



# *Trabajo Final de Adscripción*

**Universidad Nacional del Nordeste**

**Facultad: F.A.C.E.N.A.**

**Carrera: Licenciatura en Sistemas de Información**

**Profesor: Mgter. David Luis La Red Matinez**

**Alumna: Iriana Nadia Strycek**

**-2009-**

*Sistemas Integrados de  
Seguridad con Tivoli*



# Índice:

<b>Introducción.....</b>	<b>1</b>
<b>Que es Tivoli.....</b>	<b>2</b>
<b>Sistema Integrado.....</b>	<b>3</b>
<b>Administración de Servicios de Tecnologías de Información.....</b>	<b>4</b>
<b>Software Para Seguridad.....</b>	<b>5</b>
<b>Gestión de Almacenamiento.....</b>	<b>27</b>
<b>Gestión de Sistemas.....</b>	<b>28</b>
<b>La Seguridad Para el 2009.....</b>	<b>31</b>
<b>Novedades de IBM Tivoli Security Operations Manager (TSOM) V4.1.....</b>	<b>33</b>
<b>Conclusión.....</b>	<b>34</b>
<b>Bibliografía.....</b>	<b>35</b>

## **INTRODUCCIÓN**

En el contexto actual, donde la información es la esencia de una organización resulta cada vez más necesario disponer de sistemas informáticos, seguros, distribuidos, multiplataformas y que además se encarguen de la gestión automática de la información con acceso desde la web para su control y administración, mejorando la gestión, dado que no hay que estar físicamente frente a los equipos para realizar las tareas pertinentes.

Todo lo señalado precedentemente sería ilusorio si no se dispusiera del software, o del conjunto de software adecuado que facilitara la tarea de respaldar los datos, para que la información de trabajo y la información histórica estén siempre disponibles entre las distintas dependencias de las organizaciones, de forma inmediata y coherente utilizando diferentes plataformas de hardware y de software.

El avance de las nuevas tecnologías pone al alcance de las empresas soluciones capaces de dar respuesta a una globalidad de áreas: almacenamiento, disponibilidad, rendimiento, seguridad, etc. Soluciones cada vez mejores para integrar y gestionar los procesos de negocios.

Dentro de estas soluciones, IBM ha creado unos productos adaptados a la pequeña y mediana empresa, basados en estándares abiertos.

En este trabajo, se darán a conocer las características y ventajas de estos productos, agrupados bajo la marca de Tivoli, destacando especialmente el módulo de seguridad.

## **QUÉ ES TIVOLI**

Tivoli es un software de seguridad, gestión y almacenamiento. Tivoli es una marca de International Business Machines (IBM) Corporation desde su adquisición en 1996. Este software permite a las organizaciones:

- reducir el coste total de propiedad y mejorar los niveles de servicio de su infraestructura de TI y
- mantener un entorno informático seguro y dinámico entre socios, proveedores, clientes y empleados.

El software de gestión de Tivoli ayuda tanto a las empresas tradicionales como a los negocios (e-business) en todo el mundo a gestionar la seguridad, almacenamiento, rendimiento, disponibilidad, configuraciones y operaciones de su infraestructura de TI.

## **A QUIÉN VA DIRIGIDO**

Tivoli es una solución muy versátil, que va dirigida a todo tipo de empresas, con independencia del tamaño de las mismas. Hay soluciones para grandes corporaciones pero también opciones adaptables a la pequeña y mediana empresa.

Entre la larga lista de clientes, las soluciones Tivoli son utilizadas por los 20 proveedores de servicios más importantes del mundo, incluyendo a NTT, AT&T, Deutsche Telekom, WorldCom, Sprint, British Telecom, Telia, France Telecom y Embratel Brasil.

## **CUÁLES SON SUS CARACTERÍSTICAS PRINCIPALES**

Tivoli permite gestionar sistemas, redes, bases de datos, mensajería electrónica, ERPs, servicios y líneas de negocio. Asimismo, los productos Tivoli de IBM proporcionan a los clientes soluciones que simplifican la complejidad de sus entornos y la integración con otros sistemas gracias al soporte de estándares de la industria.

Esta iniciativa, que permite vincular las decisiones de negocio con la infraestructura de TI y el control de servicio que ofrece se denomina “gestión de servicios de negocio”.

El Software de IBM Tivoli ha sido diseñado para ayudar a las empresas a gestionar la complejidad en un entorno e-business dinámico, permitiendo alcanzar el objetivo de maximizar el retorno de las inversiones tecnológicas y proporcionar una infraestructura de e-business segura y con elevada disponibilidad.

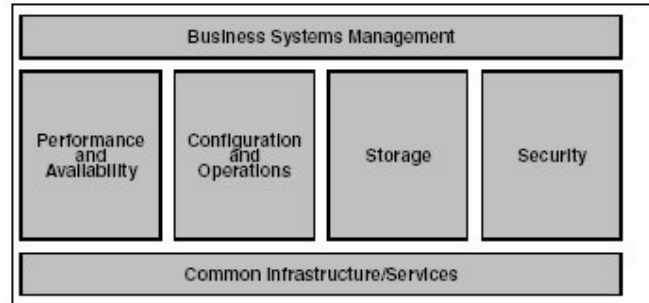
El Software Tivoli ha sido diseñado para proporcionar un mayor valor empresarial con soluciones líderes en la gestión de las prestaciones y de la disponibilidad, de la configuración y de las operaciones, de la seguridad y del almacenamiento de datos.

Los productos de Tivoli han sido agrupados en base a su función:

- Rendimiento y disponibilidad.
- Configuración y Operaciones.
- Gestión de Seguridad.
- Gestión de Almacenamiento.

## TIPOS DE TIVOLI

Tivoli se mueve en un gran mercado, dado el gran número de áreas que cubren sus soluciones: disponibilidad, almacenamiento, seguridad, etc. En el portafolio de Tivoli se integran unas 30 familias de productos que acogen, aproximadamente, 70 soluciones.



Estructura del producto Tivoli.

## SISTEMA INTEGRADO

Un sistema integrado es un sistema informático de uso específico construido dentro de un dispositivo mayor.

Los sistemas integrados se utilizan para usos muy diferentes de los usos generales para los que se emplea un ordenador personal. En un sistema integrado la mayoría de los componentes se encuentran incluidos en la placa base (*motherboard*), (la tarjeta de vídeo, audio, módem, etc.).

Dos de las diferencias principales son el precio y el consumo. Puesto que los sistemas integrados se pueden fabricar por decenas de millares o por millones de unidades, una de las principales preocupaciones es reducir los costes. Los sistemas integrados suelen usar un procesador relativamente pequeño y una memoria pequeña para reducir los costes. Se enfrentan, sobre todo, al problema de que un fallo en un elemento implica la necesidad de reparar la placa íntegra.

Lentitud no significa que vayan a la velocidad del reloj. En general, se suele simplificar toda la arquitectura del ordenador o computadora para reducir los costes.

Los primeros equipos integrados que se desarrollaron fueron elaborados por IBM en los años 1980.

Los programas de sistemas integrados se enfrentan normalmente a problemas de tiempo real.

El software integrado combina la función de varios programas con una sola interfase. Un programa así es diseñado usualmente para el usuario principiante o fortuito. Se omiten muchas características que podrían encontrarse en productos aislados. Por ejemplo, el procesador de palabras en un paquete de software integrado, no tendrá una forma automática de generar una tabla de contenido y poseerá menos opciones sobre cómo manejar las notas al pie, encabezamientos y los pies de texto.

## ADMINISTRACIÓN DE SERVICIOS DE TI

### *Una mejor manera de administrar el negocio de TI.*

La Administración de Servicios de TI ayuda a las organizaciones a manejar mejor su infraestructura de TI, para proporcionar servicios de IT más eficientemente. **Tivoli** ayuda a asegurar la continuidad del servicio de TI - optimizar los costos de TI automatizando los procesos reactivos de administración de TI. Se puede ayudar a optimizar la productividad de TI con un enfoque predictivo de administración de TI; manejo de cumplimiento y riesgos del ambiente de TI.

La intersección de negocio y tecnología es la señal de camino hacia el futuro. La complejidad, cumplimiento, velocidad de cambio, y costos impulsan la necesidad de desarrollar la TI de un enfoque tecnológico a uno de negocio. A medida que estos factores clave de mercado fuerzan a organizaciones de IT a adaptarse, estas soluciones de Tivoli están en la mejor posición para ayudar a enfrentar los desafíos de negocio y TI con productos que utilizan la tecnología autónoma, manejando la **Arquitectura Orientada a Servicios (SOA)**, tanto como herramientas de procesos y experiencia en consultoría que ayudan a concretar las necesidades.

### La forma en que lo resuelve Tivoli

#### **Innovación**

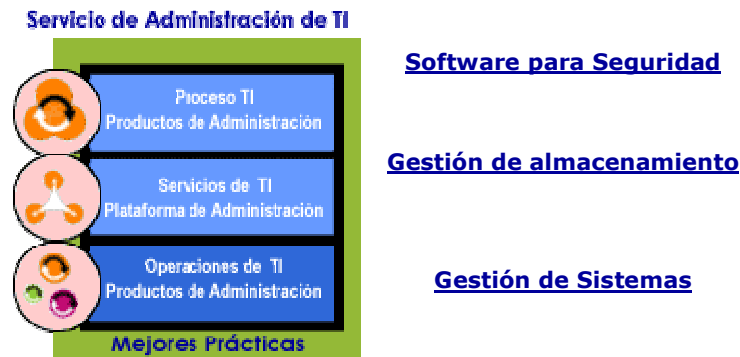
- ITSM platform – una Base de Datos integrada y federada de Change and Configuration Management (CCMDB).
- Construida sobre arquitectura SOA que puede administrar ambientes SOA.

