FORTALECIENDO LA RESILIENCIA CONTRA RANSOMWARE MEDIANTE ESTRATEGIAS DE BACKUP OPTIMIZADAS CON BACULA

Fernando Ares Robledo

Master en Ciberseguridad

Tutor: Rafael Páez Reyes

18 de junio de 2024

Índice

Contexto y Justificación

- **Contexto:**
  - Los ataques de ransomware son una de las amenazas más significativas y disruptivas en el mundo digital.
  - Este malware cifra los archivos y exige un rescate.
  - La protección de datos críticos es urgente debido al aumento de la frecuencia y sofisticación de estos ataques.
- **Consecuencias de los ataques:**
  - Impacto financiero directo por el rescate.
  - Interrupciones operativas y pérdida de datos críticos.
  - Daños a la reputación.
  - Costos asociados con la recuperación del sistema.
- Diversas estrategias existen, pero la implementación efectiva de backups es una de las más confiables y efectivas.

Aportación Realizada

- **Objetivo del TFM:**
  - Desarrollar una solución basada en Bacula para una estrategia de protección de datos contra ransomware.
- **Metas:**
  - Demostrar la eficacia de los backups.
    - Minimizar la pérdida de datos y el impacto operacional.
  - Optimización de Bacula.
    - Configuración y gestión específica para enfrentar ransomware.
    - Mejores prácticas en programación de backups, retención de datos y recuperación rápida.

Objetivos Generales y Específicos

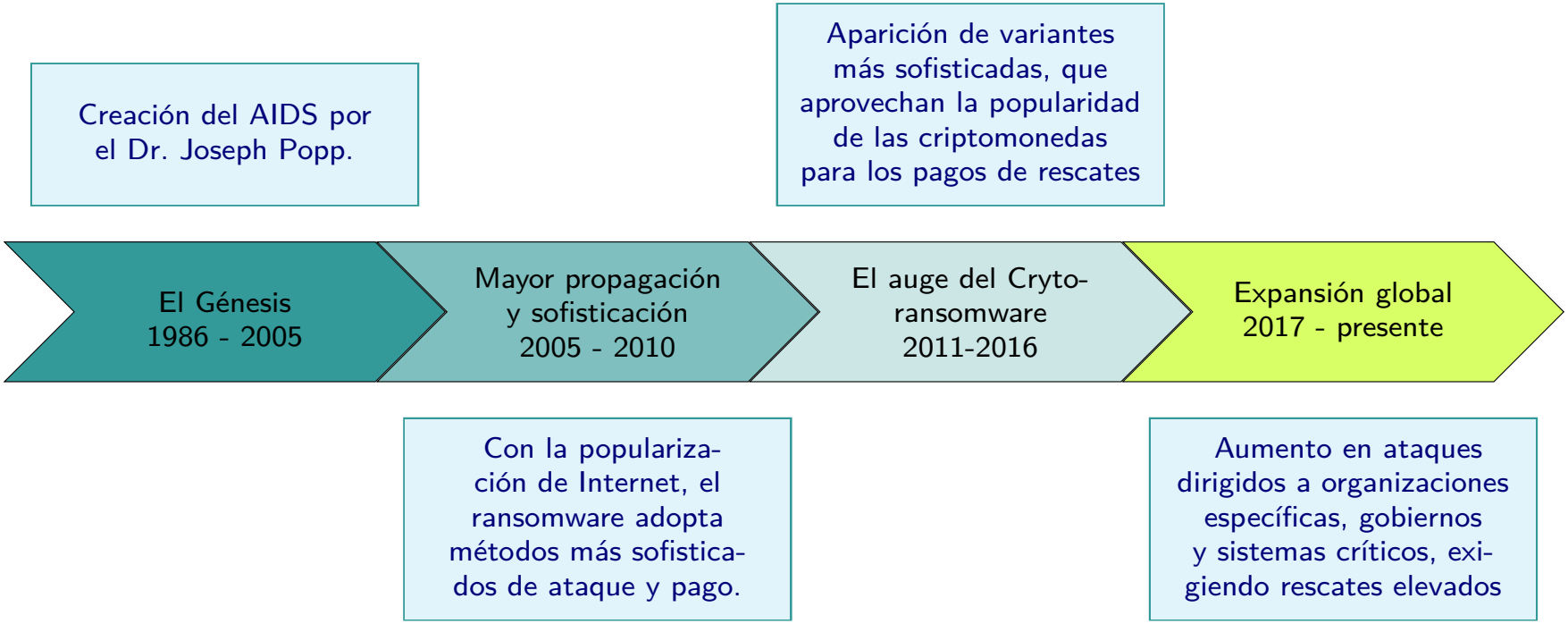
Objetivos Generales:

- Desarrollar una comprensión básica de los mecanismos y efectos del ransomware, así como de la importancia de los backups en la recuperación de ataques de ransomware.
- Implementar una solución de backup con Bacula que demuestre ser efectiva en la recuperación de datos tras un ataque de ransomware.

