Nombre: Jorge Manuel Oyoqui Aguilera
Matrícula: A01711783
Fecha: 03/05/2025
Materia: Construcción de Software y Toma de Decisiones
Grupo: 501
Profesores: Enrique Alfonso Calderón Balderas,
Denisse L. Maldonado Flores, Alejandro Fernández Vilchis

Tecnológico de Monterrey

Preguntas Laboratorio 19

- **¿En qué consiste el control de acceso basado en roles?**
  El control de acceso de acceso basado en roles (RBAC) es un mecanismo de seguridad que define los roles de un sistema y los permisos o privilegios de cada uno, esto para determinar si a un usuario se le debe dar acceso a algún recurso.
  Los permisos se asignan según el acceso (lo que el usuario puede ver), las operaciones (lo que el usuario puede hacer) y las sesiones (cuánto tiempo puede hacerlo el usuario).

  Ahora, existen tres reglas principales para implementar el RBAC, que son:

  - **Asignación de roles:** Un usuario puede ejercer privilegios si se le ha asignado un rol.
  - **Autorización basada en roles:** El rol de un usuario debe estar autorizado, lo que garantiza que los usuarios solo puedan asumir roles para los que están autorizados.
  - **Autorización de privilegios:** Un usuario puede ejercer ciertos privilegios si está autorizado para hacerlo, según su autorización y asignación de roles. (ENTRUST, S.F.)

  Este modelo tiene varias ventajas, como:

  - **Facilitar la administración de permisos**, ya que los roles pueden ser gestionados sin modificar cada usuario.
  - **Mejorar la seguridad**, limitando el acceso solo a lo necesario (principio del mínimo privilegio).
  - **Escalar fácilmente**, ya que nuevos usuarios solo necesitan ser asignados a un rol existente.

ENTRUST (S.F.). “¿QUÉ ES EL CONTROL DE ACCESO BASADO EN ROLES (RBAC)?”. Recuperado de: https://www.entrust.com/es/resources/learn/what-is-role-based-access-control#:~:text=El%20control%20de%20acceso%20basado%20en%20roles%20(RBAC)%20es%20un,las%20funciones%20de%20un%20usuario.

IBM (S.F.). “¿Qué es RBAC (control de acceso basado en roles)?”. Recuperado de: https://www.ibm.com/mx-es/think/topics/rbac

ORACLE (2011). “Control de acceso basado en roles (descripción general)”. Recuperado de: https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html

- **Investiguen y describan 2 sistemas, uno que aplique RBAC y uno que no. Realicen un análisis de ventajas y desventajas de cada uno con respecto al control de acceso.**

  Como ejemplo de un **sistema que aplica RBAC** estaría Microsoft Active Directory (AD), el cual es un sistema de gestión de identidades y accesos ampliamente utilizado en empresas, y permite asignar permisos y accesos a recursos (como archivos, aplicaciones o servidores) basándose en roles de grupo. Por ejemplo, se puede asignar el rol "Recursos Humanos" a un conjunto de usuarios, y ese grupo tendrá acceso solo a carpetas o aplicaciones relevantes. Algunas ventajas de este sistema son que es fácil de escalar y administrar (sobre todo contando que hablamos de empresas grandes), reduce riesgos de seguridad y permite aplicar políticas automáticas según cual sea el rol del usuario. Lo malo, y entre sus desventajas, es que resulta difícil ajustar excepciones (si se llegara a dar ese caso) a usuarios ya predefinidos, aparte de que una mala estructura en los roles podría afectar negativamente todo el sistema.

  Como ejemplo de un **sistema que NO aplica RBAC** sería el sistema de permisos por usuario en Linux (o al menos en la versión tradicional), pues los sistemas Unix/Linux tradicionales usan un modelo basado en usuarios y grupos, donde cada archivo o recurso tiene permisos para el usuario propietario, el grupo, y otros, pero no maneja abstracciones de roles como "Gerente" o "Editor" por ejemplo. Algunas ventajas de este modelo son que es simple y fácil de entender, sobre todo para entornos pequeños; aparte de que puedes dar accesos específicos a un usuario en específico, dando más control sobre los privilegios de cada usuario. Pero sus desventajas son que es más difícil de escalar, sobre todo cuando se trabaja en grandes organizaciones con muchos usuarios; requiere trabajar a mano los permisos de cada usuario y, gracias a eso, también es más propenso a errores humanos como dar accesos indebidos u olvidar darlos o retirarlos.

  Así que, en conclusión, el sistema RBAC es útil para mantener buena escalabilidad, para tener buena seguridad y algo de flexibilidad, recomendado para grandes empresas; aunque su mantenimiento y libertad a la hora de dar permisos sea más complicado o limitado. Mientras que los sistemas que NO usan RBAC son enfocados en tener un mantenimiento más simple y una alta flexibilidad a la hora de asignar, quitar o modificar permisos, método recomendado para empresas pequeñas, aunque si mantenimiento es más complicado y es mucho más propenso a tener errores.

Vincent Hu (NIST), David Ferraiolo (NIST), Richard Kuhn (NIST), Adam Schnitzer (BAH), Kenneth Sandlin (MITRE), Robert Miller (MITRE), Karen Scarfone (Scarfone Cybersecurity) (2019). “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”. Recuperado de: https://csrc.nist.gov/pubs/sp/800/162/upd2/final

Microsoft (2024). “¿Qué es el control de acceso basado en rol de Azure ((RBAC)?”. Recuperado de: https://learn.microsoft.com/es-es/azure/role-based-access-control/overview