#### **Ejecución**

- Una cartera de productos y servicios de las más completas de la industria.
- Soluciones y mejores prácticas que potencian las tecnologías autónomas autoadministradas.

#### **Liderazgo**

- Colaborar y soportar los ecosistemas basados en Estándares Abiertos.
- Tecnología probada que integra y automatiza los procesos de TI.
- Consultores de primer nivel de ITIL.



## SOFTWARE PARA SEGURIDAD

El software de seguridad se utiliza para proteger la confidencialidad, integridad, privacidad y seguridad de los sistemas de información.

### Tivoli Security Operations Manager

***Una plataforma diseñada para mejorar la gestión de riesgos de la información y las operaciones de seguridad.***

- Centralización de las operaciones de seguridad en distintas organizaciones, tecnologías y procesos.
- Alineación de las operaciones de seguridad con operaciones de IT y prioridades empresariales para maximizar el tiempo de actividad empresarial y de servicio.
- Tratamiento de los requisitos de conformidad y las políticas corporativas de gestión de riesgos.
- Máxima rapidez en la detección y resolución de las incidencias de seguridad.

En el módulo de seguridad de TIVOLI IBM se encuentran los siguientes productos de software que se incorporan a cada empresa según la necesidad de la misma.

### Rational AppScan

⇒ **IBM Rational AppScan Enterprise Edition: Es una solución multiusuario y está basada en web de informes y pruebas de vulnerabilidad de las aplicaciones.**

Está indicada para equipos que necesitan realizar evaluaciones de la seguridad de las aplicaciones web de forma centralizada, y proporciona un conjunto de soluciones totalmente integrado:

- Arquitectura empresarial escalable que permite explorar varias aplicaciones simultáneamente.
- Control centralizado de las pruebas de seguridad de las aplicaciones web en toda la empresa.
- Recomendaciones de reparación inteligente para facilitar el proceso de remediación una vez identificadas y validadas las vulnerabilidades.
- Supervisión ininterrumpida y agregación de métricas para asegurar la remediación y la tendencia a la mejora con el tiempo.
- Paneles de instrumentos sofisticados y vistas de informes flexibles para proporcionar visibilidad de los riesgos y el progreso de remediación en toda la empresa. Ofrece la tasa de falsos positivos más baja de la industria y encuentra los problemas de seguridad más graves.
- Más de 40 informes de cumplimiento de seguridad listos para utilizar, como PCI Data Security Standard, ISO 17799 e ISO 27001, HIPAA, GLBA y Basel II.
- Acceso a los informes y a los permisos de exploración basado en roles para facilitar la aplicación de las políticas de prueba y centralizar las exploraciones de vulnerabilidad.
- Sistemas operativos admitidos: Windows.

⇒ **IBM Rational AppScan Express Edition: Es una herramienta que prueba la seguridad de las aplicaciones web y automatiza la evaluación de las vulnerabilidades.**

Proporciona niveles categóricos de seguridad en aplicaciones web para pequeñas y medianas empresas:

- Permite realizar pruebas automáticas y completas de las vulnerabilidades de las aplicaciones web.
- Reduce notablemente la necesidad de realizar pruebas manuales, lo cual se traduce en un importante ahorro de gastos.
- Explora automáticamente las aplicaciones web complejas mediante tecnología Web 2.0, como Adobe Flash, JavaScript y AJAX.
- Ayuda a cumplir los estándares clave de conformidad, como el estándar Payment Card Industry Data Security Standard (PCI DSS).
- Ofrece resultados simplificados de la exploración gracias a un asistente experto en resultados, y proporciona recomendaciones avanzadas de remediación necesarias para solucionar los problemas que hayan surgido durante la exploración.
- Sistemas operativos admitidos: Windows.

⇒ **Rational AppScan OnDemand: Es una edición de IBM Rational AppScan para exploraciones de seguridad de aplicaciones web avanzadas.**

Ofrece pruebas de seguridad de aplicaciones web mediante software como servicio (SaaS).

IBM Rational AppScan OnDemand es una solución SaaS muy eficaz que identifica y prioriza los riesgos de seguridad de aplicaciones web en las aplicaciones de preproducción:

- Presentada y ejecutada por un equipo altamente calificado de expertos en productos de conformidad y seguridad que maximizan las funciones del producto en su nombre.
- Costes iniciales bajos y coste total de propiedad reducido de forma continuada con un servicio de suscripción que no necesita formación ni conocimientos de seguridad internos, infraestructuras, configuración ni gastos de mantenimiento de software.
- El tiempo de recuperación sin precedentes permite identificar los riesgos en línea de forma inmediata, y proporciona experiencia en conformidad y seguridad, y acceso instantáneo a las mejores prácticas del sector.
- Solución empresarial segura y escalable.
- El acceso a los informes basado en roles y los permisos de exploración implementan las políticas de pruebas y centralizan las exploraciones de vulnerabilidad. Además, sofisticados paneles de instrumentos ofrecen visibilidad de los riesgos y del progreso de remediación en toda la empresa.
- Punto de partida excelente que facilita el aprendizaje progresivo con la ayuda de expertos y acceso completamente basado en el navegador para volver a realizar pruebas, ejecutar exploraciones preconfiguradas, y crear y ejecutar nuevas configuraciones de exploración.
- Le permite centrarse en lo que realmente importa: solucionar los problemas.

⇒ **IBM Rational AppScan OnDemand Production Site Monitoring: Una edición de IBM Rational AppScan para exploraciones de seguridad de aplicaciones web avanzadas. Ofrece pruebas de seguridad de aplicaciones web mediante software como servicio (SaaS).**

Es una solución SaaS muy eficaz que identifica y prioriza de forma continuada los riesgos de seguridad asociados al contenido web dinámico publicado en sitios de producción:

- Presentada y ejecutada por un equipo altamente calificado de expertos en productos de conformidad y seguridad que maximizan las funciones del producto en su nombre.
- Utiliza un subconjunto no intrusivo de la política de pruebas AppScan, y la definición limitada sin inicio de sesión garantiza las exploraciones seguras de los sitios de producción.
- Costes iniciales bajos y coste total de propiedad reducido de forma continuada con un servicio de suscripción que no necesita formación ni conocimientos de seguridad internos, infraestructuras, configuración ni gastos de mantenimiento de software.

- El tiempo de recuperación sin precedentes permite identificar los riesgos en línea de forma inmediata, y proporciona experiencia en conformidad y seguridad, y acceso instantáneo a las mejores prácticas del sector.
- Solución empresarial segura y escalable.
- El acceso a los informes basado en roles y los permisos de exploración implementan las políticas de pruebas y centralizan las exploraciones de vulnerabilidad. Además, sofisticados paneles de instrumentos ofrecen visibilidad de los riesgos y del progreso de remediación en toda la empresa.
- Punto de partida excelente que facilita el aprendizaje progresivo con la ayuda de expertos y acceso completamente basado en el navegador para volver a realizar pruebas, ejecutar exploraciones preconfiguradas, y crear y ejecutar nuevas configuraciones de exploración.

⇒ **Rational AppScan Reporting Console: Solución multiusuario de informes centralizados basada en web. Ofrece informes centralizados sobre datos de vulnerabilidad de aplicaciones web.**

Está indicada para equipos que necesitan centralizar las evaluaciones de seguridad de las aplicaciones web:

- Arquitectura empresarial escalable que centraliza los informes de exploraciones de vulnerabilidad de varias aplicaciones.
- Acceso a los informes y a los permisos de exploración basados en roles para facilitar la aplicación de las políticas de pruebas y centralizar las exploraciones de vulnerabilidad.
- Paneles de instrumentos sofisticados y vistas de informes flexibles para facilitar la visibilidad de los riesgos y el progreso de remediación en toda la empresa.
- Más de 40 informes de cumplimiento de seguridad listos para utilizar, como PCI Data Security Standard, ISO 17799 e ISO 27001, HIPAA, GLBA y Basel II.
- Supervisión ininterrumpida y agregación de métricas para asegurar la remediación y la tendencia a la mejora con el tiempo.
- Los asistentes y las funciones de configuración de exploraciones simplifican el uso y facilitan la adopción de la tecnología.
- Sistemas operativos admitidos: Windows.

⇒ **Rational AppScan Standard Edition: Una edición de IBM Rational AppScan para exploraciones de seguridad de aplicaciones web avanzadas. Es una herramienta que prueba la seguridad de las aplicaciones web y automatiza la evaluación de las vulnerabilidades.**

AppScan realiza pruebas para detectar vulnerabilidades en las aplicaciones web más comunes, como Cross-Site Scripting, desbordamiento del

almacenamiento intermedio y exploraciones de riesgos de nuevas aplicaciones flash/flex y Web 2.0:

- Soporte para las tecnologías Web 2.0 más recientes: incluye el análisis y la ejecución de aplicaciones JavaScript y Adobe Flash; un conocimiento profundo de protocolos relacionados con relacionados con AJAX y Adobe Flex, como JSON, AMF y SOAP, y un soporte global para entornos SOA complejos, así como configuración e informes personalizados para aplicaciones de Mashup y basadas en procesos.
- Funciones de personalización y capacidad de expansión: permite a la comunidad de usuarios crear y compartir complementos de código abierto.
- Resultados de la exploración simplificados gracias a un asistente experto en resultados: proporciona las recomendaciones avanzadas de remediación necesarias para solucionar los problemas que hayan surgido durante la exploración.
- Funciones automatizadas para las pruebas de intrusión: los programas de utilidad de realización de pruebas avanzadas, junto con la infraestructura Physcan, complementan a las pruebas manuales al ofrecer más potencia y eficacia.
- Informes de conformidad a normativa: 40 informes de conformidad listos para usar, incluidos PCI Data Security Standard, ISO 17799, ISO 27001 y Basel II.
- Sistemas operativos admitidos: Windows.

