EL LABORATORIO SE ENCUENTA EN EL GIT DEL EQUIPO………………………..

¿En qué consiste el acceso basado en roles?

Es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al superusuario. RBAC puede dividir las capacidades de superusuario entre varios administradores. La gestión de derechos de procesos se implementa a través de **privilegios**. La gestión de derechos de usuarios se implementa a través de RBAC.

<https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html>

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

Experiencia21.tec.mx utiliza RBAC ya que los usuarios tienen asignados roles, por ejemplo los profesores que pueden editar los cursos, agregar materiales, calificar, etc. Pueden agregar más usuarios y proporcionar roles como colaboradores, alumnos, calificadores.

Azure Resources: La gestión de acceso para recursos en la nube es una función crítica para cualquier organización que esté usando la nube. El control de acceso basado en roles (RBAC) lo ayuda a administrar quién tiene acceso a los recursos de Azure, qué pueden hacer con esos recursos y a qué áreas tienen acceso

Kubernetes es un sistema de código libre para la automatización del despliegue, ajuste de escala y manejo de aplicaciones en contenedores.   
 Cómo se pronuncia

El control de acceso basado en roles (RBAC) es un método para regular el acceso a los recursos informáticos o de red en función de los roles de los usuarios individuales dentro de una empresa.

Sistemas de facturación como fel, factupronto, SAT, no tiene RBAC ya que todos los contribuyentes pueden realizar factura, solo cumpliendo con los requisitos necesarios, además esté se rige solo por un acceso a la plataforma para poder acceder a las herramientas otorgadas.

<https://portalproveedorespepsicomexico.com/CFDPortal/>

El portal de pepsico es para proveedores exclusivamente por lo cual no hay RBAC aplicado, ya que al igual solo existe un acceso para la razón social, en la cual pueden subir sus XML y verificar el estado de sus facturas.

Tiendas en línea: Cuando se hacen compras en líneas el único requisito es registrarse, por lo cual no ocupas tener algun otro privilegio, por lo cual con eso puedes realizar compras, verificar el estado y checar el estatus de el.

* Beneficios y desventajas de este modelo.

Ventajas:

* Los roles admiten jerarquías de roles, una relación padre-hijo, en la que todos los permisos del rol padre son heredados por el rol hijo
* Los roles se asignan naturalmente a la línea de negocio y la estructura organizativa de una empresa
* RBAC es neutral en cuanto a políticas, lo que le permite admitir diferentes políticas de seguridad.
* RBAC permite revisiones más eficientes del acceso a través de Roles Vs. Evaluaciones reales, extremadamente valiosas para los equipos de auditoría en una organización

Desventajas:

* A veces hay roles en las cuales las diferencias son muy pequeñas, lo cual nos lleva a generar nuevos roles que encapsulen adecuadamente los provilegios,el administrar estos roles se pueden volver un asunto complejo
* Debido a las opciones de abstracción que forman la base de RBAC, tampoco es muy adecuado para administrar los derechos individuales

<https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

<https://kubernetes.io/docs/reference/access-authn-authz/rbac/>

<https://security.stackexchange.com/questions/151333/role-based-access-control-disadvantages>