Software IBM
Sistemas de seguridad de IBM

Gestione identidades y el acceso para una continua conformidad y una reducción de riesgos

Administre, controle y supervise el acceso de los usuarios a recursos, aplicaciones e información

IBM

Destacados

- Valida la autenticidad de todos los usuarios que acceden a los recursos.
- Supervisa que el acceso del usuario siga las políticas apropiadas de uso y que exista coherencia con las reglamentaciones.
- Toma acciones correctivas cuando se producen violaciones
- Proporciona responsabilidad y transparencia a las titularidades de los usuarios durante todo el ciclo de vida del usuario
- Permite auditorías constantes de la actividad del usuario para hacer cumplir las políticas y ayudar a la conformidad.

Debido a que las organizaciones se esfuerzan por brindar, de manera segura, servicios de alta calidad y alta disponibilidad a sus comunidades de usuarios, estas lidian con el control de costos y las poblaciones, puntos de acceso y aplicaciones de usuarios en constante cambio. Pero eso es solo una parte del desafío más grande relacionado con la gestión de identidades y acceso (IAM). Los servicios deben brindarse sólo a las personas indicadas, con los privilegios adecuados, ya sean empleados, proveedores, socios o clientes. Esto se está convirtiendo en parte aún más importante y más difícil de lograr.

Las reglamentaciones de conformidad tales como Sarbanes-Oxley, Basel II, Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Model Audit Rule (MAR) y Payment Card Industry Data Security Standard (PCI/DSS) hacen hincapié en la importancia de la visibilidad y el control de los derechos de los individuos y los privilegios de acceso. Simultáneamente, los avances en la computación lo hacen más difícil, incluyendo:

- El crecimiento explosivo de datos estructurados y no estructurados
- El acceso a la información general.
- El crecimiento de colaboración basada en Internet y computación en nube más enriquecida

La complejidad de IAM y la presión de riesgo y conformidad demandan un nuevo enfoque y las soluciones para hacer de este acercamiento una realidad. Lo que las organizaciones requieren es un impulso por las políticas de gestión de IAM que mejoren la visibilidad, el control y la automatización para proteger los activos de los accesos no autorizados sin disminuir la productividad.

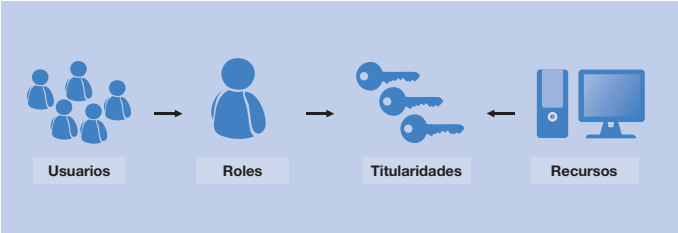

Figura 1: La gestión de IAM ayuda a proporcionar los recursos adecuados a las personas adecuadas con los privilegios adecuados.

Establecimiento de la primera línea de defensa de la empresa con la gestión de IAM

La gestión de IAM es parte de la primera línea de seguridad empresarial. Es la tecnología fundamental para determinar quién tiene acceso autorizado, para qué recursos, con qué propósito y por cuánto tiempo. Además de las tecnologías y las políticas de concesión, actualización y eliminación del acceso, La gestión de IAM también incluye las herramientas para supervisar, auditar e informar sobre lo que los usuarios hacen con sus derechos de acceso. Sin la gestión de IAM , otras tácticas de seguridad, como la administración de titularidades, la prevención de desperdicio de datos y la detección de fraude pueden tener poco o ningún punto de referencia para hacer cumplir la política de acceso. La gestión de IAM también es una parte fundamental del impulso para optimizar la protección de la empresa con inteligencia de seguridad.

La mayoría de las organizaciones han invertido en herramientas y técnicas de seguridad. Pero las defensas en capas no son lo mismo que construir una inteligencia de seguridad en su entorno. ¿Qué hay de un enfoque proactivo a la seguridad que integre el control del riesgo en su propia estructura? La gestión de identidades y acceso de IBM puede ayudar a responder a estas preguntas y a proporcionar un valor más allá de solo el control de riesgo, con la responsabilidad y la transparencia a las titularidades de usuarios durante todo el

ciclo de vida del usuario. Cuando la administración de identidad se encuentra directamente integrada con los objetivos y las prioridades de la empresa, la TI puede proporcionar servicios más optimizados al individuo lo que permite a la empresa sacar provecho de las oportunidades. Las soluciones de gestión de IAM también pueden mejorar otras tecnologías de control de políticas y seguridad y contribuir a una administración de seguridad integral.