⇒ **Rational AppScan Tester Edition: Pruebas de seguridad de las aplicaciones web integradas en el proceso de control de calidad.**

Integra las pruebas de seguridad en los procesos de control de calidad para el desarrollo de las aplicaciones web:

- Presenta un registrador de defectos de control de calidad que permite a los equipos que realizan las pruebas de seguridad configurar y ejecutar exploraciones en AppScan con la garantía de que los resultados se registran de forma rápida y sencilla en la herramienta de seguimiento de defectos elegida.
- Ofrece visibilidad empresarial con soporte e integración con IBM Rational ClearQuest, Microsoft Visual Studio Team System y Mercury Quality Center.
- Proporciona formación en tiempo real sobre pruebas de seguridad y técnicas de codificación.
- Amplía la cobertura de las pruebas más allá de las funcionales y las de rendimiento.
- Ofrece a los equipos de control de calidad una única consola, medidas y un entorno para gestionar la seguridad y las pruebas de calidad de las aplicaciones web.

- Automatiza las pruebas y la aplicación de la seguridad como parte de la ejecución normal del control de calidad, y evita que el personal que realiza el control de calidad tenga que aprender herramientas de seguridad nuevas o avanzadas.

## Tivoli Access Manager

Tivoli Access Manager for e-business es una premiada solución de control de accesos basada en políticas para las aplicaciones de e-business y empresariales. Permite a las organizaciones controlar tanto el acceso inalámbrico, como el conectado con cable a aplicaciones y datos y proporciona el inicio de sesión exclusivo (SSO) para usuarios autorizados. Se integra con aplicaciones de e-business para ofrecer una experiencia en e-business segura y personalizada para los usuarios autorizados.

### **Tivoli Access Manager for e-business facilita la integración de las aplicaciones de e-business:**

- Soporta múltiples directorios para permitir el compartimiento de información de usuario.

### **Tivoli Access Manager for e-business y otras aplicaciones:**

- Ofrece una gestión unificada de accesos y un inicio de sesión exclusivo seguro para todos los usuarios.
- Proporciona J2EE Security para servidores de aplicaciones WebSphere y BEA, sin ningún plug-in obligatorio, para habilitar aplicaciones que se gestionarán como parte de una estrategia consistente dirigida por políticas que utiliza un control de accesos basado en estándares.
- Incluye un soporte de agentes de servidor web que habilita la flexibilidad del despliegue, en términos de delegación de accesos de usuario, grupo, rol, política y aplicación que proporcionan tareas y en términos de las opciones del registro de usuario.
- Proporciona un registro que realiza el propio cliente a través de una plantilla para que los usuarios finales puedan inscribirse ellos mismos rápidamente en el entorno web de la empresa.
- Se integra con soluciones Siebel CRM, SAP y Portal desde Plumtree, WebSphere, WebLogic y otras soluciones Portal para proporcionar un modelo de seguridad común (autenticación, control de accesos, inicio de sesión exclusivo y auditoría).

### **Tivoli Access Manager para e-business proporciona nuevas capacidades como:**

- Un motor de reglas dinámicas.
- Inicio de sesión exclusivo y entre empresas mejorado.
- Integración de Tivoli Identity Manager para reducir costes con el autoservicio.
- Nuevas funciones de IBM zSeries y un mayor soporte de Linux.
- Gestión de identidades del suministrador de servicio.

- Rendimiento, integración, y mejoras en el desarrollo.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
HP-UX,  
Linux,  
Sun Solaris,  
Windows 2000,  
Windows NT.

⇒ **Tivoli Access Manager for Business Integration: Es una solución de gestión de seguridad para multiplataformas para WebSphere MQ que mejora significativamente el entorno de seguridad nativo de WebSphere MQ.**

Actualiza los servicios de seguridad de WebSphere MQ para proporcionar una protección de datos a nivel de aplicación para aplicaciones basadas en WebSphere MQ, sin la necesidad de modificarlas o volverlas compilar.

La protección de datos a nivel de aplicación difiere de la protección de datos a nivel de enlace o canal en que la integridad y confidencialidad de los mensajes puede demostrarse, no sólo mientras los mensajes están en tránsito de un sistema a otro, sino también cuando se encuentran bajo el control del propio WebSphere MQ (por ejemplo, un residente en una cola).

Esta seguridad es vital para los clientes que utilizan WebSphere MQ para procesar información que podría identificar a una persona o cualquier otro tipo de datos sensibles como, por ejemplo, transacciones de alto valor financiero.

### **Tivoli Access Manager for Business Integration amplía la seguridad para WebSphere MQ:**

- Soporta la protección de datos a nivel de aplicación de los mensajes de WebSphere MQ entre servidores heterogéneos.
- Consolida la gestión y simplifica la administración de la protección de datos y de las políticas de control de accesos para WebSphere MQ.
- Proporciona soporte entre la mayoría de los servidores más comunes en los que se ejecuta WebSphere MQ.
- Una administración basada en web permite la gestión remota de WebSphere MQ.
- Moderniza el desarrollo de aplicaciones y actualizaciones para hacerlas visibles a aplicaciones existentes basadas en WebSphere MQ.

### **Tivoli Access Manager for Business Integration proporciona una serie de nuevas mejoras:**

- Soporte de plataforma para HP-UX y SuSE Linux Enterprise Server (SLES) para IA32.
- Soportes de WebSphere MQ cliente.
- Ambas, aplicaciones Java Message Service (JMS) y C.
- Windows, AIX, Solaris, HP-UX y SLES para IA32.

- Plug-in de autorización para WebSphere Business Integration Message Broker y WebSphere Business Integration Event Broker.
- Controla el acceso de publicación/suscripción a temas si se utiliza el servicio Java Message Service en tiempo real en transporte de IP.
- Compatible con las versiones actuales de WebSphere Business Integration Brokers, WebSphere MQWorkflow y WebSphere Interchange Server.
- Compatible con el nuevo programa de salida cruzada de AP de WebSphere MQ.
- Soporte para el uso con Novelle Directory.
- Soporte para el cifrado mediante el uso de Advanced Encryption Standard (AES).
- Mejor escalabilidad.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
Sun Solaris,  
Windows 2000,  
Windows NT,  
Windows XP.

### **Anexo 1**

**WebSphere MQ** (anteriormente MQSeries), el punto central de la familia **MQ**, proporciona conectividad de aplicaciones. Puede utilizarse de forma autónoma o con otros miembros de la familia para ofrecer una solución de integraciones de negocio global.

### **IBM WebSphere MQ**

- Ofrece una mensajería fiable para la arquitectura orientada a servicios (SOA).
- Permite la integración de aplicaciones empresariales.
- Admite cualquier tipo de conectividad heterogénea, desde equipos de escritorio hasta macrocomputadoras (admite más de 35 plataformas distintas).
- Dispone de una extensa familia de interfaces de programación de aplicaciones (API) diseñados con el objeto de facilitar la creación de código para tareas de mensajería.
- Garantiza la entrega sin duplicaciones de los mensajes importantes.

### **Novedades de WebSphere MQ:**

- Soporte de la plataforma Linux para iSeries y Linux para pSeries POWER.
- Soporte integrado para los datos de Web Services en un Interfaces de 64 bits en AIX, HP-UX y Solaris.
- Soporte al protocolo de Internet versión 6 (IPv6).
- Soporte integrado para los datos de Web Services en un transporte **MQ** fiable.
- Prestaciones de publicación/suscripción integradas.
- Una interfaz ampliable de usuario para la configuración basada en Eclipse en las plataformas Microsoft Windows y Linux x86.

- El producto Quick Tour que incorpora los conceptos básicos de la conectividad de aplicaciones y describe las funciones y prestaciones de WebSphere MQ; el programa de utilidad File Transfer (en las plataformas Microsoft Windows y Linux x86) proporciona un método sencillo para enviar datos (mensajes) de un sistema MQ a otro.
- Soporte para IBM Message Service Client for C/C++.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

- AIX
- HP OpenVMS (Alpha)
- HP-UX
- iSeries i5/OS V5R3
- iSeries OS/400 V5R2
- Linux
- Linux for iSeries
- Linux for pSeries POWER
- Sun Solaris
- Windows 2000
- Windows NT
- Windows XP

⇒ **Tivoli Access Manager for Operating Systems: Es un sistema de control de accesos basado en políticas para los sistemas operativos UNIX y Linux.**

Esta completa solución de seguridad se ocupa de forma eficaz de las numerosas vulnerabilidades del sistema que rodean a las cuentas de un súper usuario o "root" de UNIX/Linux.

