

SOLUCIÓN DE CONTROL DE ACCESO A LAS APLICACIONES WEB

Actualmente las empresas disponen de diversas aplicaciones de negocio ejecutándose sobre diversos entornos Web (servidores Web, servidores de aplicación, servidores de contenidos, etc.).

En la mayoría de los casos, estas empresas no disponen de ninguna herramienta que les permita gestionar de manera centralizada su seguridad, sobre todo en aspectos tales como:

- La autenticación de los usuarios
- La autorización para el acceso a los recursos Web
- El login único en todas las aplicaciones y entornos Web

Este hecho conlleva los siguientes problemas asociados:

- La seguridad y los datos de usuarios están embebidos en cada aplicación. No hay integración entre aplicaciones, lo que supone mantener toda la información de seguridad para el mismo usuario dispersa en cada aplicación. Se multiplica el tiempo de desarrollo y de mantenimiento.
- Retrasos en la puesta en producción de nuevas iniciativas, ya que para cada nueva aplicación hay que crear su modelo de seguridad e implementarlo.
- Se hace muy difícil poder cumplir las políticas de seguridad de la empresa consistentemente en todas las aplicaciones.
- Los usuarios tienen que realizar login en cada aplicación.
- Se reciben muchas llamadas en el Help Desk para regeneración de contraseñas.
- Falta de escalabilidad del modelo y del sistema de seguridad. Cuesta mantener la seguridad y cuesta hacerla crecer.
- Riesgo de tener inconsistencias en datos de usuarios y agujeros de seguridad (por ejemplo por cuentas activas de usuarios dados de baja).
- Datos de auditoría insuficientes y sin integración.

Día a día crecen los entornos web a gestionar, aparecen nuevas aplicaciones de negocio, se migran aplicaciones, se arrancan importantes iniciativas de negocio que requieren una gestión eficaz, rápida y avanzada de seguridad, etc., y todo esto no se puede parar.

La solución a esta problemática pasa por implantar un sistema de gestión de las identidades (empleados, usuarios, proveedores, partners, etc.) que cubra todas las plataformas de servicios Web y las aplicaciones Web que se ejecutan en la empresa.

Los principales aspectos incluidos en esta solución son:

- Gestión integrada de la seguridad corporativa basada en políticas de usuarios para dar acceso a portales, aplicaciones web y aplicaciones propietarias.
- Modelo de seguridad alineado con los estándares actuales y que permite la integración de usuarios que pertenezcan a partners o clientes.
- Implementación de una delegación de administración granular, flexible y sencilla de configurar, para permitir repartir fácilmente las tareas de administración en base a departamentos, entornos u otros conceptos.
- Implementación del login único (single sign-on) para las aplicaciones web y el logon en red de Windows.
- Integración en el modelo de seguridad de aplicaciones tales como sistemas de mensajería asíncrona.
- Integración en el modelo de seguridad de aplicaciones propias, vía APIs y clases Java, que sigan los estándares de seguridad definidos.
- Configuración en alta disponibilidad para evitar una posible falta de disponibilidad del servicio central de autenticación y autorización de acceso a los recursos web.

- Modelo de seguridad que permite una arquitectura multi-empresa o multi-dominio para poder extender el modelo de manera natural.
- Integración con otras soluciones de seguridad como la gestión centralizada de identidades, soluciones de control de acceso a recursos de sistema operativo, etc.
- Auditoría de acceso centralizada para todas las aplicaciones web.