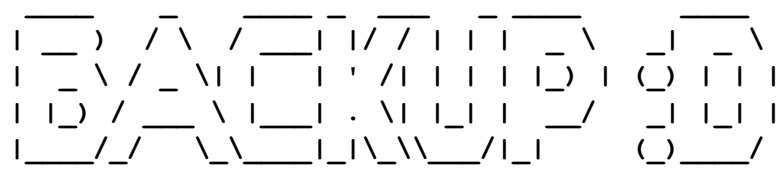


Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

Política de Copias de Seguridad para Sistemas de Información (Propuesta de lineamientos)

Introducción

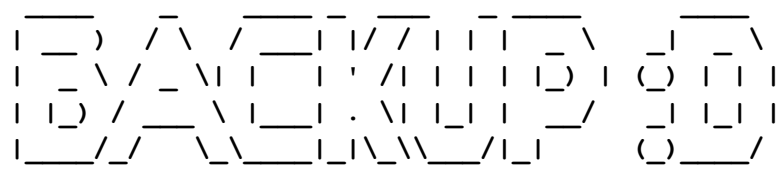
Esta política establece los procedimientos para garantizar la disponibilidad, integridad y seguridad de los datos del proyecto SENTINEL ante incidentes. Esta política es fundamental para proteger los activos de información críticos de SENTINEL y mantener la confianza en un entorno de amenazas cibernéticas en constante evolución.

Objetivos

- Garantizar la protección de los datos críticos de SENTINEL.
- Asegurar la disponibilidad de copias de seguridad recientes y verificadas.
- Definir procedimientos de restauración rápidos y confiables.
- Priorizar la recuperación de sistemas y datos críticos para minimizar el tiempo de inactividad
- Implementar mecanismos de cifrado y verificación de integridad.

Tipos de Copias de Seguridad

Tipo	**Descripción**
Backup Completo	Respaldo completo de directorios críticos (/etc, /opt, /home, /var/www) almacenado en formato .tar.gz.gpg con cifrado GPG.
Backup Incremental	Captura cambios desde el último backup completo para optimizar



Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

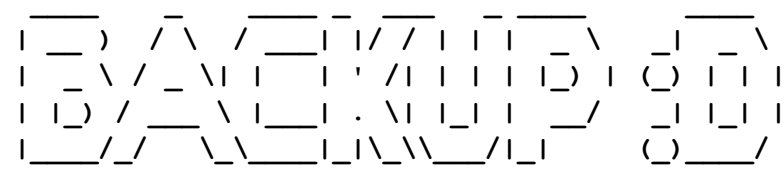
	almacenamiento y velocidad del proceso.

Procedimiento de Copia de Seguridad

1. **Ejecución del Script:** Manual con parámetro "tot" para completo o "int" para incremental
2. **Compresión y Cifrado:** Datos comprimidos con tar y cifrados con GPG usando AES256.
3. **Verificación de Integridad:** Implícita en el proceso de GPG.
4. **Almacenamiento Local:** En /root/backups.
5. **Registro en Log:** Documentación en /var/log/backup.log.
6. **Notificación:** Correo de confirmación al administrador **(sentinelmlbjp@gmail.com).**

Procedimiento de Restauración

1. **Selección del Backup:** Identificar el archivo .gpg más reciente o requerido.
2. **Desencriptación:** Uso de GPG con la frase de paso correcta para recuperar datos.
3. **Extracción de Archivos:** Desempaquetado del archivo .tar.gz.
4. **Restauración Selectiva:** Copia de archivos necesarios al sistema.
5. **Registro:** Documentación manual del proceso de restauración.
6. **Verificación:** Comprobación de la integridad y funcionalidad de los datos restaurados.



Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

Consideraciones Adicionales

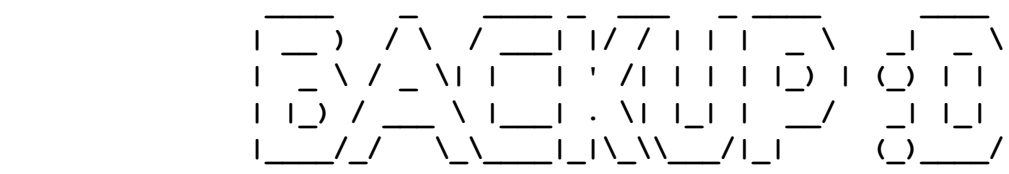
- **Contraseña :** Se utiliza una frase de paso predefinida para el cifrado GPG.
- **Directorios Respaldados:** /etc, /opt, /home, /var/www.
- **Herramientas Utilizadas:** rsync para copia, tar para compresión, GPG para cifrado, ngrok como túnel .