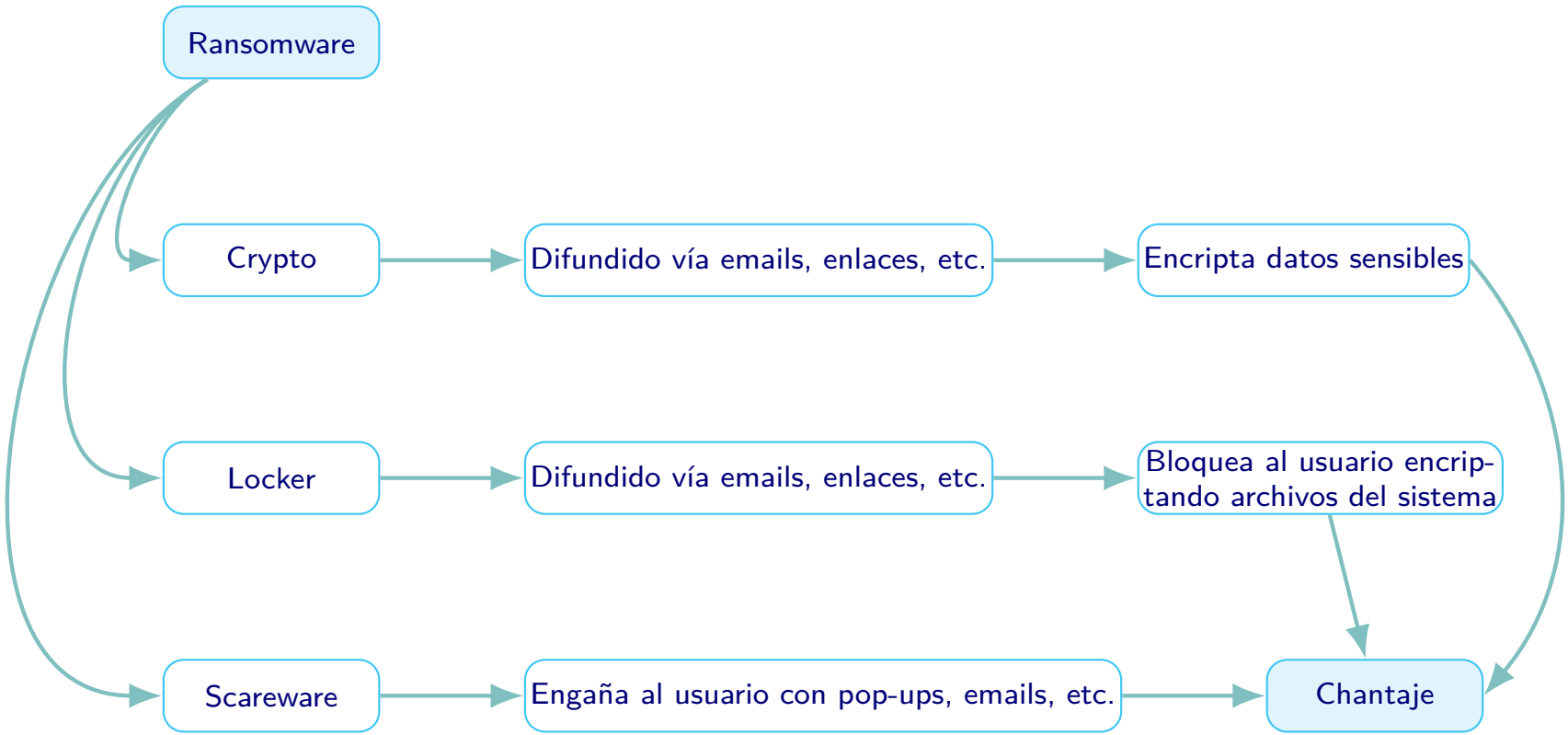
Objetivos Específicos:

- Analizar las capacidades y configuraciones óptimas de Bacula para la protección contra ransomware.
- Implementar un entorno de prueba con Bacula.
- Desarrollar una guía de mejores prácticas para el uso de Bacula en la protección contra ransomware.
- Evaluar la viabilidad y eficiencia de la solución propuesta.

