Instituto Superior Tecnológico "Los Andes" ISTLA

CÓDIGO CIENTÍFICO REVISTA DE INVESTIGACIÓN

Vol. 4 – Núm. 1/Enero – Junio – 2023

Sistemas inmutables de backup ante ataques de ransomware hacia una infraestructura TI

Immutable backup systems against ransomware attacks towards an IT infrastructure

Sistemas de backup imutáveis contra ataques de ransomware a uma infraestrutura de TI

José Reinaldo Cedeño Zambrano[1]
Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López"
jrcedeno@espam.edu.ec

César Armando Moreira Zambrano[2]
Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López"
cmoreira@espam.edu.ec

Como citar:
Cedeño, J. & Moreira, C. (2023). Sistemas inmutables de backup ante ataques de ransomware hacia una infraestructura TI. Código Científico Revista de Investigación, 4(1), 600-612.

Recibido: *12/03/2023* ***Aceptado:*** *14/04/2023* ***Publicado:*** *30/06/2023*

[1] Ingeniero en informática de la Escuela Superior Politécnica Agropecuaria de Manabí
[2] PhD. Docente de la universidad Técnica de Manabí y Escuela Superior Politécnica Agropecuaria de Manabí ESPAM MFL.

Resumen

En la actualidad, los ataques cibernéticos son una de las principales preocupaciones de las empresas y más aún amenazas de ransomware de todo tipo, instituciones gubernamentales, compañías financieras, proveedores de salud y otros han sido sujeto a este tipo de ciberdelito, por lo tanto, el objetivo de esta investigación es realizar un estudio e implementación de un sistema de respaldo inmutable mediante software libre como segunda línea de defensa frente a un ataque de informáticos, que pueda comprometer la infraestructura tecnológica. La metodología utilizada fue de tipo cuantitativa y el método de ejecución fue ciclo en V, el mismo que integra las fases de: especificación, diseño de alto nivel y de detalle, implementación y fase del test unitario, de integración y operacional. Como resultado se realizó una copia de seguridad inmutable de los datos, que es una estrategia y línea de defensa ante ransomware, garantizando que la copia de seguridad inmutable se mantiene a salvo de los desastres o de ataques cibernéticos. Como conclusión se debe tener al menos tres copias de los datos inmutadas significa que debería tener al menos dos Backup adicionales además de los datos en producción, permitiendo que, si algo sucede con un Backup, existirá otro al cual poder recurrir.

Palabras Clave: Sistemas inmutables, Ransomware, Veeam Backup, Infraestructura TI.

Abstract

Currently, cyber attacks are one of the main concerns of companies and even more ransomware threats of all kinds, government institutions, financial companies, health providers and others have been subject to this type of cybercrime, therefore, The objective of this research is to carry out a study and implementation of an immutable backup system using free software as a second line of defense against a computer attack that could compromise the technological infrastructure. The methodology used was quantitative and the execution method was a V cycle, the same one that integrates the phases of: specification, high-level and detailed design, implementation and phase of the unit, integration and operational test. As a result, an immutable backup of the data was made, which is a strategy and line of defense against ransomware, ensuring that the immutable backup is kept safe from disasters or cyber attacks. In conclusion, having at least three copies of the data immutable means that you should have at least two additional Backups in addition to the data in production, allowing that, if something happens with a Backup, there will be another one to which you can resort.

Key Words: Immutable systems, Ransomware, Veeam Backup, IT Infrastructure.

Resumo

Atualmente, os ataques cibernéticos são uma das principais preocupações das empresas e ainda mais ameaças de ransomware de todos os tipos, instituições governamentais, empresas financeiras, provedores de saúde e outros têm sido alvo desse tipo de crime cibernético, portanto, O objetivo desta pesquisa é realizar realiza um estudo e implementação de um sistema de backup imutável utilizando software livre como segunda linha de defesa contra um ataque informático que possa comprometer a infraestrutura tecnológica. A metodologia utilizada foi quantitativa e o método de

execução foi um ciclo V, o mesmo que integra as fases de: especificação, projeto de alto nível e detalhamento, implementação e fase da unidade, integração e teste operacional. Como resultado, foi feito um backup imutável dos dados, que é uma estratégia e linha de defesa contra ransomware, garantindo que o backup imutável seja mantido a salvo de desastres ou ataques cibernéticos. Em conclusão, ter pelo menos três cópias dos dados imutáveis significa que você deve ter pelo menos dois Backups adicionais além dos dados em produção, permitindo que, se algo acontecer com um Backup, haja outro ao qual você pode recorrer.

