Backups con Borg

Pontificia Universidad
JAVERIANA
Bogotá

"Los buenos programadores saben escribir código.
Los grandes programadores saben reutilizar código."

Eric S. Raymond

Gestión de riesgos

- **Amenazas** (factores externos fuera del control de la entidad):
  - Daños en Hardware o Software.
  - Obsolescencia Tecnológica.
  - Golpes Físicos.
  - Picos de Electricidad.
  - Tormentas Eléctricas.
  - Humedad y Condiciones Ambientales Adversas.
  - Inundaciones y Desastres Naturales.
  - Ransomware y Ataques de Malware.
  - Ladrones y ciberdelincuentes.

Memorias de la charla

Gestión de riesgos

- **Vulnerabilidades** (factores internos bajo el control de la entidad):
  - Almacenamiento centralizado, sin redundancia ni copias de respaldo.
  - Falta de Monitoreo y Detección de Intrusiones.
  - Ausencia de Actualizaciones y Parches de Seguridad.
  - Dependencia de Personal Clave.
  - Falta de control de acceso, autenticación o inadecuada autorización.
  - Usuarios no capacitados o no sensibilizados.
  - Funcionarios descuidados con los equipos o medios de almacenamiento.

Memorias de la charla

Escenarios del riesgo: Pérdida de datos

- **Golpes Físicos x Almacenamiento Centralizado**: Si toda la información está almacenada en un único dispositivo físico, cualquier daño accidental o incidente físico puede resultar en la pérdida completa de los datos.
- **Ransomware x Falta de alertas tempranas**: Un ataque de ransomware que no se contenga adecuada y oportunamente puede encriptar todos los datos críticos de la organización. El pago del rescate no garantiza la recuperación de la información.
- **Pérdida de dispositivos x Funcionarios descuidados**: La desaparición de un computador portátil generalmente es más peligrosa por el valor de la información almacenada en el equipo que el valor del computador portátil.

Memorias de la charla

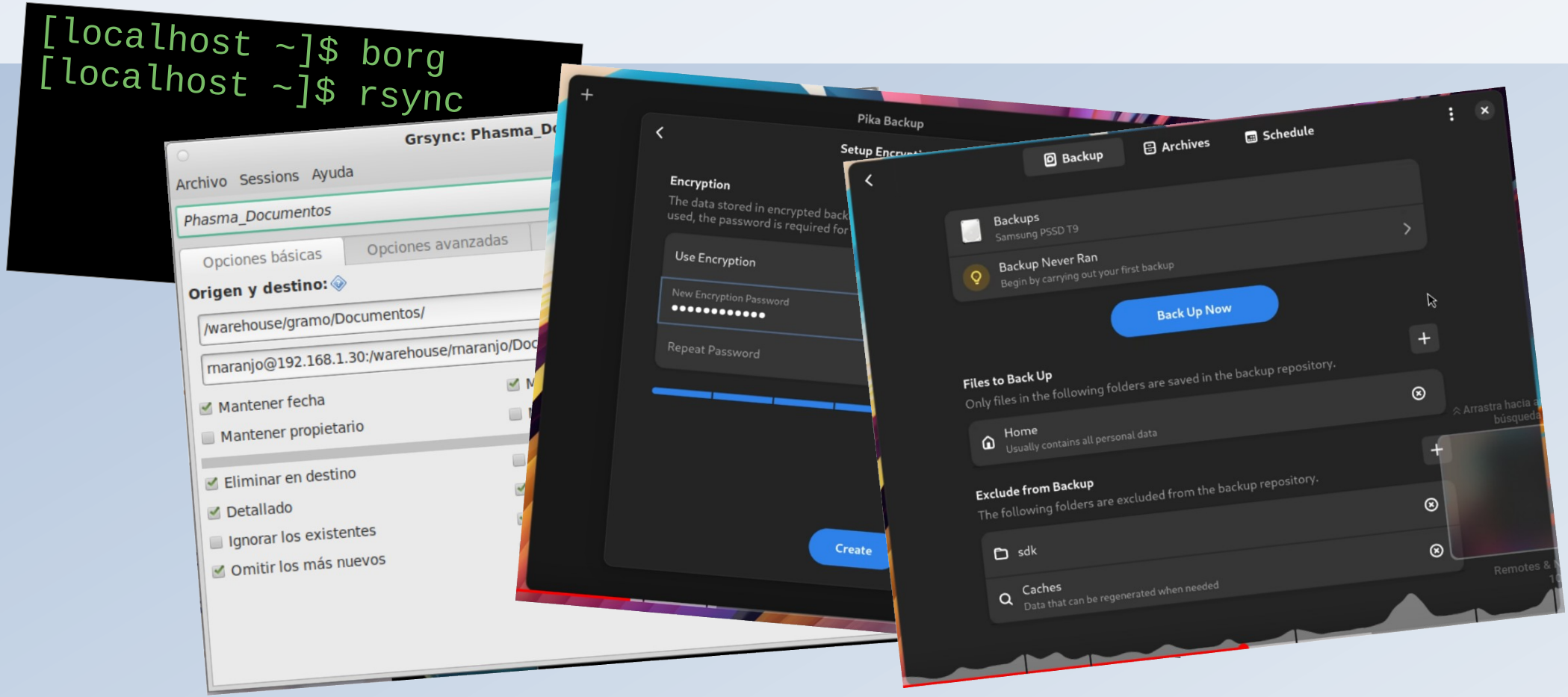
El backup para evitar la pérdida de datos