Infraestructura y Comunicaciones

- **Dispositivo Principal:** Se utiliza una Raspberry Pi como servidor de backup remoto del proyecto SENTINEL.
- **Túnel Seguro:** Se implementa ngrok para crear un túnel seguro y exponer los servicios locales de la Raspberry Pi a Internet.
- **Sistema de Correo:**
    - Se utiliza una máquina con Alpine Linux para el envío de correos electrónicos.
    - La herramienta msmtp está configurada en Alpine para el envío de correos a través de Gmail.
    - Los correos de notificación se envían desde la máquina Alpine a una cuenta de Gmail designada.

Seguridad de Comunicaciones

- **Configuración de msmtp:** Se debe asegurar que el archivo de configuración /etc/msmtprc en la máquina Alpine contiene los detalles de autenticación y servidor de Gmail correctos



Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz
yseguros.

- **Autenticación de Gmail:** Verificar que la configuración de seguridad de la cuenta de Gmail permite el acceso de la aplicación msmtp, considerando el uso de autenticación OAuth2 para mayor seguridad.

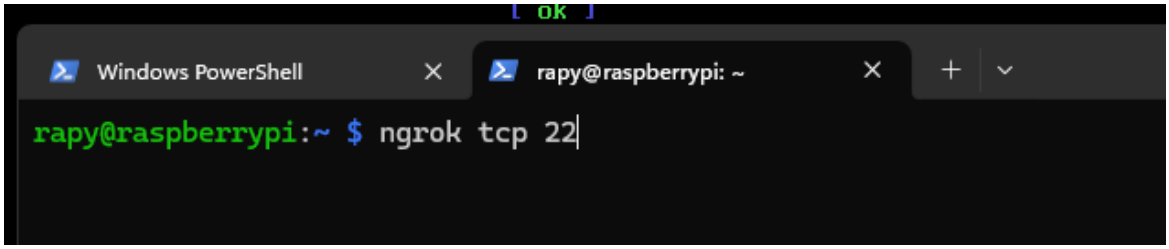
Responsabilidades en las asignaciones de roles:

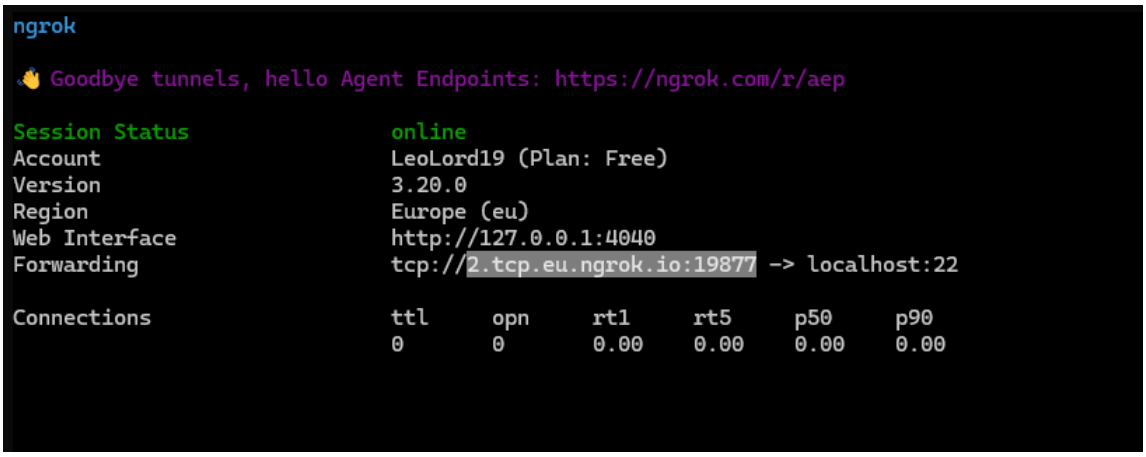
- **Responsable principal(Joel):** Encargado de supervisar todo el proceso de backup y tomar decisiones críticas.
- **Operadores de backup(Bea y Leo):** Personal técnico que ejecuta las copias de seguridad según el calendario establecido.
- **Verificadores(Gea y Marc):** Encargados de comprobar la integridad y accesibilidad de los backups realizados.

Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

Pruebas de comprobación

1. Creamos el túnel tcp en el puerto 22 del servidor remoto. **(raspberrypi pi)**





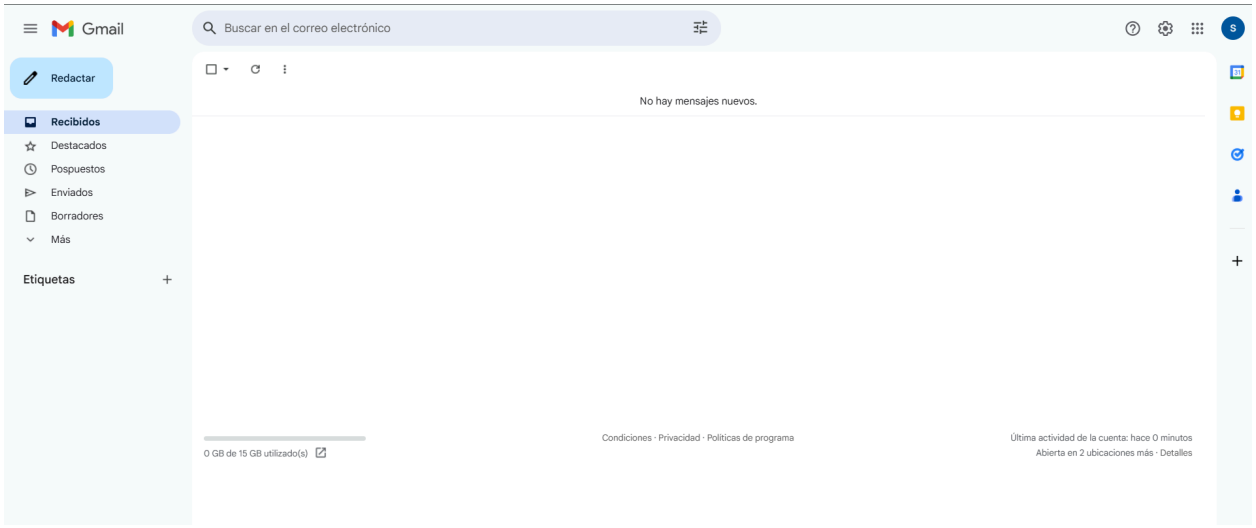
```
 ____    _    ____ _   ___   _ ____        ____
| __ )  / \  / ___| |/ / | | |  _ \      / ___|
|  _ \ / _ \| |   | ' /| | | | |_) |____| |  _
| |_) / ___ \ |___| . \| |_| |  __/_____| |_| |
|____/_/   \_\____|_|\_\\___/|_|        (_)____/
```

Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

```
rapy@raspberrypi:~/Documents/backup_test $ ls -la
total 8
drwxr-sr-x 2 rapy rapy 4096 Feb 25 22:14 .
drwxr-xr-x 3 rapy rapy 4096 Feb 25 00:36 ..
rapy@raspberrypi:~/Documents/backup_test $
```

```
~/scripts # /bin/sh ./backup.sh
Uso: ./backup.sh {tot|int}
~/scripts #
```