La gestión de IAM describe cómo las organizaciones administran, aseguran y monitorean identidades y derechos de acceso a aplicaciones, información y sistemas. Extiende, además, el valor proporcionado por las funciones principales de administración de acceso e identidad tales como el aprovisionamiento de usuarios, la gestión de acceso web y la infraestructura de directorio. Las soluciones de gestión de IAM descubren, analizan y establecen el acceso de usuarios a partir de la utilización de flujos de trabajo, herramientas y análisis de informes. Esto crea un proceso para la gestión de acceso del usuario en el que las restricciones de titularidad ayudan a gestionar conflictos empresariales. La gestión de IAM incluye las siguientes prácticas:

- Administración del ciclo de vida del usuario (aprovisionamiento y desabastecimiento de usuarios)
- Administración de contraseñas e inicio de sesión único (SSO) a aplicaciones (incluidas las opciones de autoservicio para reducir el volumen de llamadas al servicio de asistencia)
- Administración de roles (asignación de usuarios a roles según la función del trabajo y las necesidades de la empresa y la administración de la separación de conflictos de obligación)
- Políticas de certificación que establecen un proceso de revisión regular y validan que el acceso de usuario permanezca apropiado
- Administración de acceso (implementación de acceso basado en política para usuarios internos y externos que incluyen asociados de negocios y proveedores de servicios de terceros)
- Administración de titularidad (implementación de acceso a aplicaciones y servicios basados en roles, reglas y atributos refinados)
- Auditorías e informes constantes para supervisar la actividad de los usuarios, hacer cumplir políticas y ayudar a la conformidad

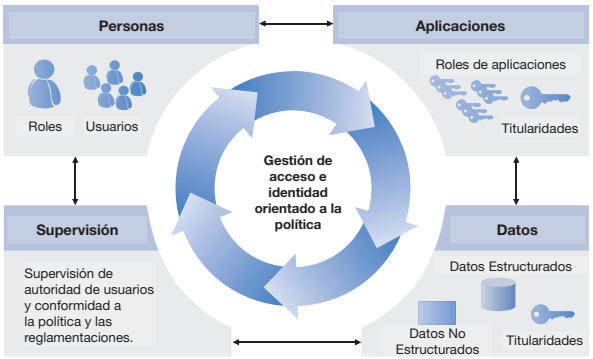

Figura 2: IBM proporciona un abordaje a la gestión de IAM orientado a la política.

Facilitar la coherencia y el cumplimiento de un enfoque basado en políticas para IAM.

El control del acceso a los datos y a las aplicaciones es fundamental teniendo en cuenta las preocupaciones de seguridad y privacidad crecientes y una concentración permanente en la conformidad y la supervisión empresarial. Las organizaciones deben probar que poseen controles de acceso fuertes y coherentes. También desean asegurarse de que las decisiones tomadas sobre las titularidades de usuarios estén alineadas con las políticas y objetivos de la empresa. La gestión de IAM de IBM ofrece recursos para administrar requisitos de acceso de usuarios específicos de la empresa con gran responsabilidad y transparencia, ayudando a gestionar y hacer cumplir el acceso de usuario, de una manera más efectiva. El acercamiento orientado a la política de IBM para administrar personas, aplicaciones y datos proporciona la consistencia y amplitud necesarias para una gestión de IAM efectiva y también ayuda a facilitar la conformidad.

IBM guía a los clientes a través de un enfoque probado orientado a la política que incluye cinco fases del ciclo de vida de administración de acceso e identidad, incluidos:

- Definición de controles
- Inscripción y prueba de usuarios
- Emisión y administración de derechos de usuario

- Administración e implementación del control de acceso
- Monitoreo, auditoría e informes sobre actividades y derechos de usuario.