Palavras-chave: Sistemas imutáveis, Ransomware, Veeam Backup, Infraestrutura de TI.

Introducción

Hoy en día, todas las organizaciones se encuentran tecnológicamente dominadas por sistemas informáticos, que logran el control de sus operaciones en esta era digital, algún incidente dentro de su infraestructura tecnológica puede provocar pérdidas irreparables poniendo en riesgo la continuidad del negocio.

Según un estudio de Dobran (2019), indica que aproximadamente menos del 50% de las organizaciones no cuentan con un plan de recuperación ante desastres, de la misma forma cuenta con un ineficiente sistema de copia de seguridad, afectando a la disponibilidad de servicios, de la misma forma argumenta Rock (2020), afirmando que las entidades no tienen un método de restauración de datos ante un ataque de ransomware o incidente de seguridad en la infraestructura por parte de ciberdelincuentes.

Sanchez (2021), argumenta que, la información es uno de los principales y más sensibles recursos de cualquier organización, puesto que la toma de decisiones estratégicas depende del dato. y, sin embargo, no siempre se le presta la atención para cumplir con la salvaguarda de este. Y es que ya sea por un accidente fortuito (incendio, inundación, subida de tensión) o bien por acción una acción malintencionada (Malware, Ransomware), ya que existen amenazas a las que cualquier organización se ve expuesta. Últimamente se ha incrementado exponencialmente el secuestro de la información por parte de ciertos ciberdelincuentes, quienes cifran la información de la empresa

utilizando un software malicioso para después solicitar un importe, normalmente en Bitcoins a cambio de la clave que permita desbloqueo de los datos.

Arcserve (2021) detalla que, las organizaciones de TI siguen teniendo dificultades para afrontar la abrumadora tarea de hacer backup de cantidades cada vez mayores de datos en ventanas de backup cada vez más cortas. Lamentablemente, los administradores de TI están respondiendo a pedidos de restauración de datos de emergencia y tratando de mantener la infraestructura de backup para poder seguir satisfaciendo las exigencias. Las organizaciones están evaluando soluciones de almacenamiento inmutable de copias de seguridad basado en discos. Sin embargo, muchas de las soluciones actuales se basan en una arquitectura de escalamiento vertical con escalabilidad y rendimiento limitados. Si se alcanzan los límites de escalabilidad, las únicas opciones posibles son agregar otro conjunto independiente administrado por separado o proceder a la ardua tarea de realizar una actualización a gran escala y reemplazar el conjunto actual.

Zavala (2022), define a la inmutabilidad como, la aplicación de mecanismos de protección dentro de la arquitectura y diseño de los elementos que componen la plataforma de backup para que sea inaccesible por los ciberdelincuentes y además nos garantice tener tiempos de recuperación (RTO/RPO) óptimos que nos permita reducir el impacto de indisponibilidad de nuestros servicios

De la misma forma, Veritas (2023), aporta que, esto genera muchas islas de datos de backup complejas de administrar y aumenta mucho el costo de propiedad. Por lo general, estas soluciones de almacenamiento no son inmutables, con lo cual resultan vulnerables a ataques de ransomware.

Sin embargo, los planes de recuperación con lo que cuentan las instituciones son solamente replicaciones de los servicios en una ubicación alterna, pero no tienen las capacidades para restauración de los datos afectados por un ciberataque de ransomware ni mucho menos para la mitigación de este tipo de incidentes (Rubrik, 2021).

Por tal razón, es imprescindible la implementación de un plan de contingencia que logre la sistematización y automatización de una copia de seguridad inmutable, garantizando la rápida recuperación de datos comprometidos ante un ataque que pongan en peligro la seguridad de la información de la empresa.

Desarrollo

Fase de Especificaciones

En esta fase se describen las especificaciones necesarias de la solución a implementar, tomando como iniciativa de partida las características físicas con la que debe contar la infraestructura TI de la organización. Adicionalmente en esta etapa se realizó la investigación y comparación de software con las características de tener una solución de sistemas de respaldos inmutables, tal como se observa en la Tabla 1, siendo así Veeam el escogido para dicho despliegue de la solución, el cual se detalla a continuación en la Tabla 2 los requisitos y características técnicas del software mencionado.

