

UNIVERSIDADE DE SÃO PAULO
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO – DTI-RP
SEÇÃO DE DATACENTER

Configuração básica de segurança em ambiente Linux:

- 1) Bloquear acesso do usuário “root” via SSH**
 - Modificar o arquivo `/etc/sshd/sshd_config`
 - Modificar o parâmetro `PermitRootLogin` para “no”
 - `PermitRootLogin no`

- 2) Permitir usuários específicos no SSH**
 - Modificar o arquivo `/etc/sshd/sshd_config`
 - Adicionar usuários no parâmetro `AllowUsers` separados por espaço
 - `AllowUsers user1 user2`

- 3) Definir senha segura para o usuário “root”**

- 4) Permitir IPs específicos no Firewall da Cloud USP na porta pública do SSH**

- 5) Permitir IPs específicos para acesso SSH**
 - Alterar arquivos “`hosts.deny`” e “`hosts.allow`” no diretório `/etc`
 - `hosts.allow` → ALL: IP1 IP2 IP3
 - `hosts.deny` → ALL: ALL