IBM Security

IBM

Para una Mejor Gestión de Acceso, Mire Más Allá de los Roles con Derechos

IBM Security Identity Governance and Intelligence puede mejorar el control de acceso mediante la integración de sistemas existentes, sin compromiso

Visite nuestro sitio web

Hable con un especialista

Documento informativo de IBM Security

¿Por qué Existen los Roles y por qué ya No Son Más Suficientes?

Nomucho tiempo atrás, los roles en el trabajo eran relativamente fáciles de definir y controlar. Uno era “contador” o “diseñador gráfico” o “asociado de negocios”. Pero a medida que las organizaciones fueron creciendo y el software de negocios se iba tornando más sofisticado, se incorporaban nuevos roles. El “Contador de Nueva York” requería un acceso diferente a las aplicaciones y a los datos que el “Contador de Chicago”.

Los roles se inventaron para gestionar el suministro y la cancelación de usuarios de manera más fácil. Y todavía funcionan. La habilidad de darle a un nuevo usuario todo (o la mayor parte) el acceso necesario para realizar los roles de su trabajo es un progreso mucho mayor que el asignarles a los usuarios individuales sus tareas específicas según el caso.

El desafío llega con la reciente explosión en los números y los tipos de roles empresariales. Las organizaciones se tornaron tan enfocadas en tener el rol perfecto para cada grupo de usuario que incluso pocas variaciones en el perfil de una persona o las necesidades de acceso podrían llevar a la creación de un rol completamente separado. El problema fue el siguiente: Si las limitaciones de TI que controlaron los derechos de los usuarios (los permisos otorgados para tomar acciones) eran vinculadas únicamente a los roles generales, los cargos más especializados podrían ser ignorados sin ningún control.

Con la gestión de identidad, un fabricante multinacional gestiona

430 millones

de posibles conflictos de derechos con algunas cuantas normas.

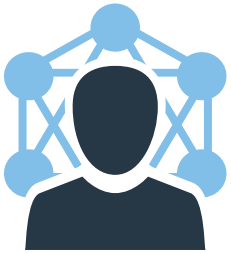
Es Importante Asegurarse de que las Necesidades de Acceso y los Derechos estén Alineados

La creación de los roles y la implementación de las herramientas de gestión de identidad les proporcionaron a las organizaciones la habilidad de entender qué usuarios habían accedido y a qué aplicación lo habían hecho, y en qué momento se les concedieron el acceso.

Esta información, sin embargo, ya no es suficiente para garantizar la seguridad y el control. Las organizaciones también necesitan saber si los accesos que tienen los usuarios son correctos. Lo que es más importante es que necesitan asegurarse de que los usuarios no tengan un acceso incorrecto.

La explosión de roles específicos significa que los roles se han incrementado no solo en la cantidad sino también que en la complejidad. Y los roles están en constantes cambios. Por eso, ya no son más la herramienta indicada para gestionar las identidades de los usuarios. Las organizaciones necesitan ver en detalle quiénes tienen qué privilegios y cómo los están utilizando.

Una manera importante, y eficaz, para lograr el punto de vista necesario de los usuarios y sus privilegios consiste en pensar como un auditor. Esto puede ayudar a mitigar los problemas ya que se asegura de que los controles necesarios estén en su lugar para evitar violaciones de datos. ¿Acaso Bob no ha utilizado un derecho particular en los últimos seis meses? Eso siempre es un buen motivo para revocar el privilegio. ¿Nancy tiene la habilidad de iniciar una solicitud, es decir, una compra de un equipo, y luego aprobarla ella misma? Otro motivo para revocarlo.



Con IBM, un minorista en línea global elimina prácticamente el

80 % de los privilegios de acceso de un usuario

después de detectar accesos pocos frecuentes.

Pensar como un Auditor Sirve Tanto para las Necesidades Empresariales como para las de TI

Una solución de gobierno de identidad fácil para el auditor es la clave para gestionar de manera eficaz a los usuarios y sus titularidades. Los auditores les dan una gran importancia a las reglas indicadas para identificar las violaciones de datos en la segregación de deberes. También necesitan controles para eliminar y prevenir estas violaciones.