Hay numerosas anomalías de seguridad en entornos UNIX/Linux procedentes del abuso de cuentas de súper-usuario o de ataques de "piratas" que acceden a esta cuenta.

- Tivoli Access Manager for Operating Systems ofrece seguridad mejorada para entornos UNIX.
- Permite a los usuarios acceder a las listas de control de accesos (ACL) para categorizar el acceso a los recursos de la aplicación y del sistema operativo, independientemente del estado de privilegio UNIX de un usuario.
- Habilita la administración centralizada de políticas de seguridad consistentes entre la empresa.
- Protege los objetos del sistema de archivos y la capacidad UNIX para conmutar los ID de usuario para garantizar la seguridad de las aplicaciones.
- Rastrea el proceso de inicio de sesión de UNIX y aplica políticas que evitan posibles accesos no autorizados.
- Incluye funciones ampliadas de auditoría y de inicio de sesión de plataforma.

### **Novedades de Tivoli Access Manager para Operating Systems:**

- Se han ampliado las funciones de auditoría y ahora proporcionan un mecanismo de reenvío para permitir la recopilación centralizada de datos de auditoría desde múltiples sistemas de Access Manager. Estos datos de auditoría permanecen asegurados por Access Manager for Operating Systems. La auditoría sólida quiere decir que los administradores y auditores de seguridad pueden considerarse seguros ya que cumplen por completo con las normas de seguridad corporativas y del gobierno. Además, los informes de auditoría detallados de Access Manager for Operating Systems permiten a los administradores demostrar la conformidad con las políticas corporativas y las normas del gobierno.
- Como parte de este realce, IBM también ofrecerá módulos de políticas configuradas previamente para asegurar aplicaciones de seguridad comunes listas para ser instaladas. Estos módulos proporcionan configuraciones de seguridad por omisión para las aplicaciones más populares, hecho que ayuda a evitar abusos por parte de cuentas de usuarios root o de otros usuarios.
- Directory Server y partes de WebSphere Application Server y Access Manager for e-business se incluyen para el uso restringido de Tivoli Access Manager for Operating Systems.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
HP-UX,  
Linux,  
Sun Solaris,  
Windows 2000,  
Windows NT.

⇒ **Tivoli Access Manager for Enterprise Single Sign-On: Ofrece una potente autenticación, automatización de acceso y elaboración de conformidad en los puntos finales de la empresa.**

Simplifica, refuerza y realiza un seguimiento del acceso a todas las aplicaciones de Microsoft Windows, web, Java, mainframe, etc., en todos los puntos de acceso de la red principales, incluyendo escritorios de Windows, ordenadores portátiles, kioscos compartidos, servidores Citrix, servidores Microsoft Terminal Server y portales web:

- Ayuda a simplificar la experiencia del usuario final eliminando la necesidad de recordar y gestionar nombres y contraseñas de usuario, y automatizando el inicio de sesión y el acceso.
- Mejora la seguridad reduciendo el comportamiento erróneo de las contraseñas de usuario final.

- Ayuda a reducir los costes de centro de asistencia relacionados con contraseñas disminuyendo el número de llamadas de restablecimiento de contraseñas.
- Permite la gestión completa de las sesiones de máquinas kioskos para mejorar la seguridad y la productividad del usuario.
- Mejora la seguridad a través de una amplia opción de potentes factores de autenticación.
- Aprovecha las capacidades centralizadas de auditoría e informes para facilitar la conformidad con las normas de seguridad y privacidad.
- Amplía la autorización detallada y las autorizaciones para aplicaciones web de IBM Tivoli Access Manager for e-business, gestionando completamente el inicio de sesión único en todos los puntos de acceso de la red.
- Permite la gestión completa de accesos e identidades integrando las funciones centralizadas de gestión de identidades de IBM Tivoli Identity Manager con la automatización del acceso y el inicio de sesión único de la empresa.

## **Tivoli Directory Integrator**

Tivoli Directory Integrator es una arquitectura abierta, una solución de metadirectorios para la sincronización del intercambio de información en tiempo real entre orígenes de aplicaciones o directorios. Permite a las empresas establecer una infraestructura de autorización de datos de identidad actualizada para que funcione como una plataforma para su seguridad empresarial crítica y las aplicaciones de servicios web:

- Tivoli Directory Integrator permite obtener el control de los datos de identidad empresarial.
- Una arquitectura abierta gracias a scripts de Java.
- Entorno de desarrollo de conector y conectores creados anteriormente.
- Mecanismos dirigidos por sucesos y de manejo de excepciones.
- Arquitectura flexible y eficaz de los recursos basada en el almacenamiento de datos no persistentes.

### **Novedades de Tivoli Directory Integrator:**

- Ampliaciones de la capacidad de utilización.
- Soporte de la seguridad PKI (infraestructura de clave pública).
- Nuevos conectores de Tivoli Directory Integrator.
- Una API de Java.
- Soporte de la plataforma z/OS.
- Mejoras en la capacidad de ampliación y la fiabilidad.
- El servidor Tivoli Directory Server.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
HP-UX,

Linux,  
z/OS,  
Sun Solaris,  
Windows 2000,  
Windows NT.

## **Tivoli Directory Server**

Tivoli Directory Server es un potente directorio empresarial, rico en seguridad y que cumple los estándares de las intranets corporativas e Internet. Directory Server ha sido construido para servir como base de los datos de identidad, para desarrollar e implementar rápidamente sus aplicaciones web e iniciativas de gestión de seguridad e identidad, incluida la gestión y la replicación, y las funciones de seguridad.

Con Tivoli Directory Server se podrá elegir la estrategia de autenticación, simplemente utilizar la autenticación de ID de usuario y contraseña o implementar una estructura de autenticación digital, basada en certificados, más segura. Tivoli Directory Server también incluye una interfaz de plug-in Simple Authentication Security Layer (SASL), que a su vez incluye Challenge - Response Authentication Mechanism MD5 (CRAM-MD5) y la autenticación Kerberos, de ser necesario.

Tivoli Directory Server es una potente infraestructura de identidades Lightweight Directory Access Protocol (LDAP) constituye la base para implementar aplicaciones de gestión de identidades globales y arquitecturas de software avanzadas como Web Services:

- El soporte de LDAP V3 garantiza la compatibilidad con las aplicaciones basadas en el estándar del sector LDAP.
- El fiable motor DB2 Universal Database V8.1 ofrece escalabilidad a diez millones de entradas, así como a grupos de cientos de miles de miembros.
- Ofrece soporte para una amplia gama de plataformas: AIX, Solaris, Microsoft Windows 2000 y HP-UX, así como las distribuciones Linux para Intel y las plataformas eServer iSeries, pSeries y zSeries.
- Presenta una robusta capacidad de replicación para la replicación tanto maestra como subordinada, de pasarela, en cascada y de igual a igual, con docenas de servidores maestros.
- Facilita la gestión y utilización de la GUI de administración de la web y funciones como los grupos dinámicos y anidados, junto con los resultados de búsqueda clasificados y repaginados.
- Se integra con los sistemas operativos IBM, WebSphere middleware y los productos de seguridad y gestión de identidad Tivoli.

### **Novedades de Tivoli Directory Server:**

- Mejoras en el estándar de directorios.
- Mejoras de seguridad.
- Ampliaciones en la capacidad de servicio y el despliegue.

- Soporte de plataforma ampliado.
- Mejoras en el rendimiento.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
HP-UX,  
iSeries Power Linux,  
Linux,  
Linux on zSeries,  
pSeries,  
pSeries Linux,  
zSeries,  
Sun Solaris,  
Windows 2000,  
Windows -WS2003,  
Windows NT.

### **Tivoli Identity Manager**

Tivoli Identity Manager proporciona una gestión de identidades basada en políticas en entornos heredados y de e-business.

Las intuitivas interfaces administrativas web y de autoservicio se integran con los procesos empresariales ya existentes para ayudar a simplificar y automatizar la gestión y el suministro de usuarios.

Incorpora un motor de flujo de trabajo y utiliza los datos de identidad para distintas actividades, como auditorías y generación de informes.

Tivoli Identity Manager interactúa directamente con los usuarios y con dos tipos de sistemas externos: orígenes de identidad y mecanismos de control de acceso.

Los sistemas de identidad proporcionan información de autorización sobre los usuarios que necesitan cuentas.

El sistema de suministro se comunica directamente con los sistemas de control de acceso para crear cuentas, proporcionar información de usuario y contraseñas y definir las titularidades de la cuenta. De forma inversa, los cambios administrativos locales realizados en un sistema de control de acceso se capturan y se notifican al sistema de suministro para su evaluación basada en la política:

- Tivoli Identity Manager automatiza la gestión de la información de usuarios.
- Centraliza la definición de usuarios y el suministro de servicios de usuarios para reducir la complejidad relacionada con la gestión desde múltiples interfaces nativas.
- Satisface las necesidades de gestión distribuida o basada en políticas mediante la delegación de privilegios administrativos basada en roles más allá de los límites geográficos y de su organización.

- Reduce los errores inherentes en los procesos empresariales manuales gracias a la automatización de la creación de usuarios y de las solicitudes de aprobación.
- Proporciona funciones de conciliación y el kit de herramientas de gestión de aplicaciones para dar respuesta a los cambios organizativos, como fusiones y adquisiciones.
- Da soporte a rutas de aprobación inteligentes para automatizar los procesos de envío y aprobación de solicitudes de acceso y cambios de la información de usuario.
- Incluye mecanismos de auditoría e informes para permitir a los administradores generar informes sobre los recursos a los que tienen acceso los usuarios.
- Da soporte a hasta decenas de millones de usuarios en una iniciativa de e-business.