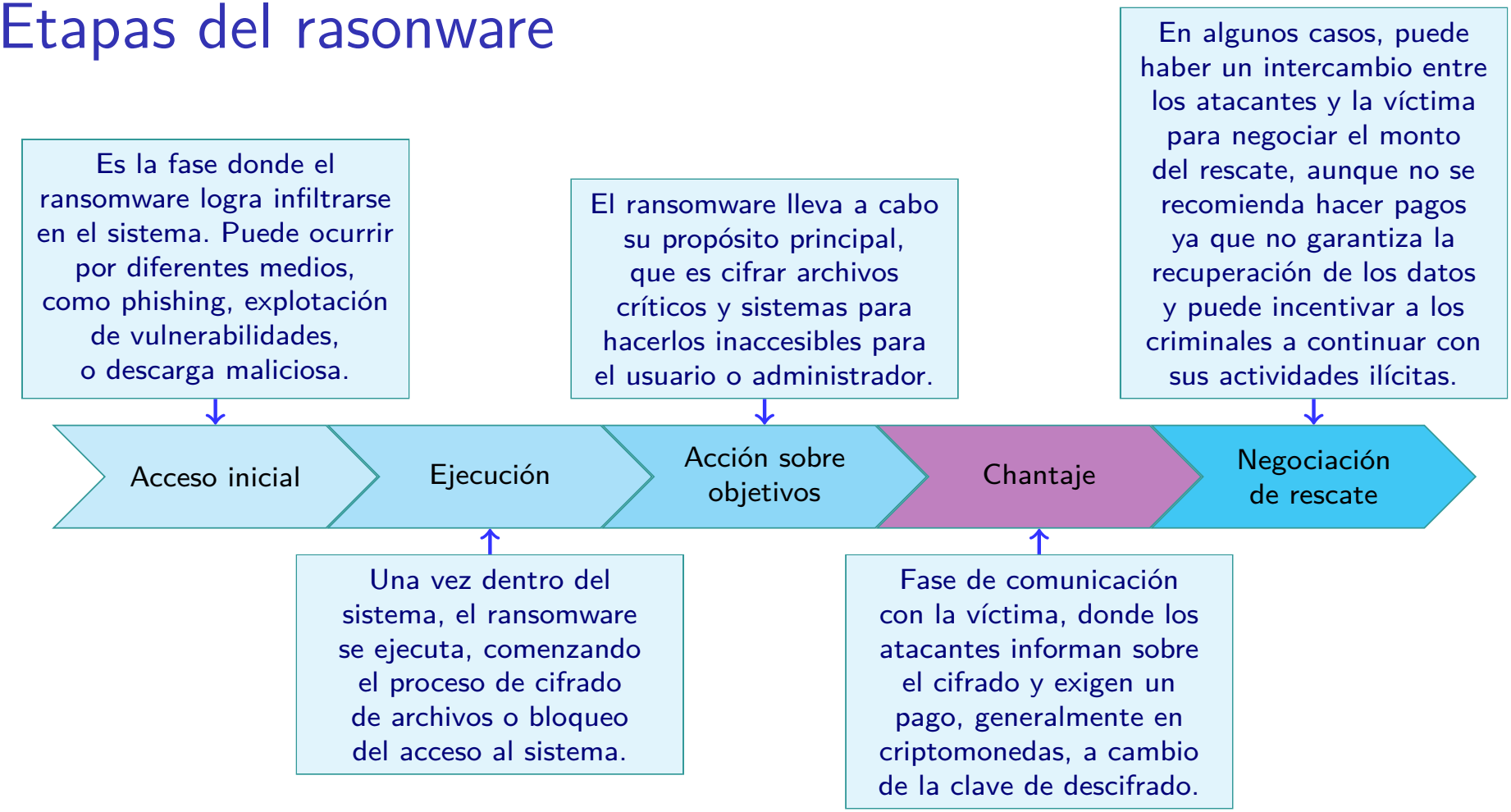
Historia


Creación del AIDS por el Dr. Joseph Popp.
Aparición de variantes más sofisticadas, que aprovechan la popularidad de las criptomonedas para los pagos de rescates
El Génesis 1986 - 2005
Mayor propagación y sofisticación 2005 - 2010
El auge del Cryto-ransomware 2011-2016
Expansión global 2017 - presente
Con la popularización de Internet, el ransomware adopta métodos más sofisticados de ataque y pago.
Aumento en ataques dirigidos a organizaciones específicas, gobiernos y sistemas críticos, exigiendo rescates elevados