Tabla 1.
Tabla comparativa de funciones.

	Soporte de hipervisores (vmware, Hyper-V y AHV)	Backup en disco, cinta y cloud	Compresión y deduplicación	Replicación integrada	Replicación continua
Veritas Netbackup	Si	Si	Si	Si, pero necesita un Media Server en Cloud	Si, pero necesita un Media Server en Cloud
Commvault	Si	Si	Si	No, es necesario licenciar otro producto	No, usa otro sofware licenciado aparte
Veeam Backup	Si	Si	Si	Si	Si
BareOS	Parcial, solo vmware	Si, limitado a S3 de AWS	Si	No, solo tiene backup a cloud	No

Después de haber analizado la tabla, se concluye que Veeam Backup es la solución más viable para la implementación del servicio de backup y recuperación ante desastres. Dicho motivo fue justificado debido a la capacidad de continuidad del negocio mediante la replicación que brinda la misma herramienta, proporcionando la facilidad de ahorro en licenciamiento, tal como lo afirma Glemot (2020), que permite la replicación continua, lo cual reducirá a menor cantidad de segundos el objetivo de punto de recuperación (RPO).

Tabla 2.
Requisitos mínimos de backup server

Especificaciones	Requisitos
Hardware	CPU: procesador x86-64 (se recomienda un mínimo de 4 cores). Memoria: 4 GB de RAM más 500 MB por trabajo simultáneo. Espacio en disco: 10 GB para la instalación del producto. Red: 1 Gbps como mínimo, recomendable 10GB. 1 Mbps como mínimo para replicación fuera del sitio.
Sistema Operativo	Solo se admiten versiones de 64 bits de los siguientes SO: Microsoft Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 Microsoft Windows 10 (versión 1803 a versión 20H2) Microsoft Windows 8.1, 7 SP1
Base de datos	Instalación local o remota de las siguientes versiones: Microsoft SQL Server 2019, 2017, 2016, 2014, 2012, 2008 R2, 2008.

Para soluciones grandes o de mediana escala es recomendable la separación entre la base de datos y el servidor de backup, de la misma manera, evitar el uso de versiones portables o express, debido a la limitación en cuanto al uso de recursos como memoria y CPU.

Fase de Diseño de Alto Nivel y de Detalle

En esta fase se diseñó la arquitectura y despliegue de la misma, El diagrama muestra el mecanismo de comunicación entre el sistema de infraestructura como servicio IaaS, y la sincronización con el sistema de Backup automatizado mediante Veeam Backup, el mismo que

debe ser filtrado En primera instancia por el firewall el cual tiene habilitado los puertos 6162 y 2500 3300, para pasar hacia el sistema. De almacenamiento repositorio donde se va almacenar la copia inmutada, cabe indicar que se recibe en un sistema Operativo Linux centos 8, tal como se observa en la Figura 1.