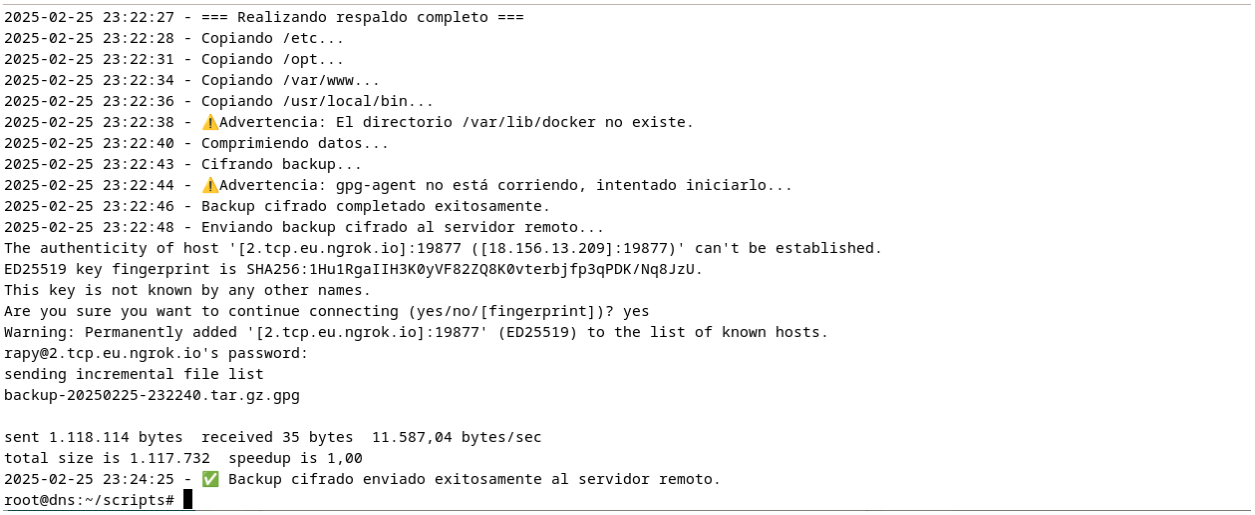
Captura del correo vacío



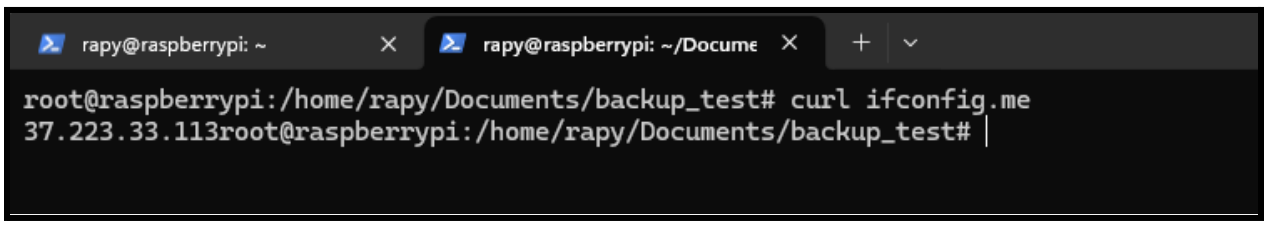
Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

SERVIDOR QUE ENVÍA EL BACKUP (92.178.173.14)

Capturas del backup completo y enviado al servidor remoto



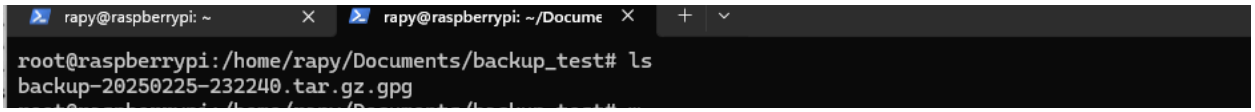
SERVIDOR QUE RECIBE EL BACKUP (37.223.33.113)



