RBAC (role-based access control)

El control de acceso RBAC (acrónimo en inglés de "Role-Based Access Control") es un modelo de control de acceso utilizado en sistemas de información y seguridad informática.

En el modelo RBAC, el acceso a los recursos del sistema se otorga según los roles que desempeñan los usuarios en la organización. En lugar de otorgar permisos individuales a cada usuario, los permisos se asignan a roles específicos y los usuarios se asignan a esos roles según sus responsabilidades dentro de la organización.

Por ejemplo, en un sistema RBAC de una empresa, se podría definir un rol "Administrador de Red" que tenga permisos para configurar la red y un rol "Empleado de Ventas" que tenga acceso a los datos de ventas. Luego, los usuarios de la empresa se asignarían a los roles correspondientes según sus funciones en la organización.

El modelo RBAC se considera una práctica recomendada en la gestión de acceso a los recursos de los sistemas informáticos, ya que simplifica la administración de los permisos y reduce el riesgo de errores o abusos. Además, facilita el seguimiento de la actividad de los usuarios y ayuda a asegurar la confidencialidad, integridad y disponibilidad de los recursos protegidos.

Vamos a ver 3 reglas fundamentales por las cuales se rige el RBAC:

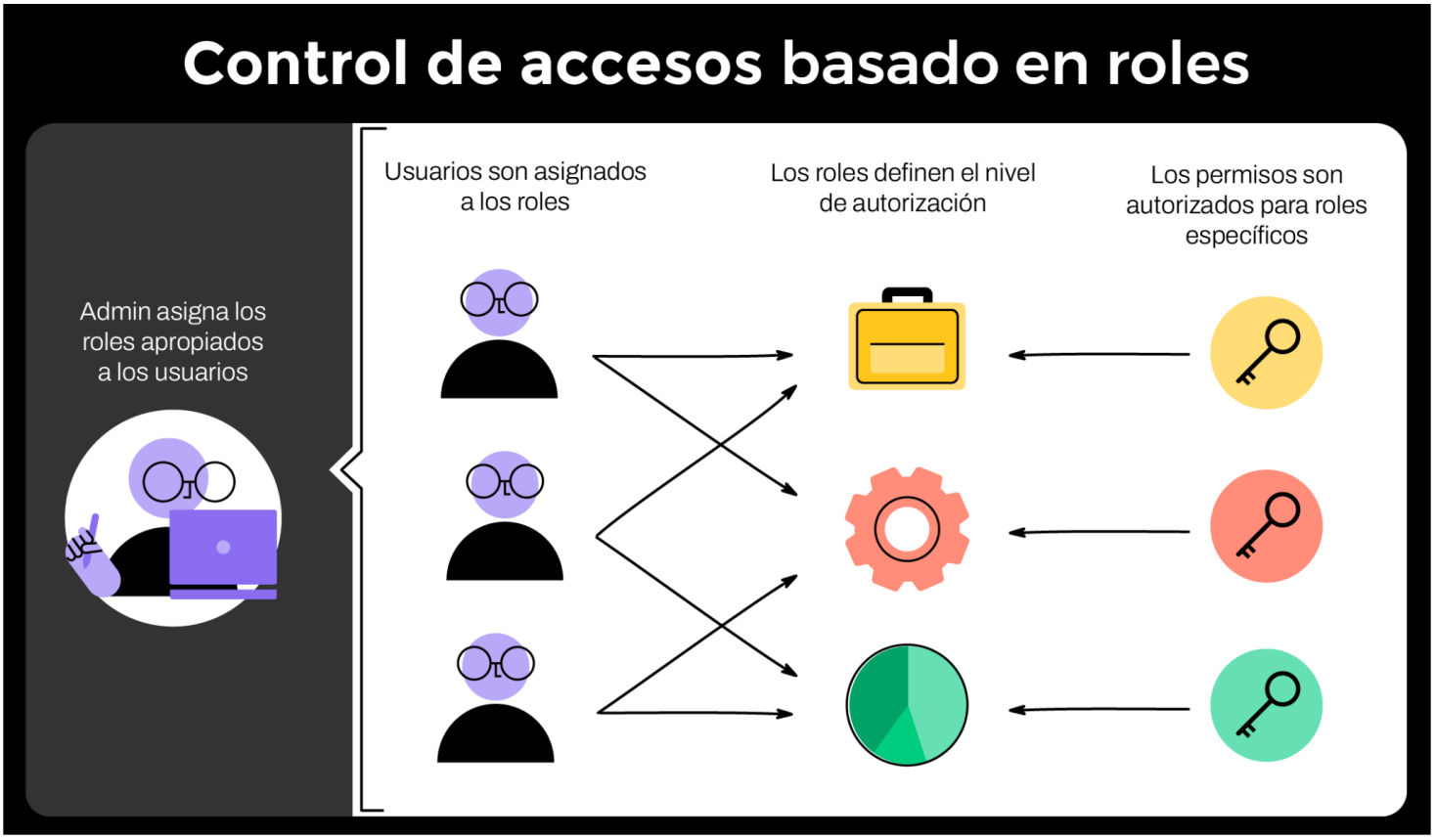
1. **Asignación de roles** un usuario solo puede ejercer privilegios si se le ha asignado un rol.
2. **Autorización basada en roles**: dicho rol del usuario debe estar autorizado, lo que garantiza que los usuarios solo puedan asumir roles para los que están autorizados.
3. **Autorización de privilegios** un usuario puede ejercer ciertos privilegios si, por supuesto, está autorizado para hacerlo.