#### **Novedades de IBM Tivoli Identity Manager:**

- Simulación de políticas, que proporciona unos casos de ejemplos potentes que elaboran conjeturas relacionadas con el cambio de las políticas de seguridad.
- Nuevos informes centralizados sobre políticas de seguridad, derechos actuales de acceso y sucesos de auditoría para gestionar mejor las necesidades de conformidad.
- Corrección e inteligencia para la conformidad de políticas, que direcciona las cuestiones de conformidad complejas a través del flujo de trabajo y proporciona acciones de inteligencia y recomendadas sobre los temas de conformidad, lo cual elimina la necesidad de revisar manualmente políticas.
- Un equipo mejorado de administrador a través de la notificación agilizada, la gestión de elementos masivos que se deben hacer y la propiedad y delegación de tareas.
- Capacidades para importar / exportar configuración y políticas para migrar fácilmente valores de políticas y de configuración entre diferentes entornos o servidores Tivoli Identity Manager como, por ejemplo, la garantía de calidad para la producción.

#### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
HP-UX,  
Sun Solaris,  
Windows 2000.

### **Tivoli Identity and Access Manager**

Ofrece gestión del ciclo de vida de los usuarios y controles de accesos para los usuarios internos y externos.

Ofrece una solución de gestión de usuarios segura, automatizada y basada en las políticas.

IBM Tivoli Access Manager for e-business es un hub de autenticación y de autorización para aplicaciones web y otras aplicaciones que centraliza la gestión de la seguridad y facilita y rentabiliza el despliegue seguro de dichas aplicaciones:

- Permite los inicios de sesión únicos y flexibles para las aplicaciones basadas en web y puede reducir las llamadas al centro de atención que conlleva disponer de varias contraseñas.
- Reduce los costes de administración asociados a la gestión de cuentas, políticas, credenciales y derechos de acceso a lo largo del ciclo de vida del usuario.
- Centraliza y automatiza la gestión de usuarios, la autenticación, los derechos de acceso, las políticas de auditoría y el suministro de servicios de usuario.
- Agiliza la incorporación de aplicaciones y de usuarios nuevos a través de políticas y plantillas preconfiguradas.
- Nueva modalidad "sólo lectura" para auditores, informes de conformidad adicionales, programa de creación de informes personalizado e integración con Tivoli Compliance Insight Manager para los informes de auditoría relacionados con reglas y métodos recomendados.
- Corrige los derechos de acceso que no cumplen con las normativas mediante flujos de trabajo de renovación de certificados o, de forma automática, a través de políticas de control de accesos, y proporciona detalles útiles para el auditor a fin de mantener la conformidad.
- Permite controles de inicio de sesión avanzados, como de dispositivo de tarjeta inteligente, de certificados y de autenticación incrementada o de varios factores mediante la autenticación en un único punto.

## **Tivoli Privacy Manager for e-business**

Tivoli Privacy Manager for e-business está diseñado para ayudar a las empresas a crear políticas y prácticas de privacidad directamente en sus aplicaciones y su infraestructura de comercio electrónico. Puede utilizarse para automatizar muchas actividades de cumplimiento de la privacidad, lo que simplifica la incorporación, supervisión e imposición de estas políticas en los procesos comerciales.

Tivoli Privacy Manager for e-business proporciona una visión panorámica de las políticas de privacidad de la empresa, permitiéndole crear, editar, imponer y gestionar de manera centralizada dichas políticas en toda la infraestructura de TI.

Tivoli Privacy Manager for e-business trabaja en conjunción con Tivoli Access Manager for e-business al incorporar especificaciones de objetivos comerciales y opciones para el usuario final en las solicitudes de acceso. De este modo, Tivoli Privacy Manager for e-business proporciona la primera plataforma de

gestión empresarial que garantiza que el acceso a los datos confidenciales se realiza con un propósito aprobado:

- Tivoli Privacy Manager for e-business proporciona la gestión de la privacidad para toda la empresa.
- Ofrece una herramienta basada en la Web para transformar la política de privacidad escrita en formato electrónico, creando una política de privacidad digital que puede implantarse en diversos sistemas.
- Permite asignar campos de datos, objetivos comerciales y grupos específicos a aplicaciones y sistemas de TI supervisados, lo que automatiza la publicación de cambios en las políticas existentes o la adición de nuevas políticas a las aplicaciones y sistemas.
- Proporciona herramientas de generación de informes para generar pistas de auditoría con secciones optativas y permite el acceso a la información de identificación personal a los usuarios de los datos.
- Supervisa el envío de información a los repositorios LDAP y las solicitudes de acceso a fin de activar la supervisión de la privacidad en LDAP.
- Incluye un kit de herramientas de programación de software para desarrollar nuevos agentes de supervisión.
- Aprovecha la infraestructura de seguridad de Tivoli Access Manager y la infraestructura de aplicaciones de WebSphere.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
Sun Solaris,  
Windows 2000.

### **Tivoli Risk Manager**

Tivoli Risk Manager le ayuda a gestionar de forma centralizada los incidentes y vulnerabilidades de seguridad en toda la empresa desde una única consola de seguridad. Gestiona y asigna prioridades a la ingente cantidad de eventos de seguridad generados por todas las aplicaciones, sistemas operativos y dispositivos de red a fin de proporcionar una visión global de la arquitectura de seguridad.

Tivoli Risk Manager ayuda a eliminar la información confusa, como los falsos positivos, y a identificar y gestionar con rapidez los incidentes y puntos vulnerables de seguridad con el objeto de que los administradores puedan responder con medidas de seguridad adaptativas.

Gracias a sus funciones de generación de informes, los administradores pueden detectar los riesgos de seguridad empresarial y aplicar acciones correctoras.

Tivoli Risk Manager ahora también incluye Tivoli Enterprise Console, Tivoli NetView y DB2. La integración entre Tivoli Enterprise Console y Tivoli NetView ofrece la capacidad de efectuar análisis en profundidad de la topología de la red a fin de comprobar dónde están los recursos afectados y permite determinar con exactitud la causa original de los problemas.

Asimismo, Tivoli Risk Manager incluye Tivoli Enterprise Data Warehouse, que aporta funciones de generación de informes empresariales:

- Tivoli Risk Manager realiza la gestión centralizada de los incidentes de seguridad y los puntos vulnerables.
- Consolida los eventos de seguridad procedentes de diversos productos de seguridad, como por ejemplo, servidores de seguridad, sistemas de detección de intrusos, aplicaciones de red y equipos de escritorio.
- Utiliza una correlación avanzada de eventos para eliminar la información confusa, como los falsos positivos, identificar con prontitud las verdaderas amenazas para la seguridad y determinar la gravedad de dichos ataques.
- Proporciona una solución lista para utilizarse que permite gestionar los incidentes en toda la organización.
- Integra los eventos de gestión de red, sistemas y seguridad para acelerar la resolución de problemas.
- Admite el almacenamiento persistente de alertas e incidentes en una base de datos relacional que suministra registros históricos de los ataques e intrusiones.
- Admite herramientas avanzadas de auditoría y generación de informes.

#### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
HP-UX,  
Linux,  
Sun Solaris,  
Windows 2000,  
Windows NT,  
Windows XP.

### **Tivoli Key Lifecycle Manager**

IBM Tivoli Key Lifecycle Manager permite a las organizaciones de IT gestionar mejor el ciclo de vida de las claves de cifrado, ya que centraliza y refuerza los procesos de gestión de claves:

- Centraliza y automatiza el proceso de gestión de claves de cifrado.
- Mejora la seguridad de los datos y reduce significativamente el número de claves de cifrado que se deben gestionar.
- Simplifica la gestión de las claves de cifrado mediante una interfaz de usuario intuitiva para la configuración y la gestión.
- Minimiza el riesgo de perder o de poner en peligro la información importante.
- Facilita la gestión de la conformidad con los estándares normativos, como las leyes Sarbanes-Oxley y Health Insurance Portability and Accountability Act (HIPAA).

- Amplía las funciones de gestión de claves en los productos IBM y no IBM.
- Aprovecha los estándares abiertos para adquirir flexibilidad y simplificar la interoperabilidad entre proveedores.

## **Tivoli Compliance Insight Manager**

Supervisa de forma eficaz y automática la actividad del usuario mediante un panel de instrumentos de alto nivel e informes de conformidad:

- Obtiene rápidamente más detalles acerca del comportamiento del usuario, la actividad del sistema y la información de seguridad en todos los tipos de plataforma.
- Compara entradas de registros siguiendo una política de línea base para detectar y minimizar los problemas de seguridad.
- Crea informes para dar soporte a las solicitudes de pruebas de los auditores y a las investigaciones de los gestores de seguridad, sin necesidad de invertir una gran cantidad de dinero en expertos en plataformas.
- Responde rápidamente a las incidencias gracias a su habilidad para establecer acciones y alertas acerca de la actividad de usuarios privilegiados y, al mismo tiempo, permita que los administradores realicen su trabajo.

