

RESUMEN SOBRE LA SOLUCIÓN

Administración de identidades y accesos basada en contenido | Febrero de 2012

¿De qué modo la Administración de identidades y accesos basada en contenido puede darme el control que necesito para impulsar mi negocio con confianza?

agility
made possible™



+

Las soluciones de Administración de Identidades y Accesos basada en contenido de CA Technologies le permiten controlar las identidades, los accesos del usuario y el uso de la información. Puede lograr un cumplimiento más eficaz, reducir el riesgo de TI y expandir las relaciones con clientes y socios de negocios para impulsar el crecimiento de su negocio.

+

resumen

Desafío

Administrar las identidades y los derechos de acceso de las personas internas de la empresa y las externas a ella se ha convertido en una preocupación primordial de las organizaciones de TI en la actualidad. **La reducción del riesgo de TI**, el cumplimiento de los requisitos legales y el incremento de las eficiencias son todos aspectos centrales para su negocio. Al mismo tiempo, necesita desarrollar formas nuevas e innovadoras de expandir el negocio y de aprovechar los nuevos modelos de servicio, como la computación en la nube.

Oportunidad

La IAM basada en contenido de CA Technologies es una solución integral y escalable para administrar identidades de usuarios, el acceso y el uso de la información. **Protege sus recursos de TI importantes, desde la Web al mainframe, incluyendo los entornos virtualizados y de nube.** Proporciona también la automatización de los controles de seguridad y cumplimiento, lo que aumenta la eficacia y simplifica las auditorías de cumplimiento.

Beneficios

El cumplimiento normativo continuo y sostenible (mediante la automatización de controles de seguridad y una prueba más eficaz de los controles) constituye una ventaja primordial del conjunto de programas de IAM basada en contenido de CA Technologies. No obstante, igualmente importantes son los beneficios de negocios, como la reducción de costos y el mejoramiento de las eficiencias a través de la automatización y centralización de la administración de identidades, que **reducen el riesgo aumentando la seguridad de los recursos y la información de TI**, y posibilitan mayor desempeño de negocios mejorando la capacidad de respuesta competitiva, las experiencias en línea del cliente y los ecosistemas de socios de negocios.

Sección 1: Desafío

Reducir el riesgo, mejorar el cumplimiento y hacer crecer el negocio

Hoy en día, las organizaciones enfrentan importantes desafíos de seguridad y la protección de los datos empresariales esenciales puede resultar costosa y desalentadora. Por ejemplo, debe proteger proactivamente contra el acceso no autorizado su información, sus aplicaciones y sus recursos basados en servidores más importantes. También debe garantizar que no se comuniquen incorrectamente sus datos, ni interna ni externamente. Debe cumplir con las reglamentaciones gubernamentales y del sector, y al mismo tiempo con las políticas internas de seguridad o del negocio. Por sobre todo, debe garantizar la continuidad de las operaciones de negocios mitigando el riesgo en prácticamente todos los niveles de la organización, y a la vez mantener los presupuestos y lograr eficiencia operativa.

Como si fuera poco, también debe ser capaz de desarrollar y ofrecer nuevos servicios en línea de forma rápida y segura, además de ampliar el alcance y la eficacia del ecosistema de socios de negocios. Únicamente así será capaz de cumplir con los objetivos de crecimiento de su negocio.

Además, debe continuar evaluando y adoptando nuevos y atractivos modelos de servicio o tecnologías, como la computación en la nube o la virtualización. Por lo tanto, las soluciones de seguridad que elija deberán ofrecer capacidades integrales que le permitan aprovechar estos nuevos enfoques tecnológicos.

Una sólida administración de identidades y accesos (IAM) ofrece la base para lograr una seguridad eficaz, ya que garantiza que todos los usuarios obtengan únicamente el nivel adecuado de derechos de acceso a todos los recursos protegidos y que esos derechos se respeten. Contribuye a reducir los costos administrativos por medio de la automatización de muchas de las funciones de administración del sistema, así como del aprovisionamiento y desaprovisionamiento de cuentas y derechos de acceso. Asimismo, la IAM mejora en gran medida el cumplimiento normativo a través de la automatización de los controles de seguridad y la simplificación de las auditorías de cumplimiento. Finalmente, posibilita oportunidades de negocios y ayuda a solidificar las relaciones existentes con clientes y socios de negocios, además de desarrollar más eficazmente las relaciones expandidas.

