

Control de acceso: quién entra y qué puede hacer



El control de acceso es un conjunto de mecanismos que aseguran que solo los empleados adecuados accedan a los recursos correctos, en el momento correcto. Estos mecanismos se basan en:

Identificación y autenticación

Los empleados declaran su identidad y esta es verificada por el sistema (autenticación).



Los empleados pueden identificarse usando contraseñas, tokens o datos biométricos

Autorización

Se determina a qué recursos puede acceder el empleado y qué acciones puede realizar.



Los empleados deben contar solo con los privilegios necesarios para realizar su trabajo.

Auditoría

Se lleva un registro de todas las acciones que los empleados realizan con los permisos que se le concedieron. Estos registros son detallados, esto con el fin de detectar y prevenir incidentes.

ING. ALDO GM
DESARROLLADOR
BACKEND IV



ID: 977579

UBICACIÓN
DIVISIÓN DE DESARROLLO
DEPARTAMENTO 12 - BACKEND

PRIVILEGIOS LIMITADOS
NIVEL 3/5

ACCESO 0793 - SERVIDOR 15
ACCESO 0102 - CLOUD 3
ACCESO 0546 - ACCESO A INST

ÚLTIMAS ACCIONES REALIZADAS

22-11-2025 19:30 - REINICIÓ SERVIDOR 15. AUT.3452
22-11-2025 9:10 - ACCESO A INSTALACIONES. AUT.3452
21-11-2025 12:51 - ACCESO A CLOUD 3. AUT.0238
21-11-2025 9:28 - ACCESO A SERVIDOR 15. AUT.0124
21-11-2025 9:15 - ACCESO A INSTALACIONES. AUT.3452

El control de acceso es fundamental para la seguridad de la información, su correcta implementación previene problemas como la filtración de datos.

Bibliografía:

Neil, I. (2020). CompTIA Security+: SY0-601 Certification Guide: Complete coverage of the new CompTIA Security+ exam to help you pass on the first attempt (2nd ed.). Packt Publishing.