industria mediante la selección de la lista desplegable en este caso seleccionamos **Education**. Haga clic en **Next**:



15. Información de Instalación. Verifique la información que ha introducido sea correcta, sí no lo es de clic en Back hasta la pestaña que necesita modificar; sí es correcta haga clic en **Install** para continuar con la instalación de la herramienta:



16. Haga clic en **Finish** para cerrar el asistente de instalación.

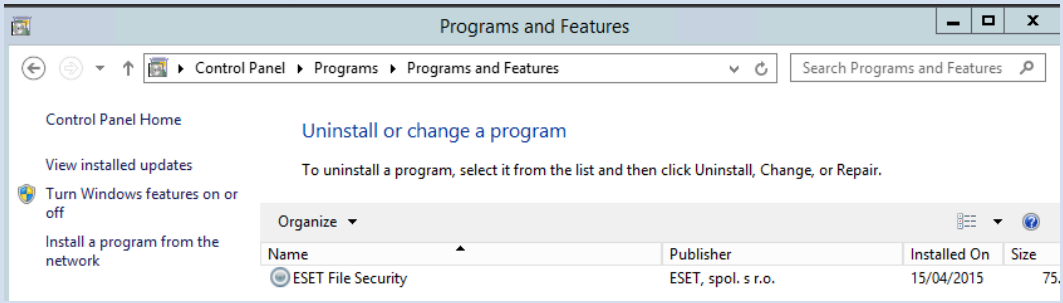


17. Se ha completado correctamente la instalación de Trend Micro® Deep Security Manager®.

Memoria de instalación Trend Micro® Deep Security Agent 9.5

a) Instalación del agente de antivirus en equipos Windows

1. Validar que no se cuenta con alguna herramienta de antivirus, esto lo podemos hacer dirigiéndonos a Panel de Control > Programas > Programas y Características > Desinstalar Programas. En caso de que no se cuente con ninguna herramienta de antivirus pasar al Paso En caso contrario, desinstalar la herramienta de antivirus manualmente.



2. Confirmar que el servidor a proteger cuente con los requerimientos necesarios tanto de sistema, como de espacio en disco para la instalación del programa Deep Security Agents.

View basic information about your computer

Windows edition

Windows Server 2008 R2 Enterprise

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

Processor: Intel(R) Xeon(R) CPU X5675 @ 3.07GHz 3.06 GHz

Installed memory (RAM): 6.00 GB

System type: 64-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:

Full computer name:

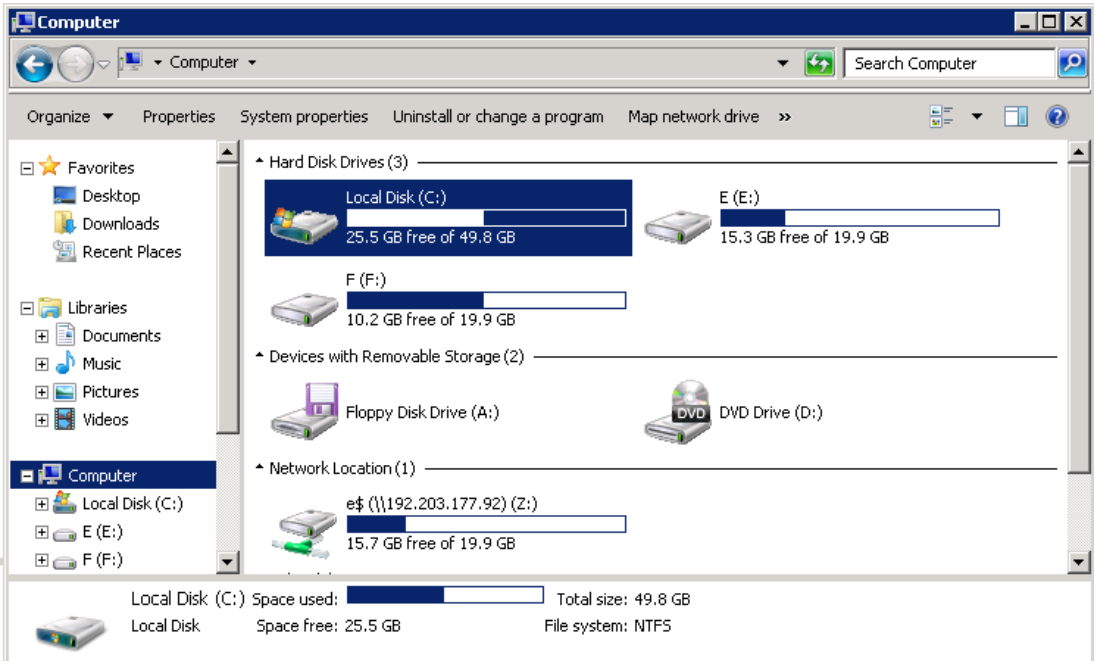
Computer description:

Domain:

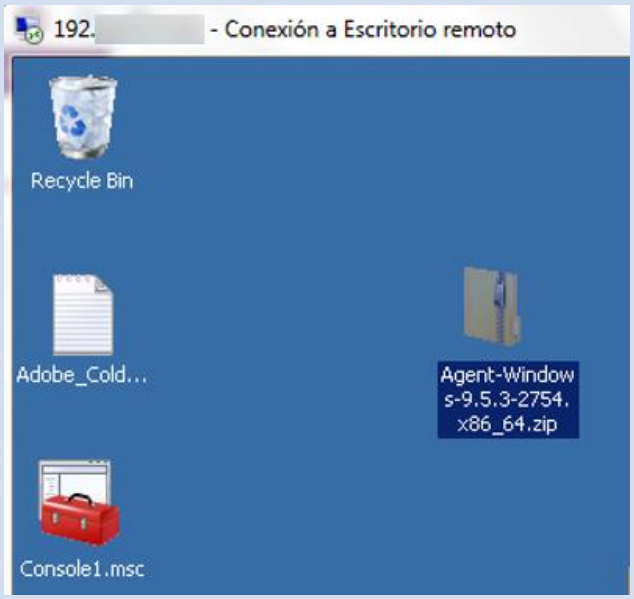
Windows activation

Windows is activated

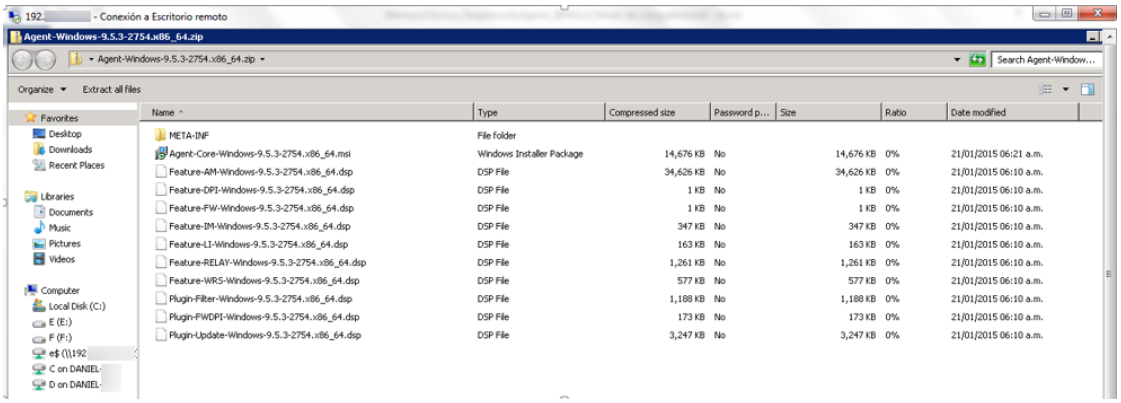
Product ID: 55041-262-0680331-84928 Change product key



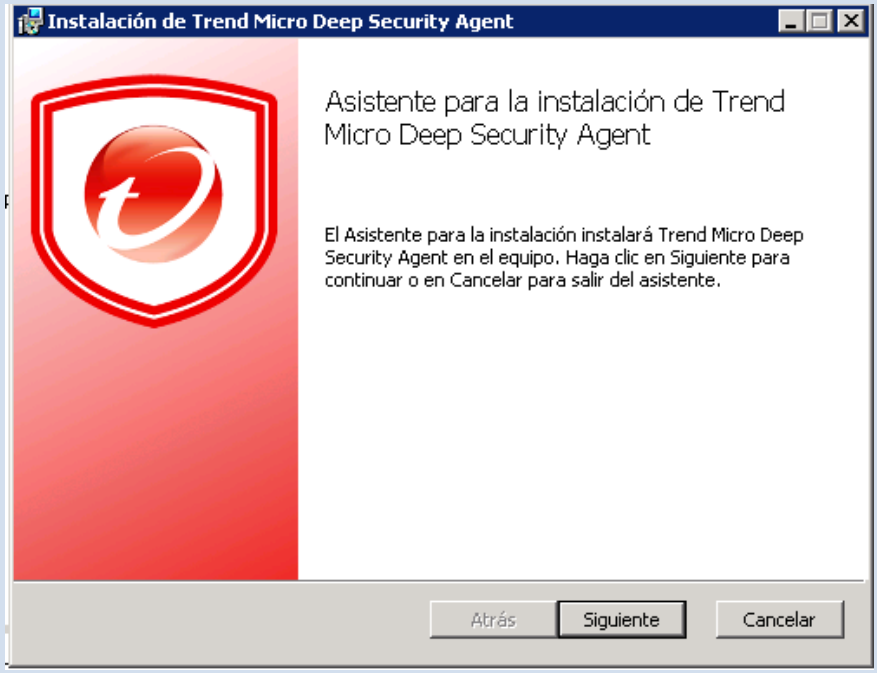
3. Copie el archivo de instalación en el equipo de destino:



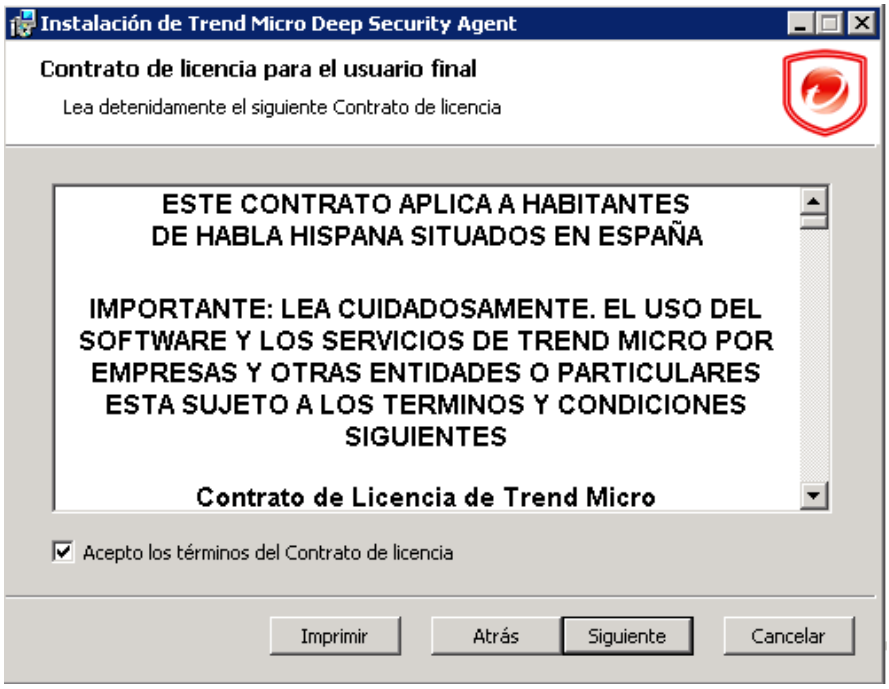
4. Haga doble clic en el archivo comprimido para abrirlo y de doble clic en el paquete de instalación del agente para ejecutarlo:



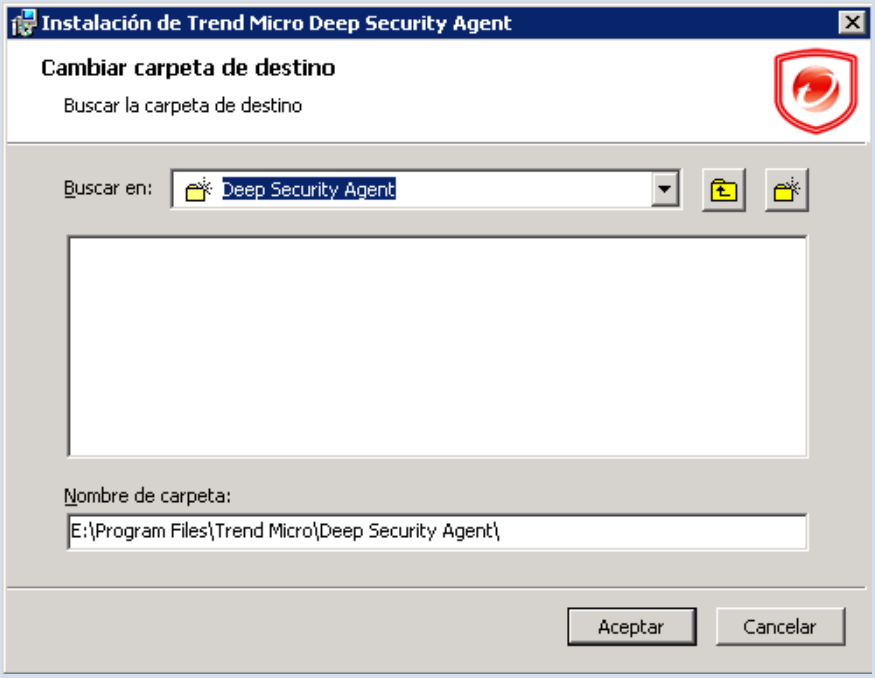
5. En la ventana de bienvenida haga clic en **Siguiente** para continuar con la instalación:



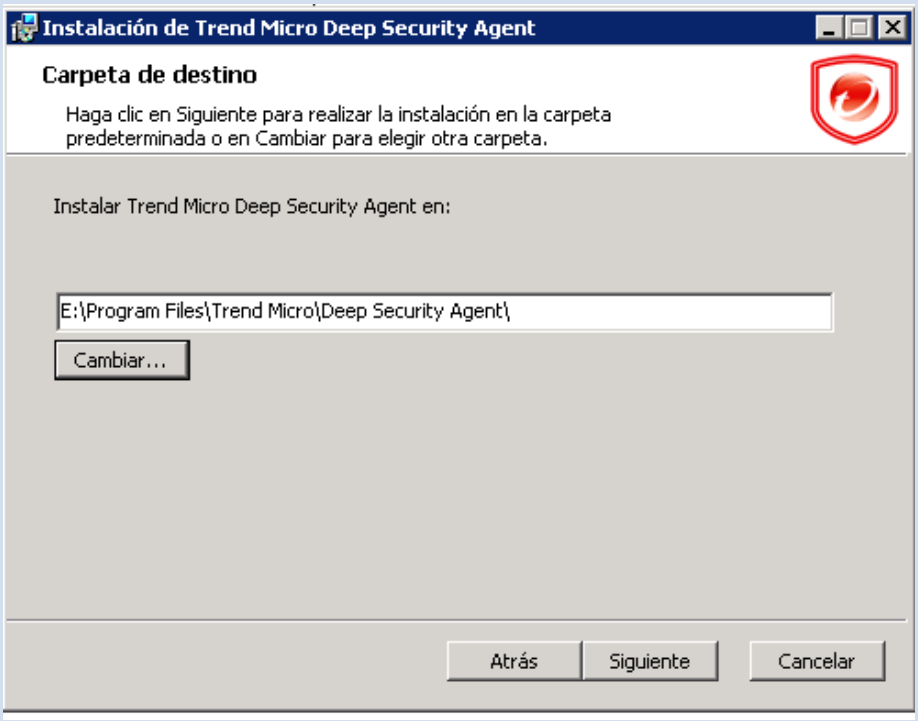
6. Contrato de licencia para el usuario final: Lea el contrato de licencia, si usted está de acuerdo seleccione el checkbox de **I accept the terms of the license Agreement** y de clic en **Siguiente** para continuar:



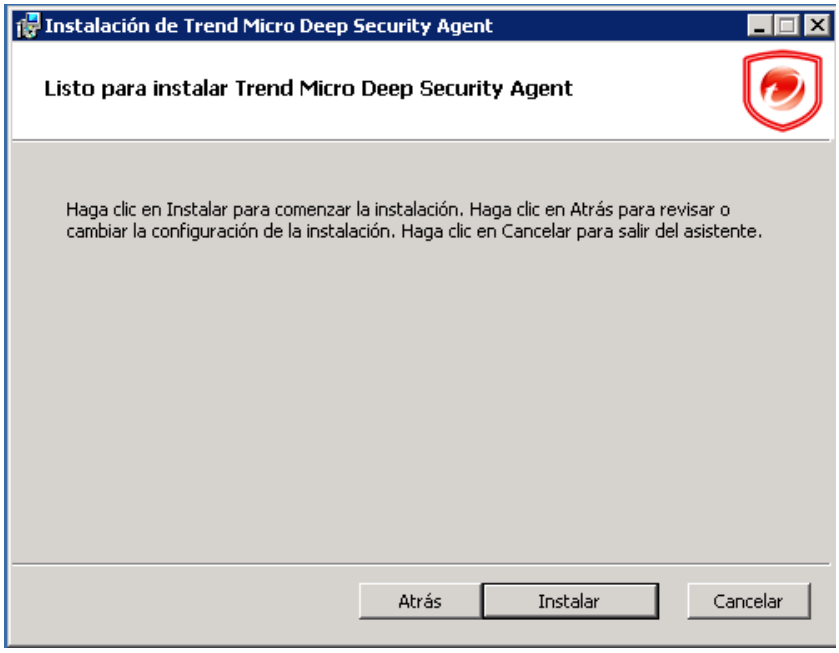
7. Ruta de instalación Carpeta de destino: Seleccione la unidad en la cual desea que se instale el agente de antivirus de Deep Security.