Tipos de rasonware



Etapas del rasonware



Vectores de Ataque

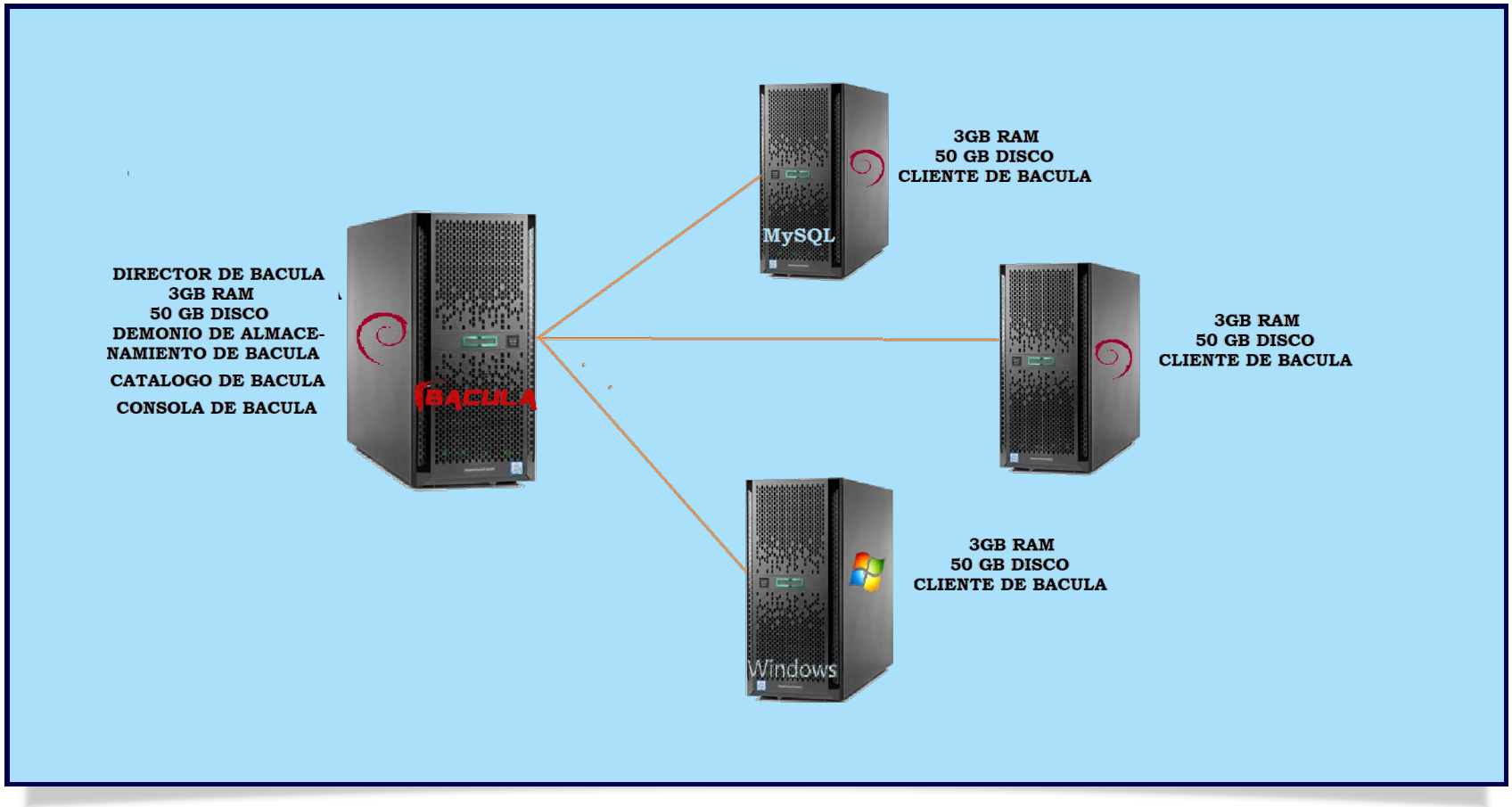
- **Phishing:**
  - Uso de correos electrónicos y mensajes engañosos para obtener información sensible.
  - Los atacantes se hacen pasar por entidades legítimas.
- **Explotación de Vulnerabilidades:**
  - Aprovechamiento de debilidades técnicas en software y hardware.
  - Búsqueda de fallos de seguridad para acceso no autorizado.
- **Abuso de Credenciales:**
  - Uso indebido de contraseñas débiles o comprometidas.
  - Obtención de acceso mediante ingeniería social o fuerza bruta.

Bacula

✓Control de trabajos: Programaciones automáticas, ejecución simultánea, secuenciación por prioridad.
✓Seguridad: Verificación de archivos, autenticación CRAM-MD5, encriptación TLS y de datos, firmas digitales.
✓Restauración avanzada: Restauración interactiva, recuperación completa del sistema, restauración de catálogos.
✓Gestión de catálogo SQL: Soporta MySQL, PostgreSQL, SQLite.
✓Administración de volúmenes y piscinas, gestión flexible de almacenamiento.
✓Soporte multiplataforma: Compatible con múltiples SO, compresión GZIP, coherencia en Win32 con VSS.

✗Programación interna limitada, manejo estático de prioridades.

Arquitectura de nuestro sistema



Implementación de Bacula

¿Qué?

Especificar qué datos serán incluidos mediante un FileSet. Precisar exclusiones para omitir archivos innecesarios.

¿Cuándo?

Definir cuándo se realizarán los backups con un Schedule. Configurar eventos para distintos tipos de backups (completo, incremental, diferencial).

¿Dónde?

Agregar el cliente o los clientes que serán parte del backup.

Creación del Job

- Vincular FileSet, Client, y Schedule.
- Definir el tipo y destino del Job.
- Configurar políticas de retención y opciones avanzadas.

