Universitat Oberta de Catalunya

uoc.edu

Implantación sistema BaaS

DAVID SANCHEZ ORTIZ

Grado de Tecnologías de Telecomunicación

Área del TFG:

Administración de redes y sistemas operativos

Profesor responsable de la asignatura:

JORDI SERRA RUIZ

MARIO PRIETO VEGA

6 de junio de 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	Implantación sistema BaaS
Nombre del autor:	David Sanchez Ortiz
Nombre del consultor:	Mario Prieto Vega
Nombre del PRA:	Jordi Serra Ruiz
Fecha de entrega (mm/aaaa):	06/2021
Titulación:	*Grado de Tecnologías de Telecomunicación*
Área del Trabajo Final:	Administración de redes y sistemas operativos
Idioma del trabajo:	Español
Palabras clave:	Backup, RTO, BaaS DRaaS

Exposición inicial del trabajo

Muchas empresas, ignoran la importancia de los datos que se generan diariamente, esto es debido a que no han tenido un problema serio con ellos. No obstante, no significa que no puedan sufrir cualquier eventualidad que provoque en definitiva la perdida de datos.

En definitiva, la perdida de la información puede comprometer no solo la continuidad de un servicio, sino la propia continuidad del negocio. La pregunta que debe realizarse cualquier organización es: ¿cuánto valor tiene para mi negocio los datos que tengo? (Contabilidad, facturación RRHH ,etc..)

En consecuencia, la proliferación de amenazas del tipo ransomware durante los últimos años ha provocado que los backups formen parte del kit esencial de seguridad de cualquier empresa, siendo la regla 3-2-1 del Backup, una de las más utilizadas al permitir abordar de forma efectiva cualquier escenario de fallo consistiendo en almacenar tres copias de los datos, en dos soportes distintos y una copia del Backup offsite

Este Trabajo Final de grado abordará, las soluciones tecnológicas actuales reales, que permitan garantizar la continuidad del servicio y del negocio, proporcionando un sistema de salvaguarda y recuperación de datos, que cumpliendo la regla 3-2-1, robusto y eficaz, con un reducido RTO, haciendo uso de la tecnología BaaS o DRaaS

Para ello se analizarán todas las tecnologías que intervienen en el proceso de Backup y se seleccionaran las diferentes herramientas para realizar una implantación a partir de un marco practico, pre establecido consistente en:

- 3 sedes interconectadas a través de tunelización ipsec vpn entre sedes
- Cada sede tiene un nas como repositorio Backup.
- Cumpliendo de esta manera la regla 3-2-1

Con la intención de estructurar toda la información se hará uso de la guía de proyecto PMBOK, que está se superponen e interactúan a lo largo de la realización de las fases del proyecto. Sin olvidar una parte práctica al consistir uno de los objetivos en realizar una implantación de una solución Backup utilizando diferentes puntos de vista.

Abstract

Many companies ignore the importance of the data that is generated daily, this is because they have not had a serious problem with them. However, this does not mean that they cannot suffer any eventuality that ultimately leads to data loss.

In short, the loss of information can compromise not only the continuity of a service, but the continuity of the business itself. The question that any organization should ask itself is: how much value does the data I have have have for my business? (Accounting, HR invoicing, etc.).

Consequently, the proliferation of ransomware type threats in recent years has made backups