Preguntas clave que toda solución de administración de identidades y accesos debe responder:

- ¿Quién tiene acceso a qué?
- ¿Son quienes dicen ser?
- ¿Qué pueden hacer con ese acceso?
- ¿Qué pueden hacer con la información que obtuvieron?
- ¿Qué hicieron?

Si responde estas preguntas, puede identificar y corregir los derechos de acceso incorrectamente otorgados y garantizar que los activos de TI estén protegidos.

Este resumen sobre la solución le presentará las soluciones innovadoras de IAM que ofrece CA Technologies y destacará el modo en que estas soluciones pueden simplificar en gran medida sus esfuerzos por lograr cumplimiento, reducción del riesgo de TI y disminución de los costos totales de TI.

Sección 2: Solución

Cómo abordar los desafíos importantes de administración de identidades y accesos con Content-Aware IAM de CA Technologies

La administración eficaz de **identidades y accesos** no puede existir de manera aislada. Debería considerarse parte de una estrategia global para reducir los **riesgos generales de la seguridad de TI** y a la vez, mejorar la eficiencia y la productividad en todo el entorno. La estrategia de CA Technologies consiste en ofrecer todas las capacidades clave para que las empresas satisfagan sus necesidades de seguridad de TI, así como para integrar estas capacidades con otras funciones de administración, **como la administración de operaciones, almacenamiento y servicios.**

Existen tres problemas clave que se deben abordar al planificar una estrategia de administración de identidades, como se representa en el siguiente gráfico:

Ilustración A.



Para garantizar un monitoreo eficaz, debe hacer lo siguiente:

Controlar identidades Administre las identidades de los usuarios y sus roles, aprovisione usuarios para que tengan acceso a recursos, garantice el cumplimiento con políticas de identidad y acceso, y monitoree la actividad de los usuarios y de cumplimiento.

Controlar el acceso Compruebe las identidades de los usuarios y haga cumplir las políticas relativas al acceso a aplicaciones web, sistemas, servicios de sistemas e información clave. Además, ofrezca administración de usuarios con privilegios para evitar las acciones inapropiadas.

Controlar la información Detecte, clasifique e impida que se filtre información confidencial corporativa y de clientes.

Estos tres elementos son esenciales para un enfoque integral de la seguridad de la administración de identidades y accesos (IAM). Lamentablemente, los proveedores de IAM, en su mayoría, ofrecen solamente algunos elementos de las primeras dos categorías, pero no le permiten que proporcione control en el nivel de los datos. CA Technologies ofrece exclusivamente la solución integral para todas estas áreas importantes. En las siguientes secciones se describen las capacidades amplias e integradas que ofrece Content-Aware IAM de CA Technologies.

Control de identidades

La mayoría de las organizaciones de TI se esfuerzan por mantenerse al día con la explosión de la cantidad de usuarios de distintos tipos, la complejidad de la administración de los derechos de acceso para todos estos usuarios y la necesidad de probarles a los auditores que cada usuario cuenta sólo con el nivel de acceso apropiado. Lamentablemente, muchos enfoques hacia estos problemas consisten en procesos manuales de coordinación deficiente que exponen a las organizaciones a altos costos y riesgos. La administración deficiente de las identidades de usuarios también afecta a estos últimos, dado que los procesos ineficientes reducen la satisfacción del usuario y la productividad.

Para eliminar esta ineficiencia, es necesario automatizar todo el ciclo de vida de identidad de los usuarios. Gracias a capacidades como el aprovisionamiento automatizado y los procesos de flujo de trabajo, las empresas pueden obtener gran eficiencia, ya que los usuarios se vuelven más productivos y los administradores se ven liberados para concentrarse más en actividades que satisfagan las necesidades del negocio.

CA Technologies ofrece un enfoque exhaustivo e integrado hacia la administración del ciclo de vida de la identidad. La solución de CA Technologies brinda capacidades para la gobernanza de identidades, la administración y minería de roles y el aprovisionamiento de usuarios. Este enfoque completo incluye la creación inicial de identidades de usuarios, la asignación de cuentas y los privilegios de acceso que requieren, la modificación permanente de estos privilegios a medida que cambia el rol del usuario y la eliminación oportuna de estos derechos y cuentas cuando dejan de trabajar para la empresa.