Ejecución del Job

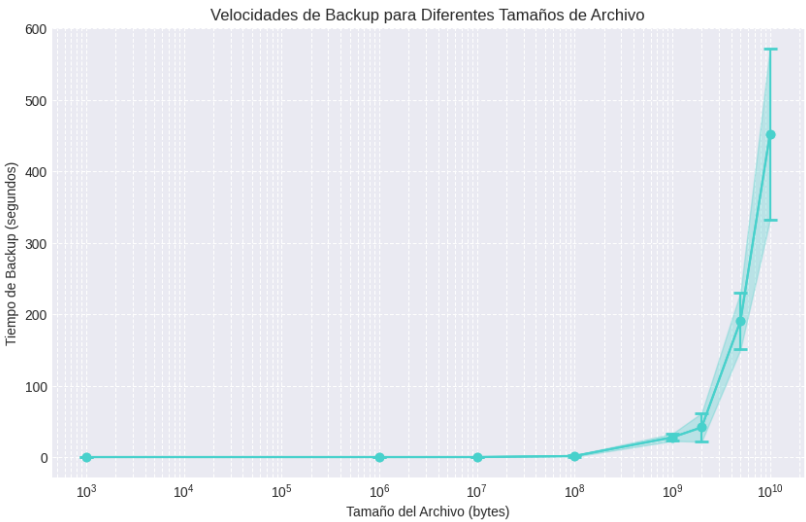
- Ejecutar manualmente o automáticamente según la programación.
- Gestionar la transferencia de datos según las políticas definidas.

Disaster Recovery Plan con Bacula

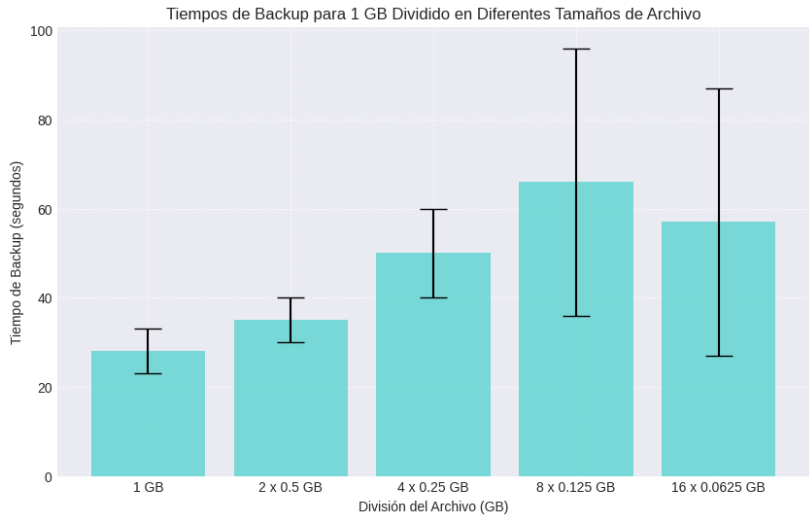
- **Importancia del DRP:**
  - Protege contra pérdida de datos y sistemas críticos.
  - Minimiza el impacto financiero y de reputación.
- **Evaluación de Riesgos:**
  - Identificación de riesgos: fallas de hardware, ataques cibernéticos, desastres naturales, errores humanos.
  - Análisis de riesgos: probabilidad e impacto potencial.
- **Soluciones de Bacula para la Recuperación:**
  - Restauración del catálogo mediante un backup.
  - Restauración del catálogo sin un backup.
  - Recuperación de archivos respaldados sin un catálogo.

Resultados de la Velocidad de Backup

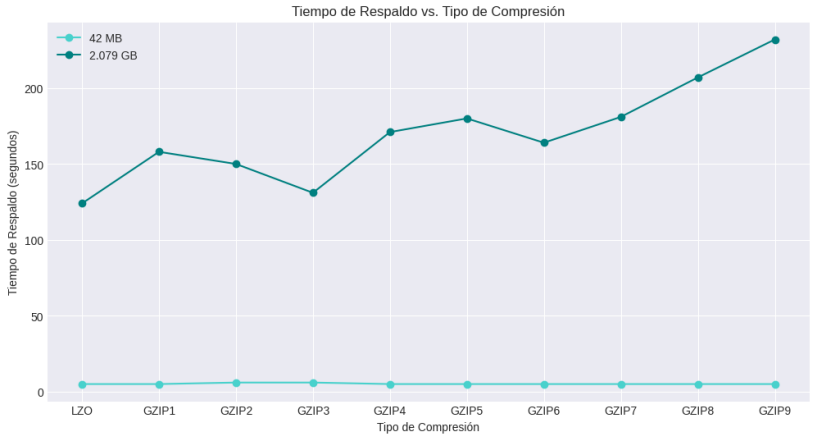
Velocidad de Backup en Diferentes Tamaños de Archivos