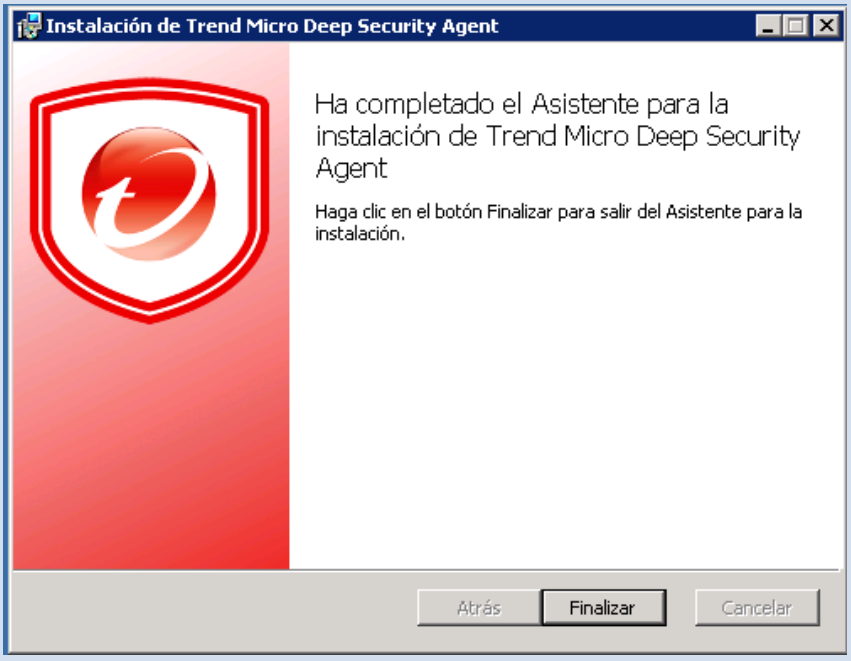
Una vez que selecciono la unidad y carpeta de destino deseadas de clic en **Siguiente** para continuar.



8. Listo para instalar el agente de Trend Micro® Deep Security®: De clic en **Instalar** para proceder con la instalación del agente.



9. Completado: Cuando la instalación ha terminado correctamente de clic en **Finalizar**.



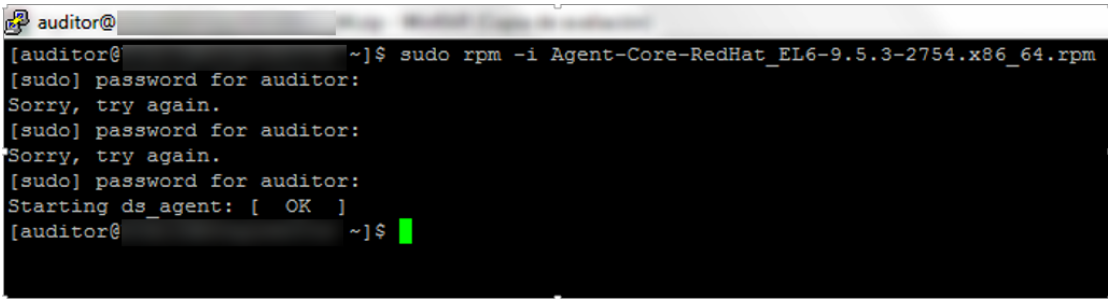
10. Se ha completado la instalación de manera correcta la instalación de Deep Security Agent.

b) Instalación del agente de antivirus Deep Security® en equipos Linux

1. Validar que no se cuenta con alguna herramienta de antivirus. En caso de que no se cuente con ninguna herramienta de antivirus pasar al Paso 2. En caso contrario, desinstalar la herramienta de antivirus manualmente.
2. Copie el archivo de instalación en el equipo de destino.
3. Posicione el archivo en la unidad en la cual desea instalar y colóquese en esa carpeta.
4. Ejecute el siguiente comando:

   # rpm -i <package name>

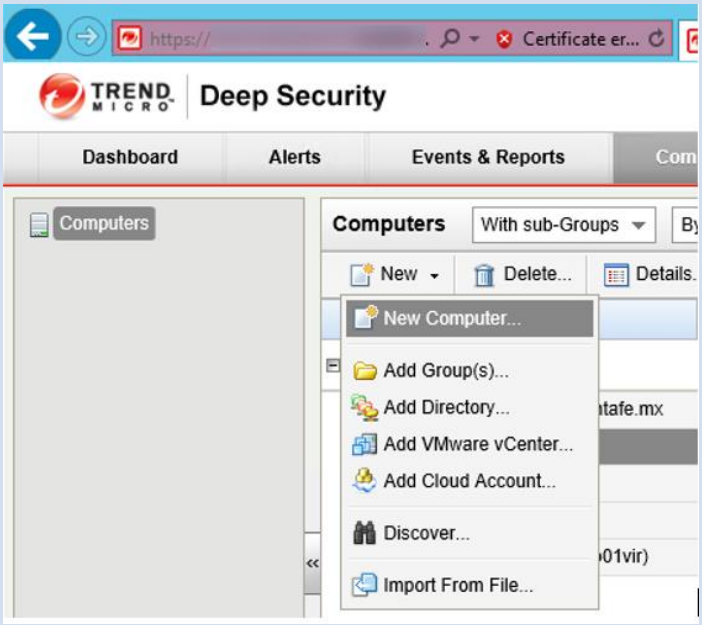
   Donde package name es el nombre del paquete de descargar de acuerdo a la versión y velocidad del Sistema operativo.