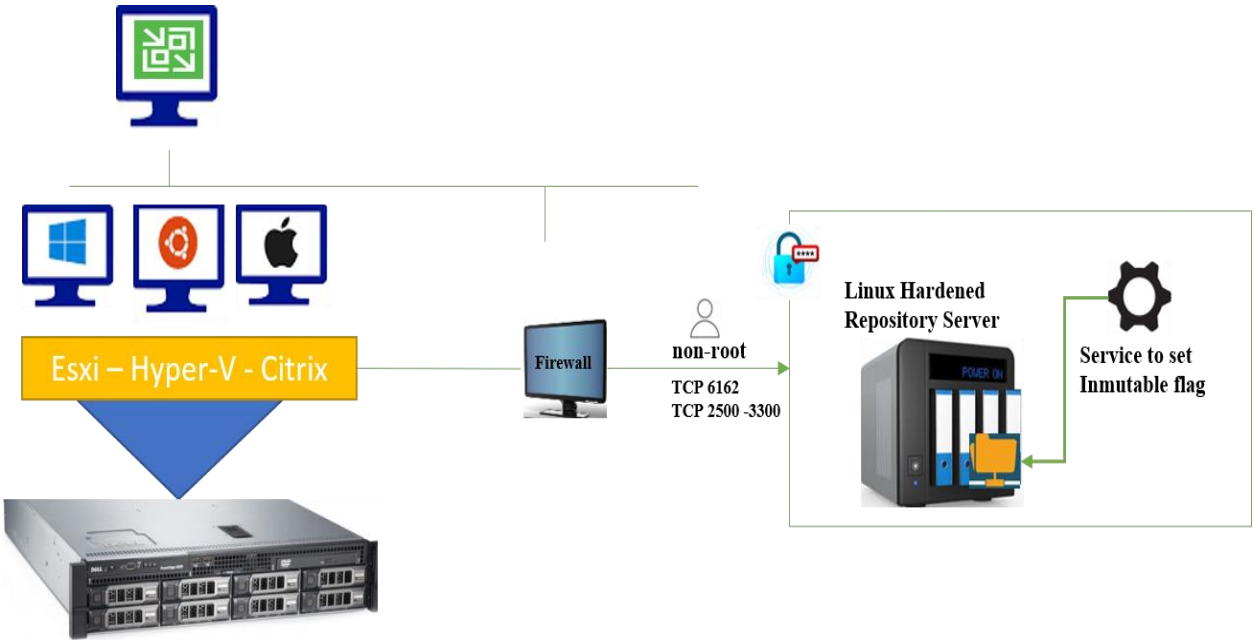

Figura 1. Diagrama de servidor de backup

Tabla 3.
Herramientas y sistemas operativos utilizados.

Herramientas	**Dirección IP**	**Mascara de red**	**Gateway**
Servidor Blade C3000	172.30.4.50	255.255.255.240	172.30.4.54
Host 1	172.30.4.51	255.255.255.240	172.30.4.54
Host 2	172.30.4.52	255.255.255.240	172.30.4.54
Host 3	172.30.4.53	255.255.255.240	172.30.4.54
Firewall	172.30.4.54	255.255.255.240	N/A
SAN HP P2000	172.30.4.55	255.255.255.240	172.30.4.54
Swicht Cisco SG 550X	172.30.4.56	255.255.255.240	172.30.4.54
Windows 2016 Server	172.30.4.57	255.255.255.240	172.30.4.54
Linux CentOS 8	172.30.4.58	255.255.255.240	172.30.4.54

Fase de Implementación.

Partiendo de la fase anterior y con el objetivo de la pronta recuperación ante desastres teniendo en cuenta la infraestructura TI adecuada, se procedió a la instalación y configuración del sistema de respaldo inmutable, la cual se detalla en la Tabla 3 la cual define las herramientas y sistemas operativos utilizados.

Se procedió con la virtualización del almacenamiento disponible dentro del sistema operativo CentOS 8, luego de eso, se realizó la conexión vía SSH a dicho servidor y para el caso de estudio de utilizó la herramienta veeamhubrep, la cual nos permite la gestión y configuración del repositorio inmutable.

Fase del Test Unitario, de Integración y Operacional

Para realizar los respaldos de cada una de las instancias virtualizadas y de los volúmenes lógicos de almacenamiento se utilizó Veeam Backup, permite hacer que los puntos de recuperación en estos repositorios sean inmutables. Con la aplicabilidad de inmutabilidad, los puntos de recuperación se almacenan mediante el modelo de escritura única, lectura múltiple (WORM). La inmutabilidad agrega otra capa de seguridad a las copias de seguridad al proteger los puntos de recuperación del cifrado por ransomware o eliminaciones y modificaciones accidentales, el mismo que permite minimizar los fallos, esta herramienta cumple con las características apropiadas para realizar los respaldo y restauración en periodos de tiempos cortos, por la tecnología que integra, manteniendo la seguridad en todo momento.