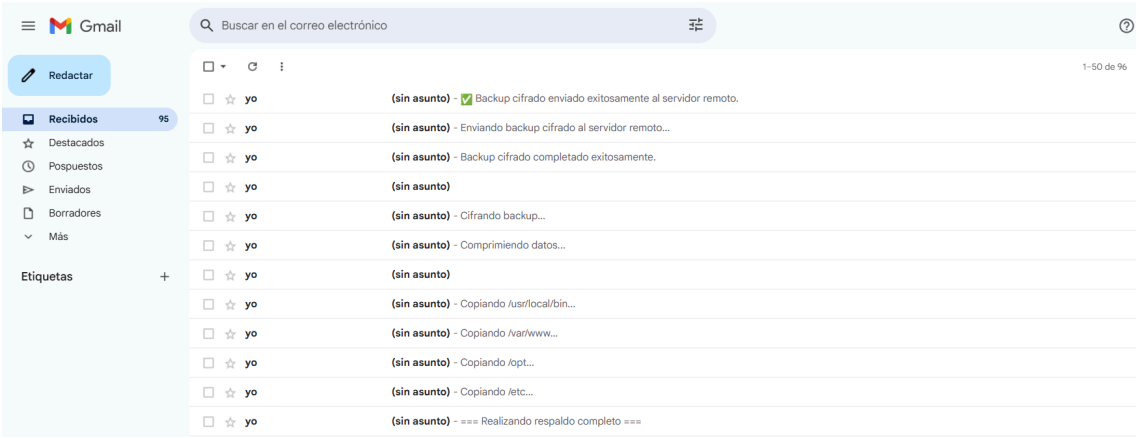
Backup en la raspberry pi

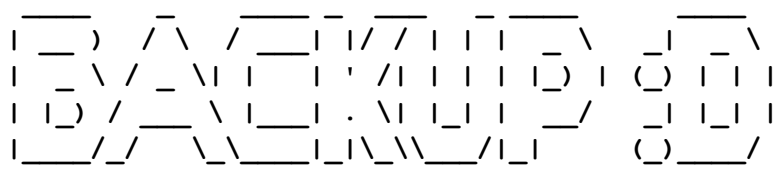
```
 ____    _    ____ _  ___   _ ____       ____
| __ )  / \  / ___| |/ / | | |  _ \     / ___|
|  _ \ / _ \| |   | ' /| | | | |_) |   | |  _
| |_) / ___ \ |___| . \| |_| |  __/    | |_| |
|____/_/   \_\____|_|\_\\___/|_|        \____|
```

Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz



Registro de correo con el backup completo





Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

Backup incremental

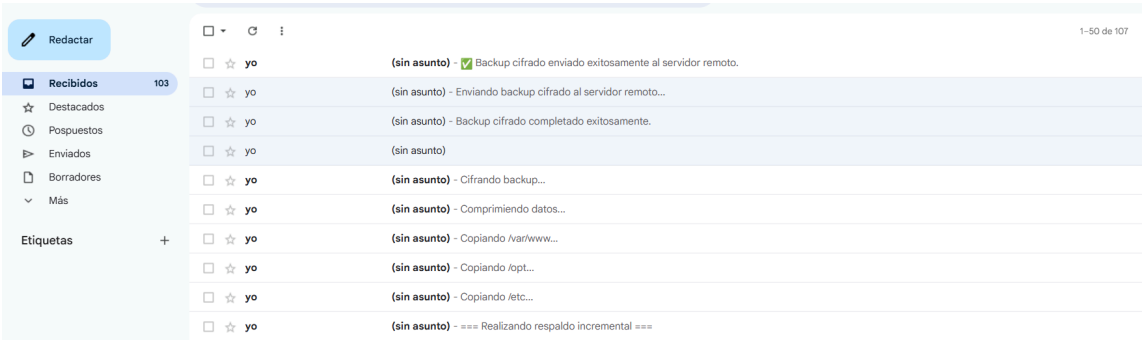
dns1@dns: ~

```
rsync: [sender] link_stat "/var/lib/docker" failed: No such file or directory (2)
--link-dest arg does not exist: /root/backups/backup-20250225-232240.tar.gz
rsync error: some files/attrs were not transferred (see previous errors) (code 23) at main.c(1338) [sender=
2025-02-25 23:33:21 - Error al copiar en respaldo incremental
root@dns:~/scripts# nano backup.sh
root@dns:~/scripts# ./backup.sh int
--link-dest arg does not exist: /root/backups/backup-20250225-232240.tar.gz
2025-02-25 23:39:20 - === Realizando respaldo incremental ===
2025-02-25 23:39:22 - Copiando /etc...
2025-02-25 23:39:25 - Copiando /opt...
2025-02-25 23:39:27 - Copiando /var/www...
2025-02-25 23:39:29 - Comprimiendo datos...
2025-02-25 23:39:32 - Cifrando backup...
2025-02-25 23:39:34 - ⚠️Advertencia: gpg-agent no está corriendo, intentado iniciarlo...
2025-02-25 23:39:37 - Backup cifrado completado exitosamente.
2025-02-25 23:39:38 - Enviando backup cifrado al servidor remoto...
rapy@2.tcp.eu.ngrok.io's password:
sending incremental file list
backup-20250225-233929.tar.gz.gpg

sent 1.118.114 bytes  received 35 bytes  15.860,27 bytes/sec
total size is 1.117.732  speedup is 1,00
2025-02-25 23:40:50 - ✅ Backup cifrado enviado exitosamente al servidor remoto.
root@dns:~/scripts#
```

Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

Capturas de correos recibidos del backup incremental

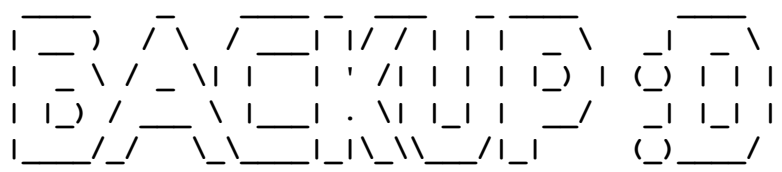


Ejecución del restore

dns1@dns: ~

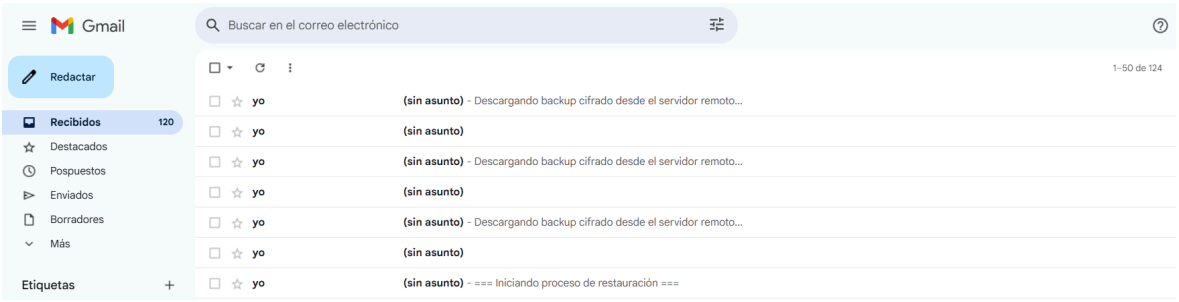
```
root@dns:~/scripts# ./restore.sh backup-20250225-232240.tar.gz.gpg
2025-02-26 00:05:37 - Descargando backup cifrado desde el servidor remoto...
rapy@2.tcp.eu.ngrok.io's password:
receiving incremental file list
backup-20250225-232240.tar.gz.gpg

sent 6.397 bytes  received 1.118.115 bytes  118.369,68 bytes/sec
total size is 1.117.732  speedup is 0,99
2025-02-26 00:05:48 - ✅ Backup cifrado descargado exitosamente.
2025-02-26 00:05:50 - Descifrando backup...
gpg: datos cifrados AES256.CFB
gpg: cifrado con 1 frase contraseña
2025-02-26 00:05:52 - ✅ Backup descifrado exitosamente.
2025-02-26 00:05:54 - Extrayendo backup...
2025-02-26 00:05:56 - ✅ Backup extraído exitosamente en /root/restored.
2025-02-26 00:05:57 - === Restauración completada exitosamente ===
root@dns:~/scripts#
```



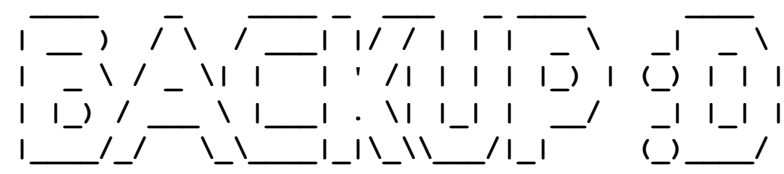
Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz

Correos pruebas del restore



Adjunto de capturas del restored

```
root@dns:~/scripts# cd ..
root@dns:~# ls
backups  restored  scripts
root@dns:~# cd restored/
root@dns:~/restored# ls
bin  etc  opt  www
root@dns:~/restored#
```



Leonardo Duarte Marc Montouto
Beatriz Suarez Joel Diaz