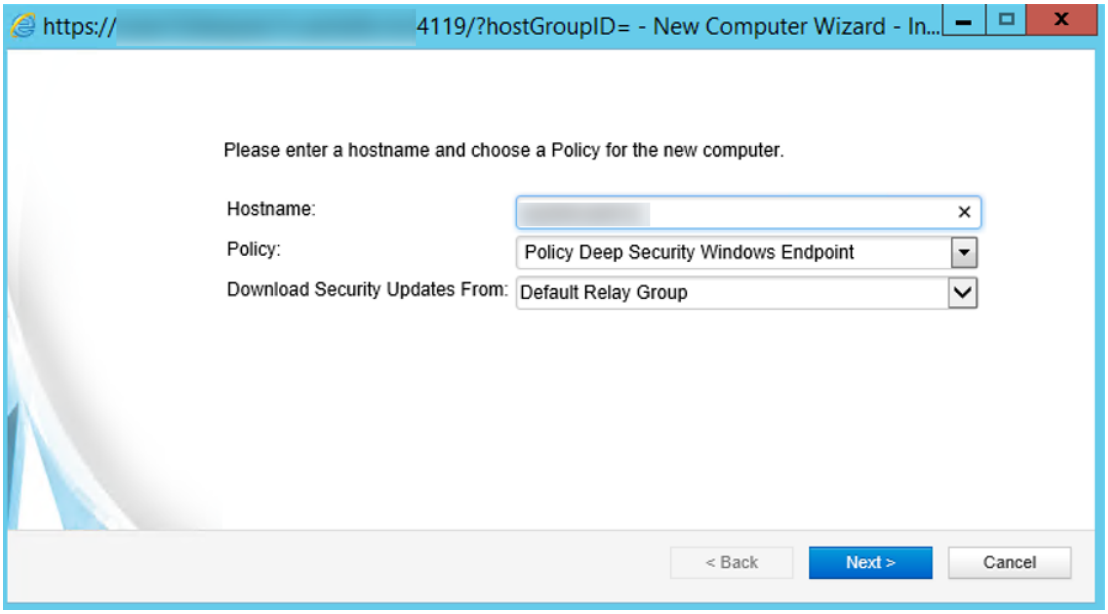
5. El agente de Deep Security® se iniciará después de terminar de manera correcta la instalación.
6. Se ha completado la instalación de manera correcta la instalación de Deep Security Agent.

c) Agregar agentes a la consola de administración Web

1. En la consola de Deep Security Manager®, diríjase a la pestaña de **Computers** y de clic en **New** en la barra de herramientas y seleccione **New Computer** en el menú desplegable:

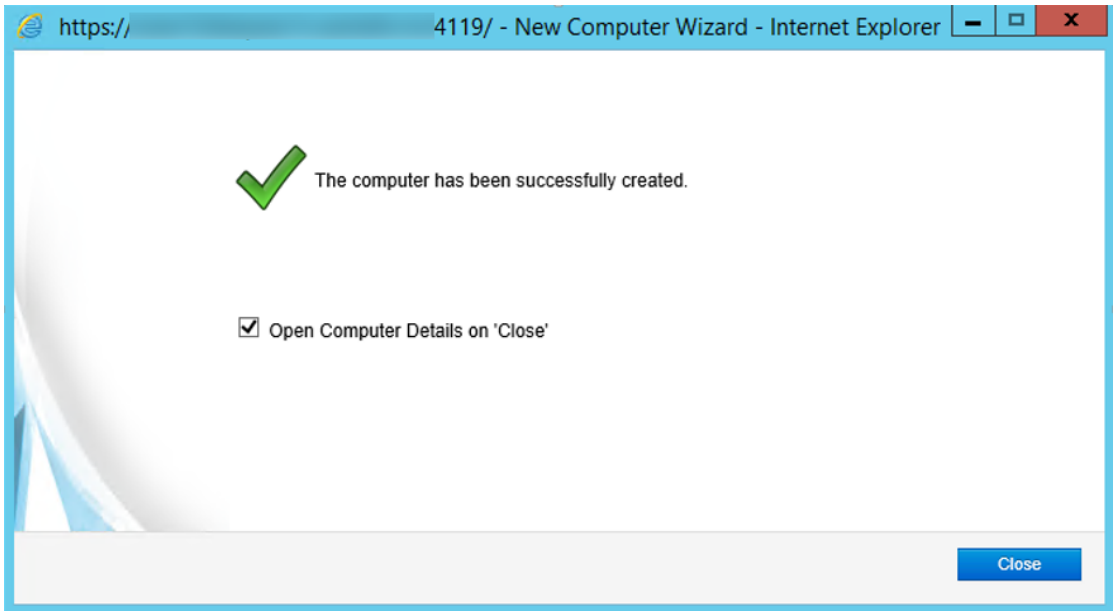


2. En el asistente de **New Computer**, ingrese un hostname o dirección IP del servidor que desea agregar y seleccione la política de Seguridad que aplique a ese servidor del árbol de políticas en el menú desplegable.