### **Novedades de Tivoli Compliance Insight Manager V8.0:**

IBM Tivoli Compliance Insight Manager V8.0 permite:

- Automatizar los informes de auditorías mediante un panel de instrumentos de conformidad empresarial y varios módulos de gestión de la conformidad.
- Recopilar, almacenar y recuperar los registros de forma eficiente y fiable mediante una gestión automática de los registros.
- Aprovechar las funciones de búsqueda fáciles de utilizar para optimizar los análisis y las investigaciones forenses de los incidentes de alta seguridad incluidos en los registros almacenados.
- Realizar auditorías y supervisiones efectivas de usuarios privilegiados y auditorías (PUMA) en bases de datos, aplicaciones, servidores y mainframes.
- Integrar con las soluciones IBM Tivoli de gestión de los eventos de seguridad, de control de accesos y de gestión de la identidad para optimizar los esfuerzos dedicados a la capacidad de respuesta ante emergencias y requisitos de conformidad.

Los retos de seguridad y conformidad son mayores que nunca debido al incremento de los requisitos, del coste de la falta de conformidad y de la complejidad en entornos de IT, así como a la falta de previsión y visibilidad en las infraestructuras. Como resultado, las organizaciones de IT deben encontrar

un modo de dar soporte a las tareas imprescindibles, como gestionar los riesgos de seguridad, responder a los requisitos de conformidad y dar soporte a la actividad principal, que unas veces se solapa y otras compite. La necesidad de atender a estos imperativos de forma simultánea con recursos limitados ha creado un entorno de IT complejo al que deben hacer frente los CIO.

IBM Tivoli Compliance Insight Manager V8.0 es una solución automatizada para supervisar, investigar e informar acerca de la actividad de los usuarios en la empresa. Tivoli Compliance Insight Manager ofrece una seguridad continua y no intrusiva, así como pruebas documentales de que sus datos y sistemas se están gestionando según las políticas empresariales.

Podrá comprobar rápidamente la actividad de los usuarios gracias a un sencillo panel de instrumentos de conformidad de la seguridad que resume los archivos de registro en un gráfico general. Mediante este panel de instrumentos puede obtener una visión general de las actividades de conformidad de seguridad, conocer las actividades de los usuarios y los eventos de seguridad en comparación con las infraestructuras reguladoras y de uso aceptable, y supervisar a los usuarios privilegiados y los eventos de seguridad.

## **Tivoli Security Compliance Manager**

Tivoli Security Compliance Manager (SCM) es un producto de conformidad de políticas de seguridad que le permite definir políticas de seguridad coherentes y supervisar la conformidad de las políticas de seguridad definidas.

Tivoli Security Compliance Manager ofrece políticas de seguridad como directrices para empezar a trabajar con el producto. Se puede modificar estas políticas de seguridad y se puede crear nuevas políticas.

Con las funciones de automatización y centralización de Tivoli Security Compliance Manager, se puede reducir el tiempo necesario para gestionar políticas de seguridad, establecer conformidades y realizar auditorías de seguridad:

- Tivoli Security Compliance Manager proporciona unas mejores prácticas para la conformidad de políticas de seguridad.
- Proporciona unas mejores prácticas de seguridad a través de la automatización y centralización.
- Establece fácilmente políticas de seguridad que pueden ayudar a cumplir con los estándares del sector y de la empresa.
- Se podrá modificar las políticas proporcionadas para satisfacer requisitos concretos.
- Se podrá identificar rápidamente si los sistemas operativos cumplen las políticas de seguridad.
- Disminuye los costes y ahorra tiempo al cambiar estos procesos manuales por exploraciones automáticas de sistemas y escritorios.

### **Sistemas Operativos y Plataformas de Hardware Apropriadas:**

AIX,  
HP-UX,  
Linux,  
Sun Solaris,  
Windows 2000,  
Windows 95/98,  
Windows NT,  
Windows XP.

## **Tivoli Security Information and Event Manager**

Solución de gestión centralizada de la seguridad y la conformidad que proporciona visibilidad del estado de la seguridad de la empresa.

IBM Tivoli Security Information and Event Manager V1.0 permite a las organizaciones de seguridad de IT obtener datos valiosos acerca de la seguridad a partir de los que tomar las medidas convenientes:

- Facilita la conformidad mediante paneles centralizados de herramientas y funciones de creación de informes.
- Protege la propiedad intelectual y la privacidad auditando el comportamiento de todos los usuarios, tengan o no privilegios.
- Gestiona eficazmente las operaciones de seguridad, ya que correlaciona los sucesos, les da prioridad, los investiga y responde a ellos, todo de forma centralizada.

IBM Tivoli Security Information and Event Manager V1.0 ofrece:

- Integración e intercambio de sucesos entre los motores de correlación de IBM Tivoli Security Operations Manager e IBM Tivoli Compliance Insight Manager.
- Nueva tarificación de punto final para la recopilación de registros de auditoría e incidentes de seguridad.

La gestión de los sucesos y la información de seguridad (SIEM) es una de las principales preocupaciones de los CIO y los CSO de la mayoría de las empresas. Existe la necesidad de centralizar los sucesos importantes para la seguridad y analizar los datos consolidados para obtener información útil acerca de la seguridad y la conformidad.

IBM ofrece dos propuestas complementarias de SIEM:

- Un panel de instrumentos de gestión centrada en los sucesos de la red en tiempo real que facilita la detección de ataques y la gestión de las incidencias de seguridad.

- Un panel de instrumentos de análisis de la información para supervisar hasta qué punto se adhiere una organización a sus políticas de gobierno y seguridad.

IBM Tivoli® Security Information and Event Manager V1.0 está formado por dos productos que trabajan de forma conjunta para ofrecer todas las ventajas de la SIEM empresarial: IBM Tivoli Security Operations Manager V4.1 e IBM Tivoli Compliance Insight Manager V8.5. Ahora, es posible centralizar la recopilación de registros y la correlación de sucesos en toda la empresa utilizando un panel avanzado de instrumentos de conformidad, así como informes que cumplen con la normativa, para aplicar las políticas corporativas a los sucesos de seguridad y al comportamiento de los usuarios.

Tivoli Security Information and Event Manager V1.0 constituye la base ideal desde la que responder a los requisitos de SIEM, tanto ahora como en el futuro. Así, permite a las organizaciones de IT minimizar la vulnerabilidad a las infracciones en la seguridad; controlar el coste de la recopilación, los análisis y los informes de sucesos relacionados con la conformidad, y gestionar la complejidad de las diversas tecnologías e infraestructuras. IBM Tivoli Security Information and Event Manager incluye funciones globales, tales como:

- Panel de instrumentos de conformidad con la seguridad.
- Panel de instrumentos de operaciones de seguridad para gestionar las incidencias de seguridad.
- Agregación de registros, correlación y análisis de las incidencias de seguridad.
- Integración de las operaciones de IT:
  - Detecta e investiga las incidencias y reacciona ante ellas automáticamente.
  - Agiliza el seguimiento, el manejo y la resolución de las incidencias.
- Análisis de auditoría del mainframe, el sistema operativo, las aplicaciones y las bases de datos.
- Supervisión y auditoría de los usuarios con privilegios (PUMA).
- Creación de informes de gestión de registros.

## Tivoli Federated Identity Manager

- ⇒ **Tivoli Federated Identity Manager:** Permite a las entidades empresariales establecer una colaboración segura. Ofrece un modelo sencillo para gestionar identidades y proporcionar acceso a los recursos.

Abarca empresas y dominios de seguridad para que las identidades puedan acceder a la información y a los servicios sin replicar la administración de identidades y seguridad de las dos empresas.

- Ofrece una gestión de la seguridad basada en las políticas para los servicios web federados en empresas que desplieguen arquitectura orientada a servicios (SOA) y servicios web.
- Facilita la administración y permite que las empresas amplíen la gestión de accesos e identidades a usuarios y servicios de otros proveedores, de forma que los clientes puedan controlar el acceso a las aplicaciones según su rol de usuario en la organización.
- Amplía el catálogo de gestión de servicios IT de IBM, con el que las empresas podrán reducir la complejidad tecnológica a través de la automatización y la integración de procesos.
- Ofrece una integración de la seguridad entre las nuevas aplicaciones distribuidas y las aplicaciones de mainframe existentes, como CICS.
- Mejora los controles de auditoría para los datos heredados y las transacciones recibidas que utilizan la arquitectura orientada a servicios (SOA) y los servicios web, y entrega control de acceso basado en roles para los nuevos servicios web.
- Aprovecha System z como plataforma de primera calidad para la entrega de aplicaciones a través de funciones nuevas de gestión de identidades, servicios web y auditorías.
- Integra silos empresariales, que facilitan las adquisiciones y fusiones y tratan la conformidad y el gobierno, para asegurar el éxito de los proyectos de SOA.
- Sistemas operativos admitidos: AIX, HP Unix, Linux, Windows, z/OS.

### **Novedades de Tivoli Federated Identity Manager V6.2**

IBM Tivoli Federated Identity Manager V6.2:

- Proporciona un soporte a la gestión de identidades centrada en el usuario, ya que ofrece soporte a Information Card Profile y OpenID para los roles de proveedor de identidades y de usuarios de confianza.
- Permite el despliegue modular de federación y la interoperatividad mediante la integración a la solución de gestión de accesos y los servidores de aplicaciones.
- Agiliza la gestión de la identidad de la arquitectura orientada a servicios (SOA), ya que proporciona un servicio de gestión fiable y conectable, basado en WS-Trust 1.3, para desplegar un bus de servicio empresarial de reconocimiento de identidades y una integración de CICS con RACF PassTicket.
- Amplía las auditorías y la creación de informes para la conformidad mediante:
  - La inclusión de BIRT (Business Intelligence Reporting Tool) 2.1.2 para crear informes nuevos y personalizados y para proporcionar
  - la capacidad de crearlos a través de la consola o la línea de mandatos de Tivoli Federated Identity Manager.
  - La integración con IBM Tivoli Compliance Insight Manager para la creación de informes de conformidad centralizados.

