



**S.I.G.I.E**  
Chronos  
Ciberseguridad

Rol	Apellido	Nombre	Cédula Identidad	Email	Tel./Cel.
Coordinador	Chapuis	Juan	5.630.283-4	jchapuis@scuolaitaliana.edu.uy	098844043
Sub-Coordinador	Roizen	Agustín	6.339.592-9	aroizen@scuolaitaliana.edu.uy	097259510
Integrante	Marino	Bruno	5.707.620-6	bmarino@scuolaitaliana.edu.uy	092617596

Docente: Farias, Gustavo

Fecha de entrega: 28/07/2025

**Primera Entrega**



## Manejo de Permisos

### Ubuntu 22.04 LTS (Terminales)

Modelo de Permisos:

Usuarios estándar: Sin acceso root por defecto.

sudo: Configurado para usuarios administrativos mediante grupo sudo.

### Debian 12 (Servidor)

Modelo de Permisos:

Root: Acceso restringido solo a administradores.

sudo: Similar a Ubuntu, pero con configuración más estricta en instalaciones mínimas.

## Políticas de Contraseñas

### Ubuntu 22.04 LTS

Configuración por Defecto:

PAM (Pluggable Authentication Modules):

Archivo de configuración: /etc/pam.d/common-password.

Parámetros clave

password requisite pam\_pwquality.so retry=3 minlen=8 difok=3  
ucredit=-1 lcredit=-1 dcredit=-1



minlen=8: Longitud mínima.

difok=3: Mínimo 3 caracteres diferentes de la contraseña anterior.

ucredit=-1: Requiere al menos 1 letra mayúscula.

lcredit=-1: Requiere al menos 1 letra minúscula.

dcredit=-1: Requiere al menos 1 dígito.

### **Herramientas de Gestión:**

passwd: Para cambiar contraseñas.

chage: Para forzar cambio periódico (ej: chage -M 90 usuario).

### **Debian 12**

Configuración por Defecto:

pwquality: Similar a Ubuntu, pero con reglas más estrictas en entornos empresariales.

bash

/etc/security/pwquality.conf:

minlen = 12

minclass = 3 # Requiere 3 de 4 tipos (mayúsculas, minúsculas, dígitos, símbolos).

Expiración de Contraseñas:

bash

/etc/login.defs:

PASS\_MAX\_DAYS 90

PASS\_MIN\_DAYS 7



PASS\_WARN\_AGE 14

Comandos Clave:

pwscore: Evalúa fortaleza de contraseñas.

faillock: Bloqueo temporal tras intentos fallidos (configurable en /etc/security/faillock.conf).