3. El asistente contactará al equipo de cómputo, lo agregará a la pestaña de Computers, detectará el agente inactivo, lo activará y aplicará la política seleccionada, de clic en **Finish.**

4. Cuando el equipo de cómputo se haya agregado el asistente desplegará un mensaje de confirmación.



5. Seleccione la casilla de **Open Computer Details on 'Close'** para ver información relacionada a la configuración del equipo y de clic en **Close**.

Glosario

A

Ambientes físicos: son infraestructuras de cómputo en las cuales únicamente se emplean equipos de cómputo final y servidores de tipo físicos.

Ambientes virtuales: son infraestructuras de cómputo en las cuales únicamente se emplean equipos de cómputo final y servidores de tipo virtuales.

Amenazas avanzadas persistentes: están diseñadas para atacar a un objetivo específico, aprovechando cualquier medio que le permita ganar acceso a una organización y mantiene oculto el ataque.

Anti-malware: también conocido como anti-virus es un tipo de programa diseñado para prevenir, detectar y remediar software malicioso (malware) en los equipos de cómputo comprometidos.

Ataques dirigidos: son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas. No son ataques masivos, porque su objetivo no es alcanzar al mayor número posible de equipos de cómputo. Su peligro radica precisamente en que son ataques personalizados, diseñados especialmente para engañar a las potenciales víctimas.

B

Baseline: es una especificación que se ha revisado formalmente desde la cual de ahí en adelante servirá como base para un desarrollo posterior que puede cambiarse solamente a través de procedimientos formales de control de cambios.

Botnet: también conocidos como equipos zombies son equipos de cómputo los cuales han sido infectados con código malicioso sin el conocimiento de los usuarios y que son manipuladas para realizar distintas actividades como ataques DDoS, enviar programas maliciosos como spyware y SPAM.

BuróMC: es una Empresa especializada en el diseño e implementación de soluciones integrales de seguridad informática para el perímetro, backbone y endpoint, apoyándose en tecnología y métodos de vanguardia.

BYOD: de las siglas en inglés Bring Your Own Device es una política empresarial que consiste en que los empleados lleven sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa como correo electrónico, bases de datos, aplicaciones, entre otros más.

C

Centro de datos: se denomina centro de datos a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Control Manager®: es una plataforma que nos permite gestión centralizada para detección de amenazas y protección de datos centrada en el usuario, la cual nos permite conectar diferentes productos Trend Micro® para de manera centralizada observar todas las consolas de administración y de esta manera nos ofrece visibilidad centralizada y defensa conectada frente a amenazas.

Consultor de Seguridad: es una persona que aconseja o da su opinión sobre un tema general o específico dentro de su especialidad, es decir, tiene como función asesorar a la empresa sobre políticas de seguridad y los sistemas más adecuados para su infraestructura de red.

D

Deep Security®: es un dispositivo de Seguridad el cual provee Seguridad avanzada para servidores físicos, virtuales y en la nube. Protege aplicaciones empresariales y datos de brechas y disrupciones de negocios sin la necesidad de aplicar parches de emergencia.

Deep Discovery Inspector®: es una solución de gestión de amenazas de tercera generación, está diseñado para detectar amenazas persistentes avanzadas y dar visibilidad de ataques dirigidos, así como también brindar percepción y control de la red informática.

F

Firewall: es un dispositivo de red el cual se utiliza para bloquear el acceso no autorizado a direcciones IP o URL´s, permitiendo de la misma manera comunicaciones autorizadas, los firewall pueden estar implementados ya sea como hardware o software.

G

Gusanos: también conocidos como gusanos informáticos son programas autónomos capaces de propagar copias funcionales de sí mismo a otros sistemas informáticos.

I

IDS: de las siglas en inglés Intrusion Defense System es un programa de detección de accesos no autorizados a un equipo de cómputo o una red informática.

IPS: de las siglas en inglés Intrusion Prevent System es un software que ejerce control de acceso en una red informática para proteger a los sistemas de cómputo de ataques provenientes del exterior.

M

Malware: es un programa que realiza actividades maliciosas como propagación, destrucción, comportamiento no autorizado o inesperado, control remoto, robo de información, engaño, entre otros más; están diseñados para infiltrar o dañar una computadora sin consentimiento del usuario.

N

Nube: también conocido como computación en la nube o informática en la nube es un paradigma que permite ofrecer servicios de computación a través de Internet.

O

OCM-IT Seguridad en Virtualización: es una consultoría de cómputo dedica a proveer soluciones tecnológicas a la medida de cualquier tipo de negocio entre las que se encuentran virtualización, seguridad informática e infraestructura tecnológica.

R

Ransomware: es un tipo de malware que impide o limita a los usuarios a que accedan a su equipo de cómputo mediante algoritmos de cifrado ya sea cifrando por completo el equipo de cómputo o en algunos casos cifrando archivos, para después obligar a sus víctimas a pagar rescate a través de ciertos métodos de pago en línea.