- Eficaz siempre y cuando:
  - Periodicidad adecuada.
  - Almacenamiento redundante.
  - Disciplina y monitoreo.
  - Retención de suficientes versiones.
  - Almacenamiento seguro / cifrado.
  - Alineado con la ley y regulación.

Cómo hacer un plan de backups

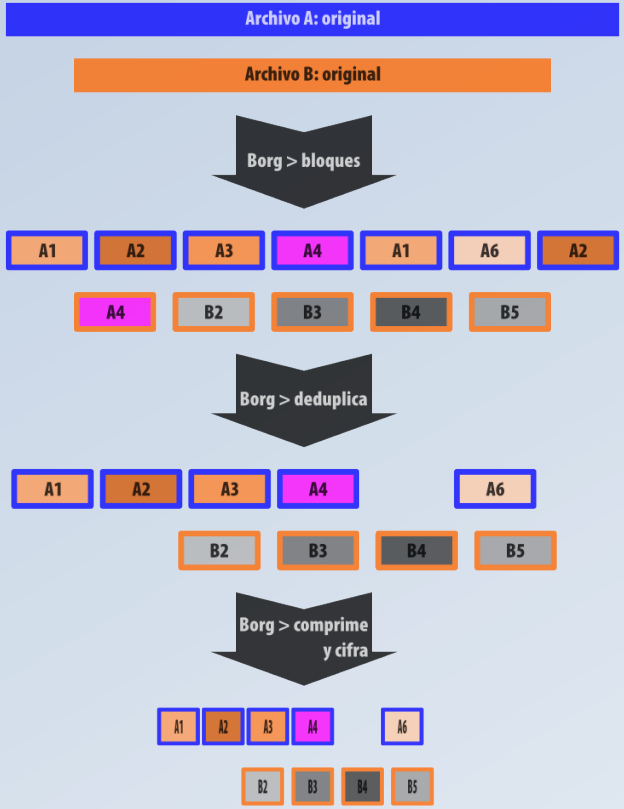
- Eficiente siempre y cuando:
  - Elección adecuada de los datos a respaldar.
  - Segmentación adecuada de la información.
  - Balance adecuado entre frecuencia y retención.
  - Determinar la antigüedad requerida.
  - Se evite la duplicación de datos.
  - Se compriman los datos.
  - Se diseñe un plan de recuperación
    - Tiempos / Tamaño / Orden

Herramientas en software libre



Borg backup

- Diseñada para realizar copias de seguridad:
  - Por bloques.
  - Deduplicadas.
  - Comprimidas.
  - Cifradas.
  - Incrementales.
  - Almacenamiento en repositorios remotos.
  - Transferencia segura.
- Desarrollada en Python.
- Optimizada para manejar grandes volúmenes de datos.
- Enfoque en la eficiencia, la seguridad y la flexibilidad.
- BSD-3-Clause License.



Instalación

- Debian/Ubuntu:
  - `sudo apt-get install borgbackup`
- RHEL/CentOS/Fedora (DNF):
  - `sudo yum -y install borgbackup`
  - `sudo dnf install borgbackup`
- Mageia (urpmi):
  - convertirse en superusuario con `su -`
  - luego `urpmi borgbackup`
- Arch Linux (pacman):
  - `sudo pacman -S borg`

Almacenamiento local de los backups

- Crear un repositorio de Borg con cifrado:
  - `borg init --encryption=repokey /backup/repositorio`
- Crear un backup de una carpeta específica indicando la fecha de realización:
  - `borg create /backup/repositorio::snapshot-YYYYMMDD /home/usuario/originales`
- Verificar el backup creado:
  - `borg list /backup/repositorio`
- Probar la restauración del backup:
  - `borg extract /backup/repositorio::snapshot-YYYYMMDD --target /ruta/de/restaura`
- Crear un backup excluyendo una subcarpeta específica:
  - `borg create --exclude '/home/usuario/originales/no_sacar_backup' /backup/repositorio::snapshot-YYYYMMDD /home/usuario/originales`
- Extraer un archivo a una ubicación diferente a la original:
  - `borg extract --output /ruta/de/destino /backup/repositorio::snapshot-YYYYMMDD /carpeta/original/archivo_especifico.ext`

Almacenamiento remoto de los backups

- Inicializar el Repositorio Remoto
  - `borg init --encryption=repokey ssh://backupusr@192.168.1.55:/ruta/al/repositorio`
- Crear el Backup Excluyendo una Subcarpeta:
  - `borg create --exclude '/home/usuario/originales/no_sacar_backup' ssh://backupusr@192.168.1.55:/ruta/al/repositorio:: snapshot-$(date +%Y-%m-%d) /home/usuario/originales`
- Verificar el Backup Remoto:
  - `borg list ssh://backupusr@192.168.1.55:/ruta/al/repositorio`
- Probar la Restauración de un Backup Remoto:
  - `borg extract ssh://backupusr@192.168.1.55:/ruta/al/repositorio::snapshot-$(date +%Y-%m-%d) --target /ruta/de/restauracion`
- Backup remoto utilizando compresión y excluyendo una carpeta específica:
  - `borg create --compression lz4 usuario@servidor:/ruta/remota/del/repositorio::snapshot-$(date +%Y-%m-%d) /ruta/archivos/originales`

A tener en cuenta

- Políticas de retención
  - Gestionar el ciclo de vida y eliminar versiones antiguas:
  - `borg prune --keep-daily=7 --keep-weekly=4 --keep-monthly=6 /ruta/al/repositorio`
  - `borg prune --keep-last=10 /ruta/al/repositorio`
  - `borg prune -v --list --dry-run --keep-daily=7 --keep-weekly=4 /ruta/al/repositorio`
- Seguridad del Repositorio y Acceso SSH
  - Uso de Claves SSH en lugar de usar contraseñas.
  - `ssh-keygen`
  - `ssh-copy-id`
- Restricción de Usuarios
  - Rechazar el acceso root directo `PermitRootLogin no`
  - Aceptar solo autenticación basada en claves `PasswordAuthentication no`

A tener en cuenta

- Firewall y Seguridad de Red
  - iptables
  - ufw
- Cifrado de Datos
  - `--encryption=none`: Sin cifrado.
  - `--encryption=repokey`:Utiliza una clave almacenada en el repositorio.
  - `--encryption=keyfile`: Utiliza una clave almacenada en un archivo separado.
  - `--encryption=repokey-blake2`: Similar a repokey, pero utiliza el algoritmo Blake2 para el cifrado.
  - `--encryption=keyfile-blake2`: Similar a keyfile, pero utiliza el algoritmo Blake2 para el cifrado.

¿Preguntas?

Memorias de la charla