Raymundo Romero Arenas

Matrícula: A00570654

Bases de datos – Grupo 1

Profesor: Ricardo Cortés Espinosa

Domingo 24 de noviembre del 2019

**Laboratorio #17**

Nota: El laboratorio será implementado por todos los integrantes del equipo en el proyecto

1. ¿En qué consiste el acceso basado en roles?

R = Es una función de seguridad que asigna permisos a usuarios basados en su rol dentro de una organización. Permite controlar el acceso a las funciones de un sistema de tal forma que un usuario pueda interactuar solamente con la información que necesita para hacer una tarea.

Es muy usado en empresas con una gran cantidad de empleados y administradores (1).

1. Investiga y describe 6 sistemas, 3 conocidos que empleen RBAC y 3 desconocidos que no, junto con su funcionamiento general.

Sistemas que usan RBAC:

* Microsoft Azure = Su sistema de RBAC permite administrar a detalle el acceso a los recursos de Azure. Los roles se pueden personalizar en función de grupos de usuarios o dominios web para determinar el acceso a máquinas virtuales o subredes (2).
* Oracle = El RBAC permite empaquetar privilegios para enviarlos de forma individual a los usuarios para que puedan realizar sus labores. Esto facilita mucho la asignación, sobre todo cuando hay privilegios compartidos entre usuarios (3).
* CISCO = El RBAC asocia usuarios con roles y redes que determinan a qué comandos tiene acceso un usuario para configurar aparatos. El módulo de control de aplicación (ACE) de los productos de CISCO tiene roles predefinidos que se pueden configurar para permitir/restringir el acceso a una subred o parte de esta. (4).

Sistemas que no usan RBAC

* Sistemas de facturación
* Sistemas de instituciones o empresas con muy pocos usuarios (Ej. Tiendas o talleres)
* Sistemas de inventariado

1. Beneficios y desventajas de este modelo (5)

Ventajas:

* Reduce el trabajo administrativo-técnico
* Maximiza la eficiencia de las operaciones
* Permite cumplir con normas regulatorias de privacidad-confidencialidad

Desventajas:

* No puede controlar el acceso a datos de un sistema
* Los privilegios sólo se pueden asignar a usuarios, no a operaciones del propio sistema

Bibliografía:

1. Auth0, 2019, “Role-Based Access Control” (24/11/2019), Recuperado de: https://auth0.com/docs/authorization/concepts/rbac
2. Microsoft, 2019, “What is role-based access control (RBAC) for Azure resources?” (24/11/2019), Recuperado de: https://docs.microsoft.com/en-us/azure/role-based-access-control/overview
3. Oracle, 2019, “Configuración de RBAC” (24/11/2019), Recuperado de: https://docs.oracle.com/cd/E24842\_01/html/E23286/rbactask-30.html
4. CISCO, 2019, “Role-Based Access Control” (24/11/2019), Recuperado de: https://www.cisco.com/c/en/us/td/docs/interfaces\_modules/services\_modules/ace/vA5\_1\_0/configuration/getting/started/guide/ace\_module\_gsg/rbac.html
5. DataInsider, 2019, “What is Role-Based Access Control (RBAC)?” (24/11/2019), Recuperado de: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more