RFP: de las siglas en inglés Request For Proposal es un documento que tiene como solicitud una propuesta a determinados requerimientos de una organización, es decir, es un documento que una empresa emite para solicitar propuestas de posibles proveedores de productos o servicios.

P

Parcheo virtual: es el desarrollo a corto plazo de la rápida implementación de una política de seguridad destinada a evitar una explotación que se produzca como resultado de una vulnerabilidad descubierta recientemente, es decir, es un trabajo de reparación rápido para un pedazo de programa o sistema operativo.

Plan de seguridad: es un plan formal que define el método de acción para asegurar información o un sistema informático. Proporciona un enfoque sistemático y técnicas para proteger un equipo de ser utilizado por usuarios no autorizados, protege contra malware, así como cualquier incidencia que pueda poner en peligro la seguridad del sistema informático.

S

Servidores: en Internet es un equipo de cómputo que provee los datos solicitados por parte de los navegadores de otras computadoras. En redes locales se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos, como por ejemplo, los servidores que almacenan información en forma de páginas web y a través del protocolo HTTP lo entregan a petición de los clientes (navegadores web) en formato HTML. El término servidor también se utiliza hoy en día para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Servidores de C&C: son máquinas centralizadas las cuales son capaces de enviar comandos y recibir datos provenientes de máquinas Botnet, así como también controlar a los equipos Zombie mediante el envío de comandos para que realicen alguna actividad en específico como ataques de tipo DDoS.

Servidores físicos: es un servidor que podemos “verlo y tocarlo”. Se trata de una configuración de hardware y software concreta, además de otras especificaciones como RAM y memoria en disco.

Servidores virtuales: se trata de una instalación de software realizada sobre un servidor físico; este servidor físico puede alojar diferentes virtuales que comparten entre sí el hardware y los recursos, pero su funcionamiento es completamente independiente. Los servidores virtuales

permiten ahorrar en costes si necesitamos varios servidores, ya que podemos tener varios virtuales dentro de uno físico.

Spyware: o programa espía es un malware que recopila información de equipos de cómputo comprometidos y después transmite la esa información a una entidad externa sin el conocimiento o consentimiento del usuario.

T

Trend Micro®: es una compañía global de software de seguridad la cual desarrolla software de seguridad para equipos de cómputo final, soluciones de correo electrónico, servidores físicos o virtuales, cómputo en la nube, entre otros más.

Trend Micro® Smart Protection Network®: es una solución de protección en la nube administrada por Trend Micro® que brinda servicios de reputación de archivos y reputación de URL´s.

Troyanos: son un tipo de malware que se presenta como un programa legitimo pero que ejecuta otras actividades de manera oculta al usuario como descarga de malware, comunicación con servidores de comando y control, entre otros más.

V

Virtualización: es la abstracción de recursos de una computadora o servidor denominado Hypervisor que crea una capa de abstracción entre el hardware de la máquina física y el sistema operativo de la máquina virtual, dividiéndose el recurso en uno o más entornos de ejecución.

Virus: es un programa informático que depende de una acción para ejecutarse, puede copiarse a sí mismo e infectar una computadora sin el permiso o conocimiento del usuario.

VMWare: es una filial de EMC corporation que proporciona software de virtualización disponible para ordenadores compatibles con x86 es capaz de funcionar en plataformas de tipo Windows, Linux y Mac OS X.

Vulnerabilidades: son fallas de seguridad o debilidades que se encuentran en un software o en un sistema operativo que pueden conducir a brechas de seguridad.

Mesografía

RFP. Proyecto de Protección Antimalware e Integridad de Archivos. Emitido por la Universidad, noviembre, 2013.

S/A. OCM-IT Seguridad en Virtualización tecnológica. Recuperado en noviembre de 2015 de: http://www.ocm-it.com.mx/

Trend Micro. Solo una defensa personalizada puede combatir eficazmente las amenazas persistentes avanzadas (APT). Recuperado el 23 de noviembre de 2015 de: http://www.trendmicro.es/grandes-empresas/ataques-dirigidos-avanzados/

BuroMC. Buro MC Seguridad Informática. Recuperado en noviembre de 2015 de: http://www.buromc.com

Trend Micro. Network Defense. Recuperado en diciembre de 2015 de: http://www.trendmicro.es/grandes-empresas/ciberseguridad/

Microsoft. Descripción general de Microsoft Solutions Framework (MSF). Recuperado en diciembre de 2015 de: https://msdn.microsoft.com/es-es/library/jj161047.aspx

Wikipedia. Proceso para el desarrollo de software. Recuperado en diciembre de 2015 de: https://es.wikipedia.org/wiki/Proceso_para_el_desarrollo_de_software

Monografías.com. Análisis y diseño de sistemas. Recuperado en diciembre de 2015 de: http://www.monografias.com/trabajos/anaydisesis/anaydisesis.shtml