Control de acceso basado en roles

El control de acceso basado en roles (RBAC) **consiste en asignar derechos de acceso a los usuarios de su organización en función de sus roles y las tareas que realizan**. Esto garantiza que los usuarios y equipos solo puedan tener acceso a los niveles que pertenezcan.

¿Cómo el control de acceso basado en roles ayuda a prevenir ataques basados en archivos?

Con el **control de acceso basado en roles**, puede configurar el **acceso** de solo lectura para ellos y evitar que copien cualquier información desde un dispositivo externo a su equipo para evitar ataques de malware intencionales o no intencionales

El **acceso basado en roles** se refiere a los derechos de acceso que se pueden asignar a un usuario o un equipo en una organización.
Los derechos de acceso incluyen: establecer permisos de solo lectura, bloquear la copia de datos desde dispositivos USB y configurar un acceso de escritura limitado.

Se le podrán asignar diferentes derechos a los participantes de una empresa o trabajo dependiendo de sus roles, creando grupos específicos para diferentes roles y asignando los derechos de acceso pertenecientes a cada rol.

Proporcionar **acceso exclusivo** a usuarios específicos
Agregar, cambiar o retirar fácilmente los permisos de acceso a archivos

Beneficios del control de acceso basado en roles.

El control de acceso basado en roles evita que deba cambiar las contraseñas del sistema cada vez que haya un cambio de roles en su organización.
. El control de acceso basado en roles le permite cumplir con regulaciones como GDPR, HIPAA, SOX, entre otras para gestionar de manera efectiva cómo se utiliza y accede a la información

El control de acceso controla las posibles violaciones de datos al restringir el acceso a información confidencial

Control de acceso basado en roles

Reduce el potencial de error al asignar permisos de usuario ya que las políticas sistemáticas y repetibles le impiden cometer errores al agregar nuevos usuarios o equipos a la red.

Mejora la seguridad con el control de acceso basado en roles utilizando permisos de solo lectura y bloquear copia de archivos desde dispositivos externos

Desventajas de control de acceso:

Pasar a un sistema RBAC es complejo y lleva tiempo, puesto que es necesario definir y determinar las funciones de cada puesto de trabajo o departamento, para poder crear roles definidos y los permisos necesarios para poder desempeñar el trabajo.