Pero hay más. Para lograr mayor efectividad, es necesario no solo pensar como auditor, sino que hablar como uno. El idioma utilizado más comúnmente en el gobierno de identidad utiliza la terminología a partir de palabras del área de TI y de negocios. Esta combinación puede ser un problema, sin embargo, para los auditores que no entienden la jerga de TI y, en vez de eso, prefieren utilizar términos de negocios. La solución de gobierno de identidad indicada reúne las áreas de negocios y de TI para ayudar a las organizaciones a entender si los usuarios tienen o no acceso a las aplicaciones adecuadas, y para dar asistencia en las decisiones y acciones empresariales que dependen del acceso apropiado.

IBM® Security Identity Governance and Intelligence le da la habilidad de mirar más allá de los roles por una visión detallada en las titularidades y las actividades de negocios. La solución de IBM proporciona la inteligencia que necesita para revocar de manera precisa y eficiente, reasignar y agregar titularidades, lo que ayuda a cumplir con las necesidades del negocio sin poner en riesgo la seguridad.

Un banco en Francia disminuye su catálogo de derechos, en el que muestra a los usuarios

entre 10 y 15 elementos

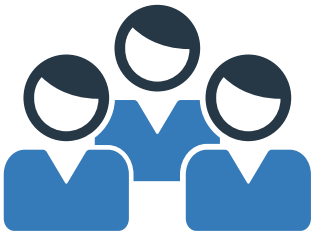
en vez de cientos de ellos.

Por Qué las Actividades de Negocios Son una Mejor Base para Gobierno

Piense en un rol como una colección de titularidades. Es un modo de definir los tipos de acceso que necesitan las personas que hacen el mismo trabajo o uno similar. Estos derechos pueden variar desde el acceso al software del correo electrónico (otorgado a todos), hasta el acceso a una aplicación que gestiona la propiedad intelectual (otorgado solo a unos pocos), hasta el acceso a funciones de aplicación muy específicas (con el acceso más limitado).

Es un proceso de tres niveles: a un empleado se le asigna un rol (por ejemplo, corredor de bolsa). Ese rol viene con privilegios que permiten el acceso a las capacidades de un software (como el ingreso de un pedido de actividad comercial). Esa capacidad permite una actividad de negocio específica (colocar una actividad comercial). El corredor de bolsa, sin embargo, tiene bloqueado la aprobación de esa misma actividad comercial. Ese privilegio se le otorga solo al personal que no tiene el permiso para colocar la actividad comercial. Los deberes se segregan para evitar un conflicto.

El problema con los roles es que evolucionan continuamente. Dentro de cada rol puede haber varios roles o grupos de roles, que pueden confundir, generar violaciones en la vulnerabilidad de conformidad y de seguridad. Un auditor que crea o hace cumplir una regla, sin embargo, podría no tener un conocimiento minucioso de los roles. ¿El resultado? Se podrían pasar por alto algunas violaciones en la segregación de deberes.



Una compañía de seguros y financiera administra el acceso de

75.000 usuarios

de SAP, aplicaciones distribuidas y del sistema principal.

Aquí Presentamos Cómo Funciona el Enfoque Basado en la Actividad de Negocio

¿Qué pasaría si usted segrega los deberes en dos roles, “diseño web” y “nómina”, para prevenir publicar los salarios de los empleados en el sitio web de la compañía? Imagínese, sin embargo, que alguien del equipo de nóminas también trabajó en proyectos relacionados con el sitio web que le permitió publicar en el sitio web sin tener el rol de “diseño web”. Para evitar esta situación, cada combinación de rol (y subrol) posible de los roles de diseño web y de nómina tendría que ser administrado, una tarea virtualmente imposible sin las herramientas adecuadas de gobierno de identidad automatizadas.

En vez de administrar los accesos de identidad y segregación con conceptos abstractos de roles, ¿por qué no utilizar algo más simple? Aquí es en donde incorporamos la gestión basada en actividades de negocios. En vez de llamar a los roles “diseño web ” y “nómina”, utilize lenguaje sencillo para describir actividades como “Habilidad para editar el sitio web” y “Habilidad para ver la información de nóminas”.

Desde este punto de vista, la organización y el auditor saben exactamente las capacidades que tiene cada usuario. Inclusive, las actividades de subcategorías (como “edición de gráficos en un sitio web”) se consideran automáticamente parte de una categoría más amplia (como “edición de un sitio web”), por lo tanto, no es necesario la gestión manual que se requiere cuando se utilizan los roles. En muchos casos, un auditor no sabrá qué roles específicos se pueden o no superponer sin conflicto. Sin embargo, los auditores sabrán qué ***actividades de negocios,*** cuando se utilizan juntas, podrían implicar una violación en la segregación de deberes y un riesgo de seguridad.

La solución adecuada de gestiõn de identidad lo ayuda a controlar sus accesos de usuario en las actividades de negocios con visibilidad específica consolidada de los derechos, no solo de los roles. Los roles cambian, se superponen, e incrementan. Como resultado, el acceso se debe gobernar al nivel de los derechos, lo que permite una visualización de las capacidades específicas que tiene el usuario, en vez de depender de las agrupaciones confusas de acceso que se le otorga a un rol. La solución indicada puede proporcionar la inteligencia que necesita para tomar las decisiones correctas acerca de quién tiene, y quién debería tener, acceso a qué.

En Resumen: Controlar con Soluciones Inteligentes de IBM

IBM Security Identity Governance and Intelligence establece la etapa de mejora del negocio al permitirle que otorgue derechos a las personas indicadas. Con una visibilidad detallada de los derechos, puede hacer cumplir mejor las políticas de la segregación de deberes para asegurar que los usuarios actualmente autorizados no tengan titularidades en conflicto. Puede administrar las cuentas huérfanas para asegurar que los usuarios antiguos no continúen con el acceso después de que se hayan ido de la organización. Y puede automatizar los controles y la creación de informes. La perspectiva de IBM le permite administrar con las actividades de negocio, que se enfoca en los roles complejos para hacer la gestión más fácil a los auditores y simplificar las tareas de gobierno.

IBM Security Identity Governance and Intelligence conecta los puntos de vista del área de TI, conformidad y negocios para mitigar los riesgos de acceso. Al consolidar los derechos de acceso específicos para las aplicaciones empresariales en un repositorio central y estructurarlas en roles empresariales, por ejemplo, se genera una mejor visibilidad en el acceso real de los usuarios.

Como una parte integral del compromiso de IBM de liderar en la identidad y la gestión de acceso, IBM Security Identity Governance and Intelligence juega un papel fundamental en el catálogo de seguridad de TI de IBM. Las soluciones de IBM, incluidos los recursos de seguridad completos y la información proporcionada por la investigación y el desarrollo de IBM X-Force®, están diseñadas para ayudar a proteger las aplicaciones fundamentales para el negocio y los datos de las amenazas de seguridad, que incluyen los conflictos posibles por fallas en los controles.

E.ON Global Commodities necesitó prevenir

estafas.

Gracias a IBM, puede hacer mejor lo siguiente:

- **gestionar la segregación de los deberes,**
- **proporcionar informes a los auditores,**
- **comprender el flujo de información en la compañía.**

Mire el video de IBM acerca de la presentación de E.ON.

Para obtener más información

Para obtener más información sobre IBM Security Identity Governance and Intelligence, comuníquese con su representante de IBM o asociado de negocios de IBM, o visite: ibm.com /security

Acerca de las Soluciones de IBM Security

IBM Security ofrece uno de los más avanzados e integrados catálogos de productos y servicios de seguridad empresarial. Este catálogo, que cuenta con el respaldo de la mundialmente reconocida investigación y desarrollo de X-Force, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger holísticamente a su personal, sus infraestructuras, sus datos y sus aplicaciones, ofreciendo soluciones para la gestión de la identidad y del acceso, la seguridad de base de datos, el desarrollo de aplicaciones, la gestión del riesgo, la gestión de terminales, la seguridad de la red y mucho más. Estas soluciones permiten que las organizaciones gestionen el riesgo de manera efectiva e implementen una seguridad integrada para dispositivos móviles, nubes, redes sociales y otras arquitecturas de negocios empresariales. IBM opera una de las mayores organizaciones de investigación, desarrollo y entrega de seguridad del mundo, supervisa 15 mil millones de eventos de seguridad diarios en más de 130 países y posee más de 3.000 patentes de seguridad.

Además, IBM Global Financing ofrece diversas formas de pago para ayudarle a adquirir la tecnología que necesita para hacer crecer su empresa. Proporcionamos una gestión de todo el ciclo de vida de los productos y servicios de TI, desde su adquisición hasta su eliminación. Para obtener más información, visite: ibm.com /financing

Visite nuestro sitio web

Hable con un especialista

IBM Security
Route 100
Somers, NY 10589

Producido en los Estados Unidos de América, octubre del 2016

WGW03177COES-00