IBM Tivoli Federated Identity Manager Business Gateway V6.2 ahora da soporte a SAML 2.0.

IBM Tivoli Federated Identity Manager V6.2 for z/OS ahora da soporte al inicio de sesión único federado.

⇒ **Tivoli Federated Identity Manager Business Gateway**: Una solución básica para utilizar el inicio de sesión único federado y estándares abiertos. Establece funciones de inicio de sesión único (SSO) federado en la web.

Utiliza estándares abiertos para ofrecer un procedimiento sencillo de migración a una aplicación de ámbito empresarial de una sola aplicación fácil de desplegar.

- Creado especialmente para que organizaciones pequeñas y medianas conecten clientes, socios y proveedores.
- Ofrece un tiempo de lanzamiento al mercado rápido para las iniciativas de e-business a través del despliegue del SSO, que se logra mediante el acoplamiento débil entre software de federación y aplicaciones empresariales.
- Ofrece una aplicación ligera y fácil de desplegar para las necesidades del SSO más directas y para una integración simplificada con los socios en línea.
- Genera registros de auditorías, informes de incidentes y seguimiento, así como de las mejores prácticas en seguridad, para cumplir con las políticas de empresa y de conformidad con la normativa.

## **GESTIÓN DE ALMACENAMIENTO**


El software de almacenamiento gestiona y garantiza la accesibilidad, disponibilidad y rendimiento de la información almacenada.

**Tivoli Continuous Data Protection for Files**: garantiza la capacidad de recuperación mediante la creación automatizada continua, el seguimiento y vuelco de puntos de recuperación fiables para datos.

**Tivoli Storage Area Network Manager**: es una solución basada en normas estándar para gestionar redes de áreas de almacenamiento heterogéneas.

**Tivoli Storage Manager**: protege los datos de la empresa frente a anomalías de hardware y otros errores por medio del almacenamiento de copias de seguridad y copias archivadas de los datos en almacenamiento fuera de línea.

**Tivoli Storage Manager Extended Edition**: proporciona una gestión del almacenamiento de bajo coste para cualquier tipo de cliente.



**TotalStorage Multiple Device Manager:** proporciona dos funciones con precio diferente, Performance Manager y Replication Manager. Cada una de estas funciones se basa en un componente común llamado Device Manager, que está diseñado para centralizar la gestión de su infraestructura de almacenamiento SAN y el entorno de disco.

**TotalStorage Productivity Center for Data :** simplifica y automatiza la gestión de una infraestructura del almacenamiento de empresa a través de un conjunto centralizado de herramientas de disco, datos e infraestructura.

**TotalStorage SAN File System:** está diseñado para ser un sistema de archivos de alta disponibilidad para el almacenamiento conectado a SAN que proporciona la posibilidad de compartir archivos y una gestión centralizada del almacenamiento para servidores UNIX, Windows y Linux.

## **GESTIÓN DE SISTEMAS**

El software de gestión de sistemas se utiliza para supervisar, controlar y optimizar los recursos informáticos.

**Tivoli AF/REMOTE:** es una solución de automatización de salida para el acceso remoto seguro al mainframe y a los sistemas distribuidos independientemente de la ubicación.

**Tivoli Business Systems Manager:** proporciona un interfaz único y sencillo para consolidar la información de gestión en una vista basada en los negocios, que abarca todo el entorno, incluyendo los componentes distribuidos, Web y de macrocomputadoras.


**Tivoli Composite Application Manager for Response Time Tracking:** garantiza el rendimiento y la disponibilidad del comercio electrónico y las transacciones empresariales para los usuarios finales.

**Tivoli Configuration Manager:** es una solución integrada para implantar software y supervisar las configuraciones de hardware y software.

**Tivoli Editor for Messages on Distributed Systems:** es la herramienta de edición de mensajes basada en navegador para IBM WebSphere MQ Development y entorno de pruebas.

**Tivoli Enterprise Console:** identifica con rapidez la causa de los problemas de rendimiento empresarial.

**Tivoli ETEWatch Workstations:** representa una tecnología que mide el tiempo de respuesta global de nivel de transacción.



**Tivoli Intelligent ThinkDynamic Orchestrator:** capta, anticipa, planifica, y controla respuestas a los requisitos de producción en tiempo real. Asimismo, presenta otros beneficios, pues dirige flujos de trabajo de TI a fin de mantener automáticamente la disponibilidad del servidor y alcanzar los niveles de servicio requeridos.

**Tivoli IntelliWatch:** es una solución global de gestión de sistemas para Lotus Domino, que ofrece una gran gama de dispositivos que incluyen la detección y corrección automática de problemas, opciones de configuración del producto a nivel del sistema, funciones personalizadas de elaboración de informes y estadísticas y recuperación de anomalías.

**Tivoli License Manager:** es una potente herramienta para la gestión de licencias de software. Dispone de funciones avanzadas de inventario y de generación de informes que ayudan a las empresas a saber qué licencias de software poseen y cuáles pueden necesitar en el futuro.

**Tivoli Monitoring:** proporciona funciones de supervisión para los recursos esenciales del sistema a fin de detectar los cuellos de botella y los problemas potenciales, así como recuperarse automáticamente de situaciones críticas. Tivoli Monitoring ahorra a los administradores de sistemas la tarea de analizar manualmente grandes cantidades de datos sobre el rendimiento para poder resolver los problemas. Mediante prácticas recomendadas de la industria, Tivoli Monitoring puede ofrecer a la empresa una rentabilidad inmediata.

**Tivoli NetView:** es una solución de gestión de red que detecta redes TCP/IP, muestra topologías de red, correlaciona y gestiona eventos y capturas SNMP, supervisa el estado de la red y recoge información sobre el rendimiento.

**Tivoli OMEGAMON DE for Distributed Systems:** proporciona información de múltiples monitores en un único panel. Tivoli OMEGAMON DE for Distributed Systems es una herramienta de integración de gestión de sistemas para el personal y la gestión de IT, que necesitan comprender la repercusión en el negocio de los sucesos del sistema en su empresa.

**Tivoli OMEGAMON XE for Databaseses:** una solución global de rendimiento y disponibilidad diseñada para ayudarle a gestionar y ajustar de forma proactiva el entorno de la base de datos de su empresa para obtener un rendimiento óptimo. Su interfaz web proporciona una única interfaz a pantalla grande y con niveles granulares.

**Tivoli OMEGAMON XE for Distributed Systems:** ofrece un enfoque único de la gestión de empresas, una automatización avanzada de proactividad, especialmente importante cuando las estructuras IT se convierten en estructuras cada vez más heterogéneas y complejas.

**Tivoli OMEGAMON XE for R/3:** es un conjunto integrado de rendimiento para la gestión de SAP R/3 en la empresa.

**Tivoli OMEGAMON XE for WebSphere Application Server on Distributed Systems:** permite ver más allá de la caja de la máquina para descubrir rápidamente los problemas que pueden llevarle a perder negocio y clientes.

**Tivoli OMEGAMON XE for WebSphere Business Integration:** supervisa y gestiona los sistemas WebSphere MQ (WMQ) on Distributed y los entornos de WebSphere InterChange Server y WebSphere Business Integration Message Broker (WBI MB).

**Tivoli Provisioning Manager:** provee y configura servidores, sistemas operativos, dispositivos middleware, de aplicaciones y de red que actúan como direccionadores, conmutadores, cortafuegos y equilibradores de carga.

**Tivoli Remote Control:** es una solución de control remoto, su capacidad de ampliación a entornos de servidores y equipos de escritorio empresariales alcanza las decenas de miles de unidades y proporciona al departamento informático un control rápido, seguro y fiable de los recursos críticos.

**Tivoli Service Level Advisor:** analiza automáticamente los acuerdos de nivel de servicio y evalúa su cumplimiento, a la vez que utiliza el análisis predictivo para evitar los incumplimientos del nivel de servicio.

**Tivoli Switch Analyzer:** presenta un enfoque único e innovador a fin de suministrar una solución líder para la automatización de la correlación de eventos y el análisis de causas.

**Tivoli System Automation for Multiplatforms:** gestiona la disponibilidad de las aplicaciones de negocio, que se ejecutan en sistemas o clústeres únicos de AIX y Linux en zSeries, pSeries, iSeries y xSeries (u otros servidores basados en Intel), de acuerdo con los objetivos definidos por el cliente.

**Tivoli Universal Agent:** amplía la potencia de sus soluciones Tivoli OMEGAMON existentes en dispositivos y aplicaciones de red, componentes que son difíciles de gestionar. Esta función es básica al intentar gestionar la topología de aplicación global y el estado de los sistemas.

**Tivoli Web Response Monitor:** captura la experiencia del usuario final del rendimiento de aplicaciones basadas en web. Calcula los tiempos de respuesta de ida y vuelta, información del URL, tiempos de resolución y carga para objetos incrustados, entre otros.

**Tivoli Web Segment Analyzer:** calcula los tiempos de respuesta de transacción entre la red, lo que proporciona una supervisión en tiempo real no intrusiva del programa de fondo del cliente, y en cualquier etapa del proceso.