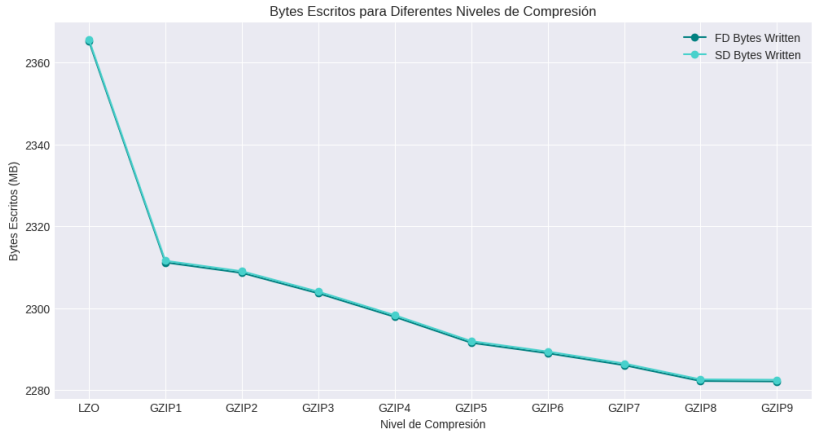


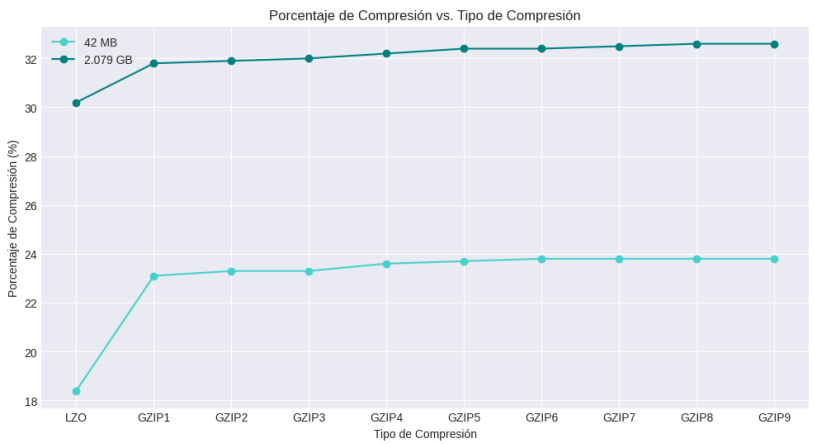
Velocidad de Backup de 1 GB en Diferentes Tamaños de Archivos de Fracción