Otro problema clave en la administración de usuarios se relaciona con la actividad del usuario y la generación de reportes de cumplimiento. Muchas organizaciones se ahogan bajo el peso de enormes cantidades de información de registro del sistema. El procesamiento manual de esta información no sólo implica inmensa pérdida de tiempo, sino que también dificulta la identificación eficaz de los eventos de seguridad importantes. Además, muchas reglamentaciones incluyen requisitos de recolección, almacenamiento y revisión de datos de registro del sistema que son casi imposibles de cumplir con un enfoque exclusivamente manual. A fin de cumplir efectivamente con estos requisitos, debe contar con un proceso automatizado y repetible para identificar y abordar infracciones de las políticas y los controles.

La solución de CA Technologies para la actividad del usuario y la generación de reportes de cumplimiento (User Activity Reporting Module) automatiza la recopilación, la normalización y el filtrado de los datos de actividades del usuario en todo el entorno de TI. Esta capacidad por sí misma puede aumentar en gran medida la eficacia administrativa, reducir los costos de TI y liberar a su equipo para que realice actividades más orientadas al crecimiento del negocio.

A diferencia de otros productos dedicados exclusivamente a acrecentar la velocidad de la recopilación de datos de registro, este módulo está diseñado de modo que lo ayude a responder con rapidez y precisión las preguntas clave que interesan a los auditores de PCI, SOX o HIPAA. Simplifica y acelera el cumplimiento gracias a los más de 400 reportes ya asignados a reglamentaciones de privacidad y cumplimiento, y a marcos y normas de control de TI. Le permite también exclusivamente mantenerse actualizado con los requisitos de generación de reportes que cambian constantemente, a través de actualizaciones de reportes de cumplimiento periódicas y automáticas.

Entre los productos de CA Technologies que le permiten controlar las identidades de usuarios de forma eficaz se cuentan los siguientes:

- **CA IdentityMinder™** Proporciona administración de identidades, aprovisionamiento y desaprovisionamiento, autoservicio del usuario, y auditoría y generación de reportes de cumplimiento. Contribuye a crear políticas coherentes de seguridad de identidades, simplificar el cumplimiento y automatizar procesos clave de administración de identidades.
- **CA GovernanceMinder™** Solución orientada a los negocios que aprovecha los datos de análisis y el flujo de trabajo para automatizar los procesos de gobernanza de identidades, lo que incluye la limpieza y certificación de privilegios, la división de obligaciones y la administración de roles. Con la automatización de estos procesos y controles, lo ayuda a reducir el riesgo, mejorar el cumplimiento y aumentar la eficiencia operativa.
- **CA User Activity Reporting** Ofrece el uso de reportes de actividades de usuario y de cumplimiento en todos los entornos físicos, virtuales y de nube.

Control de accesos

El control del acceso a los recursos importantes de la TI empresarial es necesario no sólo para lograr un cumplimiento eficaz, sino también para proteger el valor de los accionistas, la información del cliente y la propiedad intelectual. Sin autenticación eficaz de usuarios ni aplicación de políticas de acceso, el acceso inapropiado (ya sea intencional o involuntario) puede tener consecuencias desastrosas. Existen tres áreas importantes que se deben tener en cuenta:

- Control del acceso a aplicaciones y servicios basados en la web
- Control del acceso a información, aplicaciones y servicios por parte de usuarios con privilegios
- Autenticación avanzada

Administración de acceso web Actualmente, las organizaciones enfrentan dos exigencias aparentemente contradictorias. Para impulsar el desempeño y las ganancias, deben ampliar su dependencia de Internet y las aplicaciones web que las conectan con los clientes, socios de negocios y empleados. **Por otra parte, una organización que abre sus sistemas a potencialmente millones de usuarios internos y externos también expone sus aplicaciones, redes y datos a un enorme riesgo, que puede poner en peligro a toda la organización.** Muchas organizaciones son reacias a aprovechar los beneficios del crecimiento del negocio que podrían otorgar ciertos enfoques como la federación de identidades y la identidad orientada al servicio, debido a preocupaciones respecto de la seguridad.