Cada una de estas fases proporciona una oportunidad para que los clientes generen un valor empresarial de las soluciones de gestión de IAM de IBM al mejorar el servicio, reducir costos y administrar el riesgo. Las soluciones de gestión de IAM de IBM ayudan a proporcionar un acceso eficiente y de conformidad a los recursos adecuados, en el tiempo adecuado, a las personas adecuadas. Lo hacen al agilizar la autenticación de usuarios, al optimizar el acceso a la aplicación y al gestionar las actividades de aprovisionamiento y desabastecimiento de usuarios. Los clientes pueden aprovechar la profunda experiencia en seguridad de IBM para crear una solución de IAM completa que de soporte y mejore otros componentes de seguridad e impulse la eficiencia en áreas problemáticas tales como la conformidad, las políticas de uso y los informes. Al simplificar la administración del ciclo de vida del usuario y ofrecer una mejor visibilidad de titularidad de usuarios, la gestión de la Administración de Acceso e Identidad de IBM pueden ayudar a maximizar la productividad del personal de TI y reducir el costo y la complejidad de la seguridad y la conformidad.

Figura 3: Un plan de gestión de IAM viable requiere un proceso de ciclo cerrado de varios pasos.

Exploración de soluciones de IBM para la gestión de IAM

Las reglamentaciones de conformidad están llevando a las organizaciones a adoptar una tecnología IAM basada en la necesidad de probar la responsabilidad de acceso y administración de datos. IAM también puede ayudar a prevenir fraudes y a mejorar la eficiencia operativa. La administración de acceso e identidad coherente ayuda a proteger la identidad de datos y a facilitar la conformidad, incluso con las complejidades de comunidades de usuarios basadas en la nube, grandes almacenamientos de datos y mejor movilidad. Las soluciones de gestión de IAM de IBM proporcionan a los usuarios el acceso autorizado a los recursos que necesitan para hacer su trabajo a la vez que protegen las aplicaciones y los datos. Las soluciones de IBM para la gestión de IAM incluyen:

Identity Management

Identity management es el proceso de administración de la información utilizado para identificar a los usuarios, controlar el acceso del usuario, determinar los privilegios de usuario y delegar autoridades administrativas. Cuando se trata de los usuarios finales, no todos son iguales. Los ciclos de vida de los usuarios están en movimiento constante ya que los roles y responsabilidades de las personas cambian a menudo. Cuando a los empleados se les da nuevas responsabilidades o se los transfiere dentro de la organización, se deben revisar, aprobar y actualizar sus privilegios de acceso y los privilegios de acceso anteriores se deben suspender o eliminar potencialmente. Los perfiles de acceso de cliente también pueden evolucionar. Por ejemplo, los vendedores o inversionistas de valores de un sitio de subastas que alcanzan un determinado volumen de comercio necesitan que sus perfiles y autorizaciones se actualicen sin problemas.

La rapidez de la autorización es tan importante como la precisión. Los nuevos empleados pueden permanecer ociosos hasta que puedan acceder a las aplicaciones de correo electrónico o de la empresa. Las comunidades de clientes y usuarios basadas en la nube también demandan un acceso inmediato a los recursos.

Las políticas de seguridad son dinámicas también, así que las soluciones de administración de identidad deben incluir herramientas que simplifican la creación de políticas y permiten a los administradores evaluar el impacto potencial de los cambios de política sin introducirlas a un entorno de producción. La conformidad y la supervisión requieren la capacidad de administrar datos de identidad y acceso. Los informes predefinidos y eventos de auditoría deben ayudar a los auditores a obtener rápidamente una visión exacta de la postura de seguridad y el estado de conformidad de una organización.

Con su capacidad de proporcionar una administración de roles y usuario basada en políticas a través de la infraestructura de TI, Tivoli Identity Manager es un impulsor clave de la gestión de identidad y acceso. Tivoli Identity Manager ayuda a automatizar la creación, modificación y terminación de los privilegios de usuarios en todo el ciclo de vida del usuario. Proporciona capacidades como auto cuidado de usuarios, aprovisionamiento y desabastecimiento de cuentas de usuarios y recertificación de cuentas. Su recurso modelador de rol y política ofrece una gestión integral del ciclo de vida con la minería y modelado de rol, la separación de funciones y capacidades de gestión de grupos, junto con la posibilidad de simular diferentes escenarios de acceso.

Access Management

Access management es la capacidad de administrar conjuntos coherentes de políticas de control de acceso en línea con las políticas de seguridad y reglamentaciones de conformidad a través de sistemas de empresas, incluso la administración, supervisión y conformidad de políticas.

Las soluciones de Access management administran el acceso diario de las personas autorizadas a los recursos. Las soluciones efectivas integran políticas formales de seguridad en el flujo de trabajo de la administración de acceso para automatizar la administración del acceso a los sistemas operativos, redes, servidores, dispositivos de almacenamiento, bases de datos, aplicaciones de escritorio, sistemas de comercio en línea y aplicaciones empresariales. Access management también unifica los nombres de usuario y contraseñas que los usuarios suelen tener para los diversos recursos y aplicaciones en una sola, autenticación y procesos de autorización con seguridad mejorada normalmente a través de la utilización de tecnología de inicio de sesión único (SSO).

Las ofertas de Access management aplican políticas de acceso en todo el ciclo de vida del usuario al autenticar y aprovisionar el acceso a los usuarios autorizados a través de múltiples entornos y dominios de seguridad, a la vez que aplica políticas de seguridad y protección contra las amenazas internas y externas. Los productos de Access management de IBM ayudan a soportar la ejecución coherente de las políticas de seguridad a través de aplicaciones y usuarios múltiples. Permiten que el SSO mejore la experiencia del usuario y reduzca los costos del servicio de asistencia. También pueden proporcionar la administración de titularidad y cumplimiento de acceso refinados. Los productos de Access Management de IBM incluyen:

- IBM Tivoli Access Manager para e-business actúa como el centro para la autenticación y autorización para aplicaciones web y de otro tipo, centralizando la administración del acceso y haciéndolo más fácil y rentable para desplegar aplicaciones seguras de manera efectiva.
- IBM Security Access Manager para Enterprise Single Sign On: simplifica, fortalece y hace un seguimiento de acceso mediante la integración de Enterprise Single Sign-on con una autenticación fuerte, una automatización de flujo de trabajo de acceso, cambio de usuario y presentación de informes de auditoría rápidos.
- IBM Tivoli Federated Identity Manager: proporciona un inicio de sesión único federado, centrado en el usuario para compartir información de forma segura entre asociados confiables y para simplificar la integración de aplicaciones con el uso de estándares abiertos para SOA e implementaciones de servicios web a través de portales distribuidos y entornos de mainframe.
- Tivoli Security Policy Manager: centraliza la administración de políticas de seguridad y de control de acceso refinado de datos para aplicaciones, bases de datos, portales y servicios.
- QRadar Security Intelligence Platform: ofrece una arquitectura unificada para la recolección, almacenamiento, análisis y consulta de datos de registro, amenazas, vulnerabilidad y riesgos relacionados para ayudar a proteger contra las amenazas internas y controlar el costo de demostrar conformidad.
- Conjunto IBM Security zSecure: mejora la capacidad de las organizaciones para facilitar la conformidad con la seguridad, supervisar y auditar incidentes, y automatizar tareas administrativas de rutina para el mainframe.

Security Identity y Access Assurance de IBM

IBM ofrece una solución de software en grupo para ayudar a simplificar la administración de identidades y hacer cumplir las políticas de acceso en todo el ciclo de vida del usuario. Esta solución también incluye la administración de registro y control de usuarios privilegiados para mejorar la detección de amenazas, mejorar las capacidades de auditoría y facilitar las iniciativas de conformidad.

Los servicios IBM Identity and Access Management son una cartera completa de capacidades que cubre prácticamente todos los aspectos de la gestión de identidades, desde las pruebas de identidad, el aprovisionamiento de usuarios, al control de acceso.

Las ofertas de gestión de IAM de IBM son parte de un acercamiento integral que ayuda a cumplir con los requisitos de seguridad y negocios importantes, incluyendo:

- Descubrimiento, documentación y análisis de acceso de usuarios
- Establecimiento de un proceso para la gestión del acceso de usuario
- Aseguramiento de que las limitaciones ayudan a gestionar conflictos empresariales
- Hacer cumplir políticas de una manera centralizada y controlada
- Conducción del flujo de trabajo, tareas y automatización del proceso
- Monitoreo, informes y auditoría para ayudar asegurar el acceso apropiado y facilitar la conformidad

Logro de beneficios tangibles con soluciones de gestión de IAM de IBM

Un enfoque basado en políticas, con el uso de las soluciones de gestión de IAM adecuadas, proporciona la visibilidad necesaria de control y la automatización para la administración requisitos de acceso de los usuarios específicos de los negocios con una mayor responsabilidad. Los siguientes clientes de IBM se han beneficiado de este enfoque en términos de racionalización de la eficiencia de TI, la mejora de la seguridad y la reducción de riesgo y la facilitación de la conformidad.

Banco latinoamericano

Un banco brasileño ofrece créditos de nómina y soluciones de crédito a más de 100.000 clientes desde numerosas oficinas y más de 1.000 puntos de venta. Con un variado conjunto de normas de seguridad y procedimientos de inicio de sesión a través de docenas de aplicaciones, el personal luchaba por asegurarse de que a sus empleados se les proporcione un acceso adecuado y rápido y para demostrar el cumplimiento de las normas regulatorias brasileñas.

Esta solución garantiza que los usuarios tengan acceso a las aplicaciones apropiadas y proporciona acceso simplificado a los recursos de TI. Ahora, el personal y los agentes pueden iniciar sesión en la red del banco una vez y obtener acceso inmediato a todas las aplicaciones para cuyo uso están autorizados. Anteriormente, los usuarios tenían que iniciar sesión por separado en unas 15 a 30 aplicaciones diferentes para construir un paquete crediticio de un cliente. Cuando los empleados dejan la empresa o los roles agentes cambian, el equipo de seguridad puede acceder inmediatamente para desabastecer todos los sistemas con solo pulsar unas teclas para mantener los datos del banco seguros.

Como resultado, el banco redujo los costos de servicio de asistencia en aproximadamente R$ 32.000 (US$ 20.000) por año. También disminuyó el tiempo para aprovisionar a los usuarios nuevos desde un máximo de cinco días a tan solo dos horas y para restablecer las contraseñas de cuatro horas a segundos. La seguridad del sistema se ha mejorado a través del desabastecimiento rápido de usuarios cuando sea necesario, lo que también permite que el equipo de seguridad de soporte a nuevos proyectos sin necesidad de contratar personal adicional.

Ciudad europea

Una ciudad checa tiene una historia rica y se ha convertido en un creciente centro comercial y turístico. Garantizar la seguridad de TI integral para una ciudad en crecimiento requiere la automatización y centralización inteligente de muchos procesos, incluidas la supervisión y la prevención de acceso no autorizado a los sistemas informáticos de la ciudad.

La ciudad ha puesto en marcha un sistema de administración de identidad basado en normas que automatiza el acceso a cuentas de empleados según la posición del empleado, su función y departamento. Entonces, el sistema utiliza un proceso de reconciliación de cuentas automatizado para detectar y corregir (o eliminar) las cuentas que no cumplan con las reglas predefinidas. Un proceso de reconciliación de circuito cerrado identifica las cuentas “huérfanas” o fuera de fecha y elimina automáticamente el acceso a la cuenta cuando un empleado se va. La ciudad ahora puede estar segura de que los empleados que necesitan acceder a las cuentas lo hagan de forma rápida y eficiente, mientras que la seguridad de sus sistemas de TI está asegurada.

El cliente implementó un sistema de administración de identidad integrado y una solución de inicio de sesión único de IBM para reforzar la seguridad al tiempo que simplifica el acceso a la información.

Las ventajas de la solución incluyen:

- Un 100 por ciento de mejora en la rapidez de activación de los nuevos empleados; los nuevos empleados son productivos con acceso a todos los sistemas en un par de horas en lugar de varios días.
- Eficiencia administrativa mejorada y costos más bajos; un empleado de tiempo completo ahora puede administrar todas las cuentas de usuario, mientras que el resto del personal de TI desarrollar y mejorar el entorno de TI de la organización.
- Sistema de seguridad mejorado mediante la eliminación de las cuentas huérfanas y desactivación de cuentas de los empleados dentro de unas pocas horas de la terminación del empleo.

Agencia de servicios sociales de Sudamérica

En Uruguay, se puso en marcha un emocionante programa piloto que permite a los hospitales notificar a la seguridad social del gobierno y a las agencias de servicios sociales en línea cuando nace un niño. Se trata de una serie de programas de gobierno electrónico que el país está poniendo en marcha para sustituir los procesos basados en papel y proporcionar una mayor eficiencia y transparencia. Cerca de 50.000 empleados públicos y dos millones de ciudadanos utilizarán estos servicios en línea, en última instancia.

Al trabajar con IBM y con un Asociado de Negocios IBM, la organización ha implementado una arquitectura multinivel que proporciona una solución de seguridad integral para sus servicios de gobierno electrónico y que aborda la seguridad de transporte, el control de acceso y la administración de identidad. Para mantener la confidencialidad y la integridad de los servicios web IBM WebSphere DataPower Integration Appliance actúa como el punto de integración de la aplicación de políticas, que reciben las políticas desde IBM Tivoli Security Policy Manager. Tivoli Federated Identity Manager emite señales de seguridad para confirmar que los individuos que aleguen enviar un mensaje sean quienes dicen ser. IBM Tivoli Access Manager para e-business proporciona la autenticación centralizada, gestión de políticas y servicios de control de acceso para que los ciudadanos y empleados públicos accedan de manera rápida y segura a los servicios en línea. IBM Tivoli Directory Server e IBM Tivoli Identity Manager proporcionan los datos de identidad de confianza para apoyar el proceso de autenticación a través de todos los servicios web.

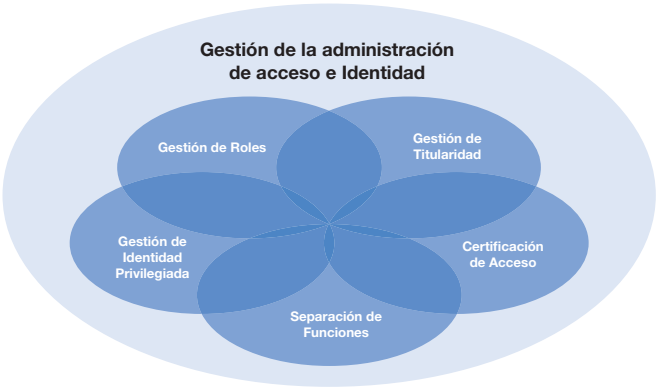

Figura 4: Basadas en las prioridades del negocio, las organizaciones deben comenzar con un subsegmento de la gestión de la identidad, como se muestra aquí y , a continuación, desarrollar un plan completo de gestión para IAM.

Primeros pasos para la mejora de la seguridad y la eficacia empresarial con la gestión de IAM

A medida que los obstáculos regulatorios se multiplican, los volúmenes de datos se expanden y los negocios sociales continúa transformando los requisitos de acceso, las soluciones de gestión de IAM son cada vez más importantes para la seguridad del día a día de una organización y operaciones de negocio, así como los esfuerzos constates de conformidad. Con un enfoque estratégico orientado a la política, la administración de acceso e identidad puede ayudar a responder a los cambios, reducir los costos de administración y proteger sus más valiosos activos de información.

Teniendo en cuenta estos factores, no es sorprendente que IAM se haya trasladado desde la periferia a la vanguardia de las prioridades de TI. Las soluciones de IBM para la gestión de IAM están ayudando a los clientes a conseguir una gran variedad de beneficios de seguridad orientados a los negocios, entre los que se incluyen:

- Una postura de conformidad mejorada con vistas centralizadas y procesos de negocio para la verificación de la identidad y la concesión de derechos de acceso.

- Costos reducidos derivados de la puesta de soluciones separadas, soluciones de administración de identidad personalizadas.
- Seguridad mejorada y costos reducidos que son el resultado menos cantidades de inicios de sesión y credenciales de los empleados.
- Productividad mejorada, la reducción de los costos de servicio de asistencia y mayor satisfacción del cliente o empleado a través de inicio de sesión único (SSO) experiencias y aprovisionamiento de acceso a pedido.
- Flexibilidad empresarial mejorada como resultado de un menor tiempo de salida al mercado y una infraestructura de seguridad centralizada estandarizada.
- Vistas centralizadas de auditoría de eventos de autorización de tiempo de ejecución, lo que permite una detección más fácil de comportamiento malicioso.

¿Por qué IBM?

La gestión de administración de acceso e identidad coherente protege la integridad de los datos y facilita la conformidad. IBM es un líder reconocido en el espacio del mercado mundial de IAM, con una perspectiva global y la comprensión de las necesidades regionales en constante evolución en todos los sectores. Además, IBM es reconocida por los analistas y la comunidad de seguridad de la excelencia solución, con las clasificaciones de los analistas de "líder" en varios informes diferentes y el reconocimiento como Mejor 2011 solución de administración de identidad por la revista Computing SC. Muchos proveedores de IAM ofrecen solo partes de una solución de gobernanza completa de IAM, exigiendo a los clientes el despliegue y gestionar los productos por separado de varios proveedores. Pero IBM ofrece un extenso conjunto integrado de software de gestión de identidad y acceso y servicios que pueden soportar entornos de terceros como Oracle, Microsoft y SAP.

Para más información

Para obtener más información acerca de IBM Security Systems, por favor póngase en contacto con su representante de ventas de IBM o Asociado de Negocio IBM, o visite la siguiente página web: **ibm.com**/security

Además, las soluciones de financiamiento de IBM Global Financing pueden permitir una gestión de dinero efectiva, protección de la obsolescencia de la tecnología, una mejora del costo total de propiedad y el retorno de la inversión. Asimismo, nuestros servicios Global Asset Recovery Services le pueden ayudar a hacer frente a los problemas ambientales con nuevas soluciones que hacen un uso eficiente de la energía. Para más información acerca de IBM Global Financing, visite: **ibm.com**/financing

IBM de Colombia S.A.
Cra 53 No. 100 - 25
Bogotá – Colombia

IBM de México S.A.
Alfonso Nápoles Gandara 3111
Col. Parque corporativo de Peña Blanca
C.P. 01210
México D.F

La página de presentación de IBM puede encontrarse en **ibm.com**

IBM, el logotipo IBM, ibm.com y X-Force son marcas registradas de International Business Machines Corporation en los Estados Unidos, otros países, o ambos. Si estos y otros términos de marcas registradas de IBM están marcados en su primera aparición en esta información con un símbolo de marca registrada (® o ™), estos símbolos indican marcas registradas en EE.UU. o ley común de propiedad de IBM al momento que esta información fue publicada. Dichas marcas registradas también pueden estar registradas o ser marcas de derecho consuetudinario en otros países. Una lista actual de las marcas registradas IBM se encuentra disponible en la web en "Copyright and trademark information" en: **ibm.com**/legal/copytrade.shtml

Otros nombres de empresas, productos o servicios pueden también ser marcas registradas o marcas de servicios de terceros.

Las referencias en esta publicación a productos y servicios IBM no implican que IBM pretenda colocarlos disponibles en todos los países en los cuales IBM opera.

La información del producto ha sido revisada para asegurar su exactitud a la fecha de la publicación inicial. La información del producto queda sujeta a cambios sin aviso previo. Cualquier declaración respecto de futuras indicaciones e intenciones de IBM están sujetas a cambio o cancelación sin previa notificación y representan solamente metas y objetivos.

El cliente es responsable de asegurar la conformidad con las exigencias legales. Es la responsabilidad exclusiva del cliente obtener asesoría legal competente sobre la identificación e interpretación de cualquier ley relevante y las exigencias obligatorias que puedan afectar el negocio del cliente, y cualquier acción que el cliente deba tomar para cumplir con dichas leyes. IBM no proporciona asesoría legal o representación o autorización de que sus servicios o productos asegurarán que el cliente esté en conformidad con cualquier ley o reglamento.

© Copyright IBM Corporation 2012

Por favor, recicle

WGB03002-ESLA-00