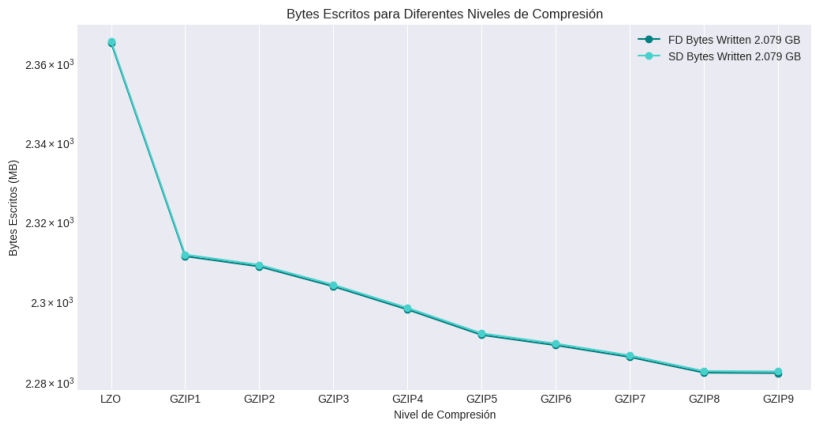


Resultados del test compresión



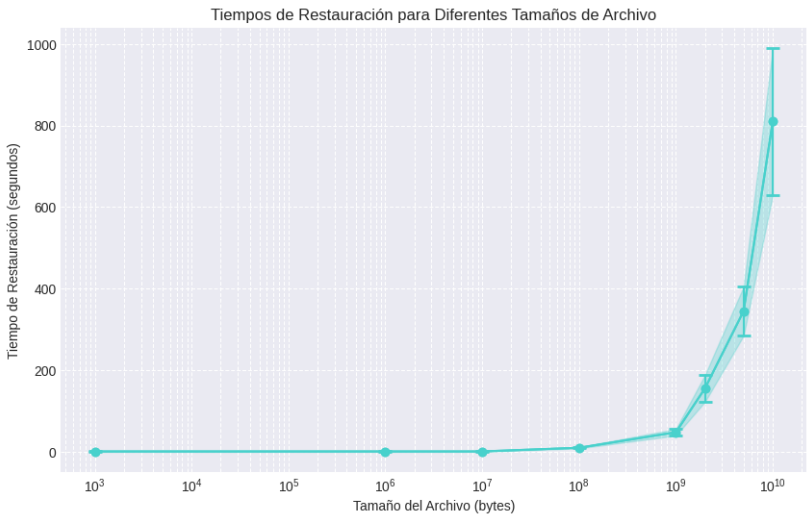




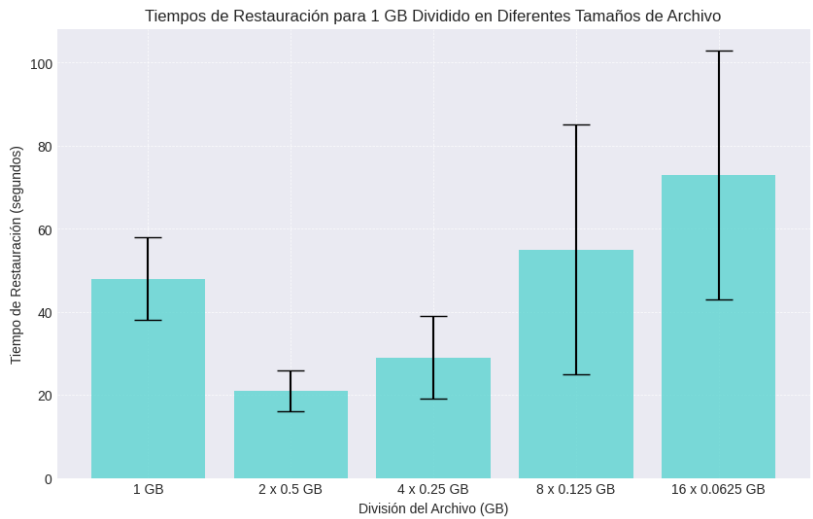


Resultados de la Velocidad de Restore

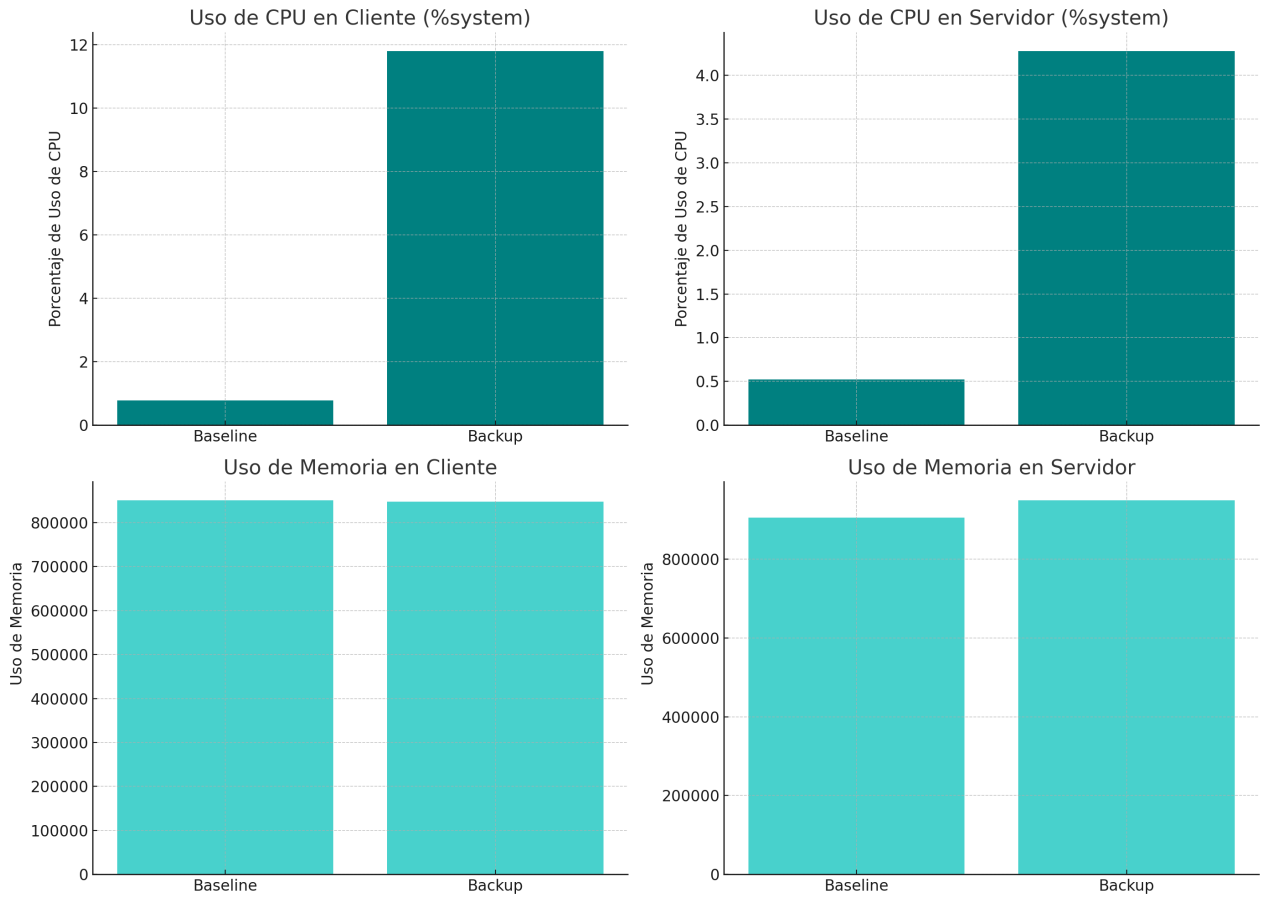
Velocidad de Restore en Diferentes Tamaños de Archivos