**Tivoli Workload Scheduler:** Gestiona las cargas de trabajo en los entornos informáticos complejos de hoy en día.

## LA SEGURIDAD PARA EL 2009

**A pesar del actual clima de recesión, la seguridad de la información sigue siendo una de las principales prioridades del panorama TI.**

Debido a la proliferación de amenazas y vulnerabilidades -que constituyen un riesgo permanente para la estabilidad de los sistemas- ocho tendencias probablemente marcarán la evolución de este mercado durante el presente año.

**1. Protección en el punto final:** Se considera seguridad en el punto final (endpoint security) al concepto en el que básicamente cada dispositivo o punto final es responsable de garantizar su propia protección frente a amenazas y vulnerabilidades.

En este sentido, los dispositivos finales están sufriendo una importante transformación: de incluir únicamente software antivirus, han pasado a combinarlo con herramientas firewall y anti-spyware. Además, este año ampliarán sus funciones antivirus con prevención de pérdida de datos y encriptación de disco.

**2. Seguridad ‘en la nube’:** Mientras la informática *cloud computing* redefine el segmento de software a través de una aproximación basada en la web, 2009 será probablemente un año marcado por los servicios de seguridad gestionada.

Esto se debe a que muchas empresas simplemente no cuentan con los fondos suficientes o la experiencia necesaria para enfrentarse a unas vulnerabilidades y ataques cada vez más sofisticados.

**3. Virtualización:** A medida que la virtualización servidor y del desktop continúan avanzando, los usuarios demandarán cada vez más medidas de protección para funciones como el control de acceso basado en roles, la gestión de identidades en servidores virtuales, la seguridad de red o la auditoría de sistemas virtuales.

VMware, Citrix y Microsoft, así como las distintas aplicaciones open source de virtualización para servidores y PCs liderarán esta tendencia, asociándose con partners del mundo de la seguridad y de las redes como IBM, McAfee, Cisco o CheckPoint.

**4. Políticas corporativas:** Todas las organizaciones, independientemente de su tamaño, deben ser capaces de descubrir y clasificar su información más sensible, aplicarle políticas de seguridad corporativas y trasladar estas políticas a la red, donde confluyen con partners y clientes.

Esta tendencia seguirá consolidándose durante 2009 a medida que a los documentos y archivos con información corporativa se añaden nuevas medidas

de protección como la prevención frente a la pérdida de datos y sistemas de gestión de derechos de acceso, sin olvidar las transacciones electrónicas garantizadas mediante encriptación PKI (Infraestructura de Clave Pública).

**5. Encriptación omnipresente:** Las tecnologías de encriptación se han añadido de golpe a los sistemas de almacenamiento de información. Así, tanto cintas como discos duros de fabricantes como Hitachi, Fujitsu o Seagate cuentan ahora con procesadores criptográficos.

Igualmente, Intel ha anunciado el lanzamiento en 2009 de una versión de su chip vPro con soporte integrado de encriptación. Siguiendo esta tendencia, en el presente ejercicio probablemente se verán múltiples capas de tecnologías de encriptación aplicándose a todo tipo de dispositivos, generando una demanda paralela de herramientas de administración para todas ellas.

**6. Gestión de derechos:** Mientras los mecanismos de autenticación permiten la entrada de los usuarios a la red, la gestión de derechos estipula lo que dichos usuarios pueden o no hacer. Durante 2009, los mecanismos de gestión de derechos se extenderán y ganarán en escalabilidad, con ofertas de actores como Cisco, IBM-Tivoli o RSA y estándares respaldados por el consorcio Oasis del tipo XACML (XML Access Control Markup Language).

**7. Mayor visibilidad:** Al igual que los CIOs están cada vez más presentes en los consejos directivos de las empresas, los responsables de negocio demandan herramientas de control y visibilidad que les permitan conocer el estado de protección de su negocio.

No les bastará con recibir informes superficiales, sino que durante este año reclamarán acceso a portales de control especializados o herramientas estadísticas más sofisticadas. De producirse, sería bueno tanto para la seguridad en sí misma -apoyada con mayor inversión- como para las grandes consultoras como Accenture, CSC, IGS BM Global Services o HP.

**8. Estandarización:** Durante el pasado año, la gran mayoría de los ataques de código malicioso se dirigieron a las aplicaciones, no a los sistemas operativos.

Este hecho, unido al creciente foco en ciberseguridad, motivará que las compañías que diseñan programas de software se unan a programas de desarrollo coordinados y basados en estándares y mejores prácticas.

El consorcio Open Web Application Security Project (OWASP) o el Software Security Institute (SANS) son algunos ejemplos de organismos de coordinación internacionales con este fin.

## **NOVEDADES DE IBM TIVOLI SECURITY OPERATIONS MANAGER (TSOM) V4.1**

IBM Tivoli Security Operations Manager (TSOM) V4.1 ofrece funciones nuevas y mejoradas para gestionar con más eficacia las incidencias de seguridad de IT:

- Administración y configuración simplificadas y más eficaces: mejoras en la utilización para reducir el tiempo y el esfuerzo de los despliegues, y administración mediante una interfaz de dispositivo centralizada y simplificada, además de una nueva función de configuración automática de origen de sucesos.
- Filtro de sucesos mejorado e infraestructura de motor de correlaciones con más flexibilidad, funciones y rendimiento.
- Operaciones de seguridad mejoradas, interfaz de usuario de consola, con más recursos de la base de conocimiento de seguridad y más capacidad de personalización.
- Gestión ampliada de casos e incidencias.
- Herramienta de análisis de hosts mejorada para la identificación y la resolución de incidencias.
- Soporte a plataformas ampliadas y actualizadas, incluidas DB2, AIX y un soporte global a la internacionalización y la globalización.
- Se integra con Tivoli Compliance Insight Manager para proporcionar una solución integral para la información de seguridad y la gestión de sucesos (SIEM).

Para los directores de los servicios de información de la mayoría de las empresas o portadoras, la seguridad de la información representa una de las mayores preocupaciones, ya que la disponibilidad de redes y recursos constituye la garantía de los negocios y los servicios. Las empresas, las instituciones públicas y los proveedores de servicios pueden sufrir pérdidas millonarias a causa de "gusanos" y otro tipo de malware que infectan los recursos corporativos y los servicios al cliente.

Para maximizar la disponibilidad de los servicios y recursos y proteger la información de los clientes, un equipo de información debe ser capaz de:

- Detectar y manejar con rapidez las incidencias de seguridad.
- Aplicar las políticas de seguridad.
- Dar soporte a las iniciativas de auditoría y conformidad.

Todas estas acciones comprenden datos de seguridad de toda la empresa. Las empresas y los proveedor de servicios deben acceder a estos datos por separado y analizarlos rápida y eficazmente, y todo ello en entornos de múltiples proveedores tan complejos como los de hoy en día que necesitan una solución automática e integrada.

IBM Tivoli Security Operations Manager (TSOM) es una plataforma de gestión de sucesos e información que contribuye a superar los retos que suponen las operaciones de seguridad. TSOM está diseñado para mejorar la eficacia y la visibilidad de la gestión de riesgos de la información y las operaciones de seguridad. Asimismo, centraliza y almacena los datos de seguridad de toda la infraestructura de tecnología, de forma que:

- Automatiza el análisis, la correlación y la agregación de registros.
- Detecta, investiga las incidencias y reacciona ante ellas automáticamente.
- Agiliza el manejo y el seguimiento de las incidencias.
- Permite la supervisión y la aplicación de las políticas.
- Ofrece la creación de informes a efectos de conformidad.

## CONCLUSIÓN

Tivoli provee la visibilidad, el control y la automatización necesarios para proveer servicios de calidad, administrar riesgos y cumplimiento, maximizar el retorno sobre las inversiones y acelerar el crecimiento del negocio:

- **Administración de activos:** Logra una mayor eficiencia en la administración de activos administrando todos los tipos de activos en una única plataforma.
- **Seguridad:** El software de seguridad se utiliza para proteger la confidencialidad, integridad, privacidad y seguridad de los sistemas de TI.
- **Administración de almacenamiento:** El software de almacenamiento gestiona y garantiza la accesibilidad, disponibilidad y rendimiento de la información almacenada.
- **Administración de sistemas:** El software de gestión de sistemas se utiliza para supervisar, controlar y optimizar los recursos informáticos.
- **IT Service Management:** Innovación, ejecución y liderazgo para que las empresas optimicen y controlen el negocio de IT.
- **Soluciones de proveedores de servicios:** Asegura que los servicios críticos están ejecutándose en conformidad con los estándares más elevados.

Mediante una combinación de productos de seguridad de IBM, se podrá gestionar toda la empresa de manera coordinada, repetible y auditable, lo que sirve de ayuda para aumentar la productividad y disminuir el coste total de la gestión. La suite de productos de seguridad IBM Tivoli pretende ayudar a ejecutar los procesos del negocio en las plataformas que se elija, mientras se gestiona la seguridad de toda la empresa, para facilitar la transición del negocio al entorno On Demand.



## **BIBLIOGRAFÍA**

### **Paginas Webs:**

- Material referido a la familia de productos Tivoli, extraído del Sitio Web del IBM Scholar Program.
- Fundación Telefónica.
- IBM.
- <http://www-01.ibm.com/support/docview.wss?uid=swg21377388>