Por otro lado, el RBAC tiene objetivos o funciones para las cuales está diseñado y orientado. Vamos a conocerlos en la siguientes imágenes:

Funciones de RBAC

Compromiso con el “principio de mínimo privilegio”	RBAC ayuda a lograr la seguridad de **zero trust** (concepto de seguridad que parte de la idea de que, por defecto, las organizaciones nunca deberían confiar en ninguna entidad interna o externa que ingrese a su perímetro), al asignar la menor cantidad de permisos de acceso a un usuario en función de sus roles. Es el rol el cual define el conjunto de permisos que necesita el usuario para realizar las tareas asignadas y que le corresponden.
Reducción de la carga administrativa	RBAC permite **agregar y cambiar roles rápidamente** e implementarlos globalmente en todos los sistemas operativos, plataformas y aplicaciones. Además, reduce la posibilidad de error al asignar permisos de usuario y facilita la integración de usuarios de terceros.
Separación de tareas	Como los roles están separados, en teoría, **ningún usuario individual puede causar una infracción significativa**, estaría limitado a los recursos a los que se le permitió acceder a esa cuenta.
Cumplimiento mejorado	RBAC ayuda con el **cumplimiento de las normas para la protección de datos y la privacidad**, así como con requisitos legales de organismos gubernamentales regionales y locales.

Control de acceso basado en roles



Texto Nexo

Todas estas características hacen del RBAC muy popular en grandes organizaciones que necesitan otorgar acceso a cientos o miles de empleados. Pero también es cada vez más popular entre las organizaciones más pequeñas, ya que a menudo es más fácil de administrar que las listas de control de acceso.

¿Y cómo hace Keycloak para poner en juego este mecanismo de seguridad?

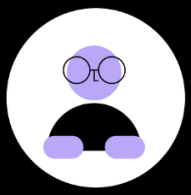
Tipos de roles y sus usos

KEYCLOAK

Tipos de roles y sus usos

De reino

En grandes rasgos, los roles que pertenecen al reino son los que generalmente representan el rol del usuario en la organización, ya que estos son inherentes al reino e independientes de los clients que tengamos definidos en él.



De client

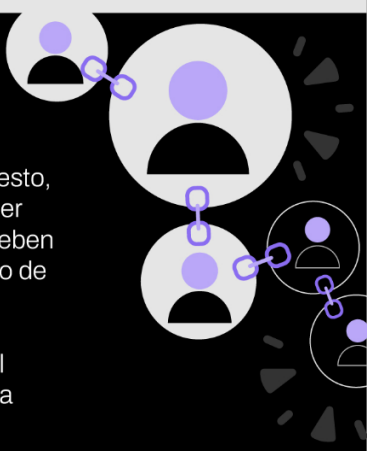
Son específicos de los mismos, por lo que el significado del rol es inherente a su uso dentro del client.

La decisión entre implementar uno u otro depende del alcance que pueda tener el rol. Si es un rol que se repetirá en múltiples clients con el mismo significado, tendrá mayor sentido implementar un rol de reino.

A la hora de crear roles:

- Se deberá tener en cuenta el alcance y la granularidad de los permisos asociados a los mismos dentro de la aplicación.
- Se recomienda no usar roles para autorizaciones de granularidad fina.
- Una gran cantidad de roles en nuestra aplicación generará dificultades a la hora de administrarlos.

Roles compuestos



Keycloak posee el concepto de **roles compuestos**, una especie de rol que encadena otros roles. Cuando a un usuario se le asocia un rol compuesto, se le asocian todos los roles de esta cadena, los cuales también pueden ser roles compuestos. Si bien es una opción que puede resultar muy útil, se deben analizar bien los casos en los cuales utilizarla, ya que tener un gran número de roles encadenados dificulta la administración de roles en la aplicación.

Los roles, además, aumentan el tamaño del token de Keycloak, por lo cual se debe mantener al mínimo el número de roles que un client necesita para autorizar a los usuarios a acceder a los recursos.