[FORT] TEMA 9: Configuración y Administración de Cuentas de Usuario

Tipos de cuentas

- Cuenta Federada: Se suelen usar para Azure, permite el multiequipo. Lo malo de esto es que se compromete la privacidad al mandar todos los datos de lo que se hace a Microsoft.
- Cuenta local: Cuenta que solo sirve para un equipo
- Cuenta de Administrador: Usuario con el rol de adminsitrador que tiene ciertos permisos de administración.
- Cuenta de Usuario estándar: Grupo Users, permite el acceso limitado al equipo. También exiten los Usuarios Avanzados, que tienen algunos permisos más.

Gestión de cuentas de usuario

Existen las siguientes opciones para mejorar la seguridad de las cuentas:

- Cambio de tipo de cuenta
- Configuración de permisos y roles
- Contraseñas Seguras
- Autenticación multifactor (MFA)

Configuración de permisos y roles

- Permisos: lo que puede hacer un usuario o un grupo sobre un archivo, carpeta o impresora (Recursos de sistema)
- Roles: conjunto de permisos que se asignan a usuarios para facilitar la gestión.
- Cuentas Invitadas: Tienen los permisos limitados y se usan para usuarios temporales que no necesitan acceso permanente a recursos del sistema.

Asignación de permisos

- Configuración de permisos en archivos y carpetas: Haciendo click derecho y pulsando en seguridad para configurar las ACL
- Uso de grupos: Permite asignar permisos de forma más cómoda. Así se pueden asignar permisos a grupos de usuarios en vez de ir uno por uno.

Configuración de roles con directivas de grupo

Se accede a ellas con gpedit desde Windows + R:

- Directiva de grupo de máquina: Se ejecutan al iniciar o apagar el equipo

- Directiva de grupo de Usuario: Se inicia al logear o desloguear un usuario.
- Aplicar políticas específicas a unidades organizativas

Permite aplicar directivas a nivel de usuario/grupo o a nivel de equipo.

Control de acceso basado en roles (RBAC)

- Implementación de RBAC
- Definir roles necesarios
- Asignar roles específicos a cada rol.

Herramientas de gestión de usuarios

- Adminsitrador de Usuarios y Grupos locales

```
lusrmgr.msc
```

- PowerShell

```
Get-LocalUser
LocalGroupMember
```

- Active directory: Se usa en entornos empresariales para la gestión de usuarios y permisos en una red. Se usa la consola de equipos y usuarios de active directory para gestionar y aplicar políticas de seguridad de forma centralizada.

Buenas prácticas en la configuración de permisos y roles

- Principio de menor privilegio: Asignar solo los permisos necesarios
- Revisión periódica de permisos: Realizar auditorías para asegurar que nadie tiene permisos de más
- Documentación y transparencia: Documentar las políticas de permismos y roles para garantizar claridad y transparencia en la gestión de accesos.

From:
http://www.knoppia.net/ - **Knoppia**

Permanent link:
http://www.knoppia.net/doku.php?id=master_cs:fortificacion:tm9

Last update: **2025/03/17 17:21**