Velocidad de Restore de 1 GB en Diferentes Tamaños de Archivos de Fracción



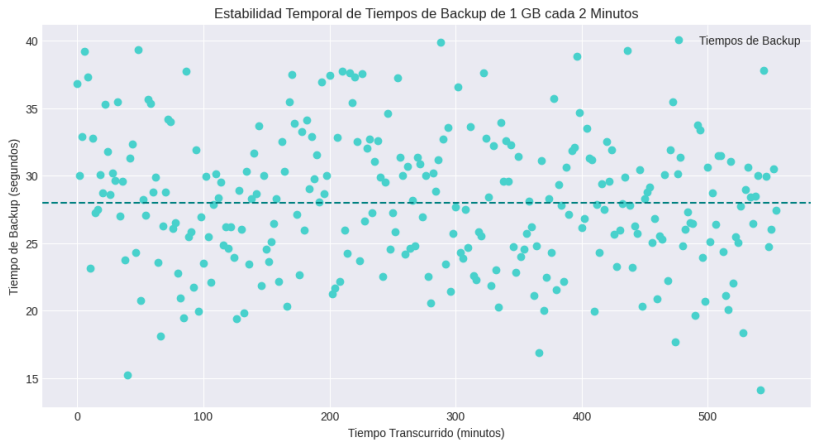
Uso de Recursos durante el Job



Número de Jobs y estabilidad temporal

Efecto del Número de Jobs en el Tiempo de Backup de 1 GB

Estabilidad Temporal de Tiempos de Backup de 1 GB cada 2 Minutos



Implementación de Estrategias GFS y 3-2-1

- **Estrategia GFS (Grandfather-Father-Son):**
  - **Backups diarios (incrementales):** Se retienen aproximadamente 1 semana.
  - **Backups semanales (diferenciales):** Se retienen aproximadamente 1 mes.
  - **Backups mensuales (completos):** Se retienen aproximadamente 5 años.

- **Estrategia 3-2-1:**
  - **Tres copias de datos:** Copia 1: Servidor local. Copia 2: Cinta. Copia 3: Nube.
  - **Datos mensuales:** 2GB.
  - **Datos anuales:** 2GB * 12 meses = 24GB.
  - **Datos en 5 años:**120GB (con un 20 % de margen = 150GB).

Costes de Implementación de la Estrategia 3-2-1

- **Servidor Local:**
  - **Hardware:** Fujitsu Server Intel Xeon 8GB/2TB.
    - Costo inicial del servidor: €986,58.
    - Costo anual de electricidad: €91,25.
- **Unidad de Cinta:**
  - **Hardware:** Unidad de cinta LTO.
    - Costo inicial de la unidad LTO $\approx$ €2000.
    - Costo de cintas LTO (12TB): €50 cada una.
- **Almacenamiento en la Nube:**
  - **Proveedor:** AWS S3.
    - Costo mensual (150GB): €3,45.
    - Costo anual: €41,4.

Limitaciones.

- Bacula ofrece herramientas de protección de datos, pero no se evaluaron todas las amenazas ni las medidas de seguridad adicionales necesarias para una protección completa.
- El entorno de prueba fue limitado, con un volumen de datos pequeño (10GB), lo que puede no reflejar los desafíos de entornos de producción de big data.
- Los costos de implementar la estrategia 3-2-1 con cintas LTO se basaron en estimaciones aproximadas y pueden variar según los proveedores y las necesidades de cada empresa.
- Bacula tiene limitaciones en entornos con alta concurrencia de trabajos. Efecto convoy o inanición de trabajos de baja prioridad.

Conclusiones

Capacidades y Configuraciones de Bacula.

- Bacula permite backups incrementales, diferenciales y completos.
- Soporte para estrategias GFS y 3-2-1.
- Flexibilidad en compresión, retención y replicación de datos.

Implementación y Pruebas

- Entorno de prueba con varios servidores locales.
- Eficiencia en procesos de backup y restauración.
- Adaptabilidad a diferentes necesidades y escenarios.

Guía de Mejores Prácticas.

- Bacula permite backups incrementales, diferenciales y completos.
- Soporte para estrategias GFS y 3-2-1.
- Flexibilidad en compresión, retención y replicación de datos.

Evaluación de Viabilidad y Eficiencia.

- Solución viable y eficiente contra ransomware.
- Costos justificados por seguridad.

¡Gracias!

Accede al repositorio de GitHub:

https://github.com/Fernando-Ares-Robledo/tfm