Tabla 4.
Script de backups inmutable

```
#!/bin/bash
listadiscos=$(lsblk)
scandisks=$(rescan-scsi-bus.sh)

echo "Scanning Disks....: $scandisks"

echo "List Disks : $listadiscos"

echo "****** Enter disk as example /dev/sdb ******: "
read
pvcreate $REPLY
vgcreate repoimm $REPLY
lvcreate -l 100%FREE --name repoveeam repoimm
mkfs.xfs -b size=4096 -m reflink=1,crc=1 /dev/repoimm/repoveeam
mkdir /repoveeam
mount /dev/repoimm/repoveeam /repoveeam
adduser repouser
echo "****** Please Enter repouser Password ******"
passwd repouser
mkdir /repoveeam/backups
chown repouser:repouser /repoveeam/backups
chmod 700 /repoveeam/backups
UUID=$(blkid | grep repoimm-repoveeam |cut -f2 -d'='|cut -f2 -d'"')
echo "******Saving /etc/fstab as /etc/fstab.$$******"
/bin/cp -p /etc/fstab /etc/fstab.$$
echo "******Adding / repoveeam to /etc/fstab entry******"
echo "UUID=${UUID} / repoveeam xfs defaults 1 1" >> /etc/fstab
echo "******Please Add The New Repository with repouser single-use credentiales in Veeam Backup & Replication******"
while [ 1 ]
do
      pid=`ps -fea | grep "veeammimmureposvc" | grep -v grep`
      echo $pid
      if [ "$pid" = "" ]
      then
            echo "******veeam Process is not here...******"
            #exit
      else
            echo "******veeam Process Detected continuing...******"
            echo "******Denying SSH /etc/ssh/sshd_config entry******"
            echo "DenyUsers repouser" >> /etc/ssh/sshd_config
            echo "******Disable SSH? Enter 1 for YES or 2 for NO******"
            select yn in "Yes" "No"; do
            case $yn in
            Yes ) $(systemctl disable sshd && systemctl stop sshd); echo "SSH Service Disabled and Stopped, Please disconnect from SSH"; exit;;
            No ) exit;;
            esac
            done
            fi
      sleep 8
done
```

Metodología

El presente trabajo de investigación tiene como finalidad la rápida recuperación de desastre ante un ataque de ciberdelincuentes, de la misma forma que mejora significativamente la sincronización y backup inmutable en la organización, dentro del mismo se aplicó la metodología cualitativa, la ejecución se la realizó mediante el método ciclo en V, el mismo que integra las fases necesarias para este tipo de desarrollo, las cuales están detalladas como fase de especificación, fase de diseño de alto nivel y de detalle, fase de implementación y fase del test unitario, de integración y operacional. Los sistemas de respaldos inmutables y su aplicabilidad en las organizaciones son una tecnología innovadora que ofrece estabilidad en las aplicaciones críticas, implementando sistemas de almacenamiento robustos que pueden alcanzar niveles de tolerancia a fallos muy reducidos, garantizando seguridad y escalabilidad a través de mecanismos de redundancias e inmutabilidad.

Garcés y Egas (2021), aportan que, el modelo en V permite hacer más explícita la tarea de la iteración de las actividades del proceso. Las pruebas que se implementarían en cada fase ayudarían a corregir posibles errores sin tener que esperar a que sean rectificados en la etapa final del proceso. Esto, sumado las pruebas unitarias y de integración se consigue obtener exactitud en los programas.

Resultados

Tras analizar los escenarios desplegados como una descripción de las soluciones más relevantes en cuanto a copias de seguridad, debemos, y evaluar la solución propuesta y funcional, para lo cual se desplego la solución y conexión entre veeam Backup y Vmware toso esto a nivel de instancias virtuales, adicional se generó el recurso de almacenamiento dentro de SAN, el mismo

que va contener los Backup generados a inmutados desde veeam, como son las máquinas virtuales en producción dentro del sistemas IaaS.

Realizar una copia de seguridad inmutable de los datos es una estrategia y línea de defensa ante ransomware, garantizando que la copia de seguridad inmutable se mantiene a salvo de los desastres o los ataques, el mismo que no puede ser modificada, borrada o cambiada de ninguna manera, ni el super usuario administrador del sistema Linux logrando recuperar rápidamente siempre que sea necesario.

El sistema de Backup de veeam es compatible con sistemas VMware y su hipervisor Esxi permitiendo ajustarse fácilmente a sistemas de infraestructura como servicio IaaS permitiendo la integración y automatización inmutable respaldando las máquinas virtuales en su total despliegue.

En la tabla 5 se observa el consumo energético y costos promedio de un servidor, por lo tanto, con la implementación de la solución planteada este indicador se optimiza, ya que la media de consumo en los servidores virtualizados no varía tanto, es decir en valores porcentuales aproximadamente en un 5% adicional al consumo eléctrico.

Tabla 5.
Consumo promedio energético y costos

Modalidad	**Costo por equipo**		**Consumo energía (watts)**	**Consumo mensual (Kwh)**	**Consumo mensual ($)**	**Consumo anual ($)**
Tradicional	$10.000,00	1	398	286,56	$25,50	$306,04
Virtualizado	$10.000,00	4	568	408,96	$36,39	$436,77

Los resultados mostrados son notables y se comprueba que la implementación de IaaS mejoró los parámetros planteados a resolver mediante el Backup inmutable automatizado, dando una solución eficiente, escalable y que contribuye en el desarrollo tecnológico y prevención de amenazas de la infraestructura tecnológica.

Backup job: UOC-Backup (Full)

Created by RX1/Administrador at 11/04/2023 20:01

martes 11 de abril de 2023 20:01:23

success	1	**start time**	20:01:23	**total size**	16GB	**Backup size**	2GB	
Warning	0	**end time**	20:06:07	**data read**	16GB	**dedupe**	5,4x	
Error	0	**duration**	0:04:44	**transferred**	2GB	**Compression**	1,5x	

Details

name	status	start time	end time	size	read	transferred	duration	details
ww2-01	success	20:01:44	20:06:00	**16GB**	16GB	**2GB**	0:04:15	

En esta prueba se realiza la validación, y que la parte fundamental del servicio de respaldo o backup funciona correctamente por lo cual se verifica que la programación y automatización de dicha copia esté operativa desde la máquina virtual al repositorio de almacenamiento local.

Conclusiones

Un sistema Backup con inmutabilidad garantiza que las copias de seguridad de las instancias virtuales y servidores físicos no se vean afectadas o encriptadas por el ransomware. Todo esto gracias a el estándar WORM Write-Once-Read-Many. los datos se escriben una sola vez y, una vez hecho, no pueden alterarse. Es decir, no pueden ser reescritos ni borrados, aunque podrás acceder a ellos cuantas veces sean necesarias.

Tener un sistema automatizado de Backup que permita la convergencia entre tecnologías garantiza que se puedan tener copias de los datos inmutadas en centros de datos alternos esto significa que debería tener al menos dos Backup adicionales, si algo llegara a suceder con un Backup, existirá otro al cual poder recurrir

Implementar una infraestructura inmutable es una manera de gestión y administración simplificada en cuanto a actualizaciones de copias de seguridad, es decir que los servicios poseen una rápida capacidad de recuperación ante desastres e inmutabilidad ante la corrupción de sus datos.

Referencias bibliográficas

Arcserve. 2021. Almacenamiento inmutable para backup y archivo de onexafe. En línea. Disponible en: https://www.arcserve.com/sites/default/files/wp-doc/Arcserve-storagecraft-onexafe-Backup-Solution-Brief-LA-L6F.pdf

Bojana Dobran. Disaster Recovery Statistics That Will Shock Business Owners. En Linea. Disponible en: https://phoenixnap.com/blog/disaster-recovery-statistics/,

Garcés, l y egas, l.2021. Evolución de las metodologías de desarrollo de la ingeniería de software en el proceso la ingeniería de sistemas software. Revista Científica Y Tecnológica. UPSE. Vol1 N°3.

Glemot C. 2020. In Backup, Continuous Data Protection, Veeam, Veeam B, and R 11. Veeam B&R 11 - Continuous Data Protection. Https://original-network.com/veeam-br-11-continuous-data-protection/

Rubrik. 2021. Recovering Fast from Ransomware Attacks:The Magic of an Immutable Backup Architecture. En línea. Disponible en: https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/magic-immutable-backup-architecture-white-paper.pdf

Sanchez, D. 2021. Implantación sistema baas. En Linea. Disponible en: https://openaccess.uoc.edu/bitstream/10609/132628/6/dasanortfg0621memoria.pdf

Tracy Rock. 23 disaster recovery statistics you should know. En Linea. Disponible en: https://invenioit.com/continuity/disaster-recovery-statistics/, July 2020.

Veritas.2023. Immutable Backups and How They Mitigate Ransomware Attacks. En Linea. Disponible en: https://www.veritas.com/information-center/immutable-backups

Zavala. C.2022. Asegura RTO y RPO de tu negocio con soluciones de Backup realmente inmutable. En línea. Disponible en: https://www.open3s.com/asegura-rto-y-rpo-de-tu-negocio-con-soluciones-de-backup-realmente-inmutable-blog/