CA SiteMinder®, el producto para la administración de acceso web líder del sector desde hace más de quince años, ofrece una base fundamental para autenticación de usuarios, inicio de sesión único, autorización y generación de reportes. Le permite crear políticas de acceso específico que pueden controlar el acceso a aplicaciones importantes basándose en un conjunto flexible de criterios estáticos o dinámicos. Esta flexibilidad facilita en gran medida el control del acceso de usuarios a sus aplicaciones y ayuda a eliminar la necesidad de códigos relacionados con la seguridad dentro de cada aplicación. El resultado es un desarrollo más rápido de la aplicación y una gran disminución de los costos administrativos y de mantenimiento.

CA SiteMinder se ha implementado con éxito en algunos de los entornos de TI más extensos y complejos del mundo. Se ha probado a escala de millones de usuarios y ha demostrado tener altísimo desempeño y confiabilidad.

IAM de CA Technologies también incluye capacidades para una federación de identidades segura, con el objetivo de activar el crecimiento del negocio a través de la expansión de ecosistemas integrales de socios de negocios. Dado que permite que los socios de negocios tengan acceso de forma segura a las aplicaciones (y viceversa), puede dinamizar las cadenas de valor y, sobre todo, aprovechar las oportunidades de crecimiento disponibles a través de las asociaciones integradas en línea. Además, se brinda seguridad integral para arquitecturas basadas en SOA, de modo que es posible proteger tanto las aplicaciones como los servicios web en una infraestructura de seguridad en común.

Entre los productos de CA Technologies que le permiten controlar el acceso a aplicaciones y servicios web de forma eficaz se cuentan los siguientes:

- **CA SiteMinder®** ofrece administración y aplicación centralizada de autenticación del usuario, autorización, inicio de sesión único y generación de reportes. Le permite proteger fácilmente las aplicaciones clave, mejorar la experiencia del usuario y simplificar sus auditorías de cumplimiento.
- **CA FedMinder™** extiende las capacidades de CA SiteMinder hasta las relaciones federadas de socios de negocios, lo cual permite que la organización implemente y administre con rapidez los ecosistemas de socios de negocios para contribuir al crecimiento del negocio.
- **CA SiteMinder Web Services Security** proporciona servicios centrales de autenticación y autorización y protege el acceso a servicios web basados en XML.

Administración de usuarios con privilegios Una de las áreas de riesgo más importantes de TI se relaciona con los usuarios con privilegios (administradores de TI y seguridad). Ya sean involuntarias o malintencionadas, las acciones inapropiadas por parte de usuarios con privilegios pueden tener efectos desastrosos para las operaciones de TI y para la seguridad general y privacidad de activos e información corporativa. Por lo tanto, es esencial que se permita a los administradores realizar únicamente las acciones para las que están autorizados, y sólo en los activos apropiados.

Además, los administradores suelen compartir (y a veces perder) sus contraseñas de sistema, lo que conlleva un riesgo aún mayor de infracciones a las políticas. Y dado que todos estos usuarios inician sesión como “Raíz” o “Admin”, sus acciones, tal como se reporta en el archivo de registro, son esencialmente anónimas. Estas condiciones no sólo plantean un gran riesgo de seguridad, sino que también dificultan sumamente el cumplimiento, ya que las acciones inapropiadas no pueden prevenirse ni asociarse con la persona que comete la infracción.

Lo que se necesita es un control de acceso específico para los usuarios administradores. Lamentablemente, la seguridad nativa del sistema operativo del servidor no proporciona control suficiente sobre quién puede tener acceso a cuáles recursos, ni tampoco ofrece la auditoría específica que se necesita para satisfacer requisitos de cumplimiento.

La solución de CA Technologies para la administración de usuarios con privilegios, CA ControlMinder™, protege los servidores proporcionando a los usuarios administrativos en todas las plataformas derechos más específicos que los que ofrecen los sistemas operativos nativos. Esto facilita el cumplimiento a través de la exclusiva especificidad del control de acceso basado en políticas y su aplicación, que incluye la división de obligaciones. La solución controla quién tiene acceso a los sistemas específicos, los recursos que tienen esos sistemas y los sistemas de servicios importantes (por ejemplo, es importante que los administradores no posean la capacidad de apagar el proceso de inicio de sesión del sistema con el fin de ocultar una actividad inapropiada). Además simplifica la administración gracias a una interfaz de usuario única para administrar todas las plataformas de servidores.

La solución admite también la administración extensiva de contraseñas de usuario con privilegios (PUPM), que ayuda a proporcionar rendición de cuentas del acceso con privilegios mediante la emisión de contraseñas temporales de un único uso o en tanto sean necesarias, a la vez que garantiza al usuario la responsabilidad por sus acciones a través de auditorías seguras. La PUPM también está diseñada de manera que permita que las aplicaciones tengan acceso mediante programación a las contraseñas de sistema y, al hacerlo, eliminen de los scripts las contraseñas integradas como parte del código.

Autenticación avanzada Las contraseñas de usuarios constituyen una gran incomodidad para los usuarios y altos costos para los grupos de TI. Además, no proporcionan la seguridad adecuada para la información y las aplicaciones importantes de la actualidad. La autenticación de dos factores ofrece una seguridad más sólida que las contraseñas, pero cuando se la **implementa en la forma de token de hardware, genera incomodidad y costos considerables**. CA AuthMinder es una versátil solución de autenticación de varios factores que elimina estos problemas y brinda mayor seguridad para sus activos importantes. Está integrada con CA SiteMinder, de modo que puede proteger y comprobar de forma transparente las identidades de los usuarios web y protegerlos contra el fraude y el robo de identidades sin modificar su experiencia normal de inicio de sesión ni exigir la posesión de tokens de hardware.

Otra preocupación para todos los grupos de TI es la prevención del fraude o robo de identidad. Los delincuentes han expandido su alcance más allá de los objetivos tradicionales de las tarjetas de crédito y la banca de consumidores, ahora buscan recoger información valiosa a la que se puede tener acceso en línea. El desafío que enfrenta es cómo detectar y bloquear la actividad fraudulenta antes de que ocurran pérdidas por fraude, sin que esto afecte a los usuarios legítimos. CA RiskMinder es un sistema de detección de fraude y seguridad basada en riesgos que ayuda a prevenir los fraudes en los servicios en línea de consumidores y de empresas. También proporciona a las organizaciones la capacidad de definir y aplicar diferentes niveles de autenticación en función del nivel de riesgo aceptable para una determinada transacción. A partir de una clasificación de riesgos y de políticas de la empresa, las organizaciones pueden implementar otras formas de autenticación firme, que incluyen el uso de CA AuthMinder, según el usuario y el tipo de transacción que desea efectuar.

La combinación de CA AuthMinder y CA RiskMinder, junto con las amplias capacidades de autenticación de CA SiteMinder, ofrecen una autenticación sólida y flexible para todos los usuarios.

Control de la información

La aplicación de control de acceso sobre la información confidencial es sólo el primer paso de un enfoque integral hacia la seguridad de la información. Una vez que los usuarios obtienen acceso legítimo a estos datos, muchas organizaciones tienen control escaso o nulo de las acciones que estos usuarios pueden realizar con ellos. Estas organizaciones no suelen tener pleno conocimiento de todos los lugares en que se almacena su información confidencial, y no tienen protección contra la exposición o revelación no autorizada de estos datos de forma interna o externa. Algo tan simple como un número de seguridad social puede tener considerable impacto negativo si se revela de forma inapropiada. Por este motivo, muchas organizaciones creen que sus propios empleados plantean una amenaza a la seguridad de los datos más riesgosa que la de personas externas, a través de conductas involuntarias o maliciosas.

CA DataMinder ayuda a mantener el control de enorme cantidad de información y, lo más importante, a proteger datos confidenciales contra la revelación inapropiada o el mal uso. Protege los datos en movimiento a través de la red, los datos en uso en la terminal y los datos en reposo en los servidores y repositorios. Le permite definir políticas que establezcan qué datos se deben comprobar, qué tipo de elemento de datos se debe monitorear y la medida que se debe tomar si se detecta actividad inapropiada. Incluye además una colección de políticas integradas basadas en casos de uso de negocio reales, que pueden simplificar la rápida implementación. La solución reduce en gran medida el riesgo de seguridad y facilita la comprobación del cumplimiento de ciertas reglamentaciones y mejores prácticas relacionadas con la seguridad.

Local o en la nube; su elección

Algunas organizaciones prefieren los beneficios “prácticos” de una implementación de IAM completamente local. Otras, con razón, desean aprovechar las ventajas de la gran eficacia y agilidad que pueden brindar los servicios en la nube. No obstante, la mayoría de las organizaciones tiende a preferir un enfoque híbrido, externalizando varios servicios a la nube y a la vez manteniendo las aplicaciones o la información más importante en la forma local.

La IAM de CA Technologies le ofrece la flexibilidad de elegir el modelo de implementación que se adapte a sus requisitos del negocio y de seguridad. Nuestras capacidades de IAM centrales se ofrecen como servicios en la nube (llamados “CA CloudMinder™”), alojados en grandes centros seguros de datos, administrados por expertos de CA Technologies. En el transcurso de los próximos doce meses, se ofrecerán otros servicios de administración de identidades en la nube. Puede adoptar servicios de IAM basados en la nube en función de sus propias necesidades y plazos, comenzando por una solución completamente local y luego migrando determinados componentes a la nube a medida que lo exijan sus necesidades y decisiones de seguridad. Este enfoque le ofrece muy alta flexibilidad y le permite aumentar la agilidad general del negocio y de TI.

La diferencia de CA Technologies: IAM basada en contenido

La administración de identidades y accesos no es un área nueva de la tecnología. Hace tiempo que reduce el riesgo y aumenta las eficiencias de miles de empresas de todo el mundo. Existen numerosos proveedores de IAM y muchos de los que venden grandes conjuntos de programas de IAM afirman ofrecer esencialmente las mismas capacidades. Por lo tanto ¿cómo decidir qué proveedor de IAM elegir?

La diferencia primordial entre los conjuntos de aplicaciones de IAM yace en la amplitud funcional de su oferta, la compatibilidad con una serie de modelos de implementaciones y entornos (por ejemplo, mainframe, en nube y virtual) y la innovación que aportan a su oferta de productos.

Nadie iguala a CA Technologies en estas áreas. Pero, sobre todo, la IAM de CA Technologies proporciona capacidades que otras soluciones de IAM no ofrecen. Generalmente, los sistemas de IAM tradicionales proporcionan control limitado sólo hasta el punto de acceso y no le permiten controlar lo que se puede hacer con la información una vez obtenida. Esto plantea una limitación importante de estas plataformas, ya que no previene completamente el mal uso ni la revelación inapropiada de su información confidencial.

Las soluciones innovadoras de IAM basada en contenido de CA Technologies amplían esta capacidad de modo que ofrezca control hasta el ámbito de los datos, con lo cual proporciona un control más estricto de lo que los usuarios pueden hacer con su información importante. Esta solución integrada también ayuda a reducir su riesgo de TI, automatiza los procesos clave de seguridad para generar un aumento de las eficiencias y mejora la posición general de cumplimiento. Y finalmente, le permite adaptar con confianza modelos de computación nuevos y emergentes, como la virtualización y la computación en la nube.

La meta es hacer avanzar el negocio de forma segura. Content-Aware IAM de CA Technologies le brinda la base que lo ayudará a lograr esta meta.

Sección 3: Beneficios

Cómo reducir el riesgo de seguridad de TI y a la vez, mejorar las eficiencias operativas y hacer posible el cumplimiento

La solución de Administración de identidades y accesos de CA Technologies, integral y comprobada, protege sus activos de TI más importantes en todo el entorno y brinda estos amplios beneficios a organizaciones de TI de todos los tamaños:

Menor riesgo de seguridad

Content-Aware IAM de CA Technologies ayuda a garantizar que los recursos de TI importantes estén protegidos y que sólo usuarios que cuentan con la autorización apropiada pueden tener acceso a ellos, y sólo de las maneras apropiadas. Le permite también administrar y analizar información de eventos de seguridad para identificar y solucionar rápidamente problemas potenciales de seguridad, como la revelación o el uso inapropiados de información confidencial corporativa o de clientes.

Cumplimiento normativo mejorado

Los productos de IAM de CA Technologies le proporcionan a su organización las herramientas necesarias para admitir el cumplimiento continuo a través de capacidades automatizadas y administradas centralmente que ayudan a reducir costos y a la vez, fortalecen los controles de seguridad de TI. Los desafíos que plantea el cumplimiento se pueden simplificar en gran medida, ya que la auditoría integral le permite ofrecer pruebas de sus controles y validar ante los auditores el funcionamiento eficaz de sus controles de seguridad establecidos. También lo ayuda a automatizar los procesos de cumplimiento de seguridad, de modo que quede garantizado el cumplimiento de las políticas corporativas o normativas y pueda ofrecer pruebas del cumplimiento, lo que se traduce en auditorías más fáciles y eficientes.

Reducción de los gastos administrativos y mayor eficiencia

Los productos de IAM de CA Technologies pueden ayudar a automatizar muchos de los procesos administrativos clave de TI, especialmente los que se relacionan con la administración de las identidades de usuarios y los derechos de acceso. Junto con el filtrado y el análisis automatizado de la información del registro de seguridad, estas capacidades pueden generar eficiencias administrativas importantes y con ello, reducir los costos generales de TI. Además, pueden ayudar a mejorar la productividad del usuario y de la administración, ya que se debe dedicar menos tiempo a los procesos manuales.

Mejor activación de negocios seguros

Los clientes y los socios de negocios sólo trabajarán con su organización si creen que usted puede brindar un entorno seguro para su información personal. Los productos de IAM de CA Technologies pueden ayudar a su organización a proteger sus aplicaciones, además de entregar nuevas aplicaciones y servicios más rápidamente a sus clientes y socios de negocios. Estas aplicaciones pueden ofrecer una experiencia de usuario personalizada y positiva, lo que fortalecería la satisfacción de clientes y socios de negocios y contribuiría al crecimiento del negocio y del ecosistema de socios.

Sección 4:

La ventaja de CA Technologies

La IAM basada en contenido de CA Technologies no sólo le permite controlar las identidades y los accesos del usuario sino también el uso de la información. Esta importante capacidad aumenta la seguridad general y ayuda a impedir el uso inapropiado de su información corporativa o de clientes.

La IAM de CA Technologies ofrece también una combinación única de ventajas, como el alcance exhaustivo que abarca aplicaciones, plataformas y servicios; el diseño modular basado en servicios e interfaces de usuario en común; aprovisionamiento, flujo de trabajo y entrega de privilegios centralizados y automatizados y finalmente, escalabilidad global.

Además, la IAM de CA Technologies es compatible con la más amplia variedad de plataformas (desde distribuidas hasta mainframe) y modelos de implementación (lo que incluye los entornos virtualizados y en nube). Puede implementarla de forma local, como servicios en la nube o en un entorno híbrido, lo que le ofrece flexibilidad y agilidad en la utilización de las soluciones de IAM. Esto posibilita que nuestras soluciones de IAM ofrezcan una plataforma uniforme y segura en todo el entorno de TI, que incluye tecnologías emergentes que podría adoptar en el futuro cercano.

CA Technologies es líder en la administración de TI desde hace más de 30 años, tiene más de 1000 clientes de seguridad y tiene el compromiso de seguir aportándoles capacidades de seguridad. Tenemos un grupo amplio y dedicado de expertos en seguridad que saben cómo hacer implementaciones de seguridad exitosas y ayudar a nuestros clientes a acelerar el tiempo de posicionamiento.

Sección 5: Próximos pasos

Si descubre que:

- Necesita capacidades más flexibles en el modo de controlar y aplicar políticas sobre el acceso de los usuarios a sus recursos de TI...
- Le preocupa que usuarios fraudulentos obtengan acceso a su información importante de negocios...
- Lo abruma los costos y esfuerzos que requiere el cumplimiento de requisitos normativos y del sector...
- Las presiones presupuestarias le exigen mayores eficiencias en las funciones administrativas...
- Le preocupan los riesgos potenciales de los privilegios excesivos de sus administradores...
- Le interesa expandir su adopción de entornos virtualizados o en nube, pero le preocupa el impacto en la seguridad o el cumplimiento...

...entonces debe echar un vistazo a Content-Aware IAM de CA Technologies. Se trata de la solución de IAM más exhaustiva e integrada que aborda los aspectos de seguridad de aplicaciones y servicios web, sistemas heredados y modelos emergentes basados en la nube.

CA Technologies es una compañía de software y soluciones de administración de TI con experiencia en todos los entornos de TI, desde entornos mainframe y distribuidos, hasta entornos virtuales y de nube. CA Technologies administra y asegura los entornos de TI, y permite que los clientes entreguen servicios de TI más flexibles. Los innovadores productos y servicios de CA Technologies proporcionan la perspectiva y el control esencial para que las organizaciones de TI mejoren la agilidad del negocio. La mayor parte de las compañías Global Fortune 500 confía en CA Technologies para administrar sus cambiantes ecosistemas de TI. Si desea obtener más información, visite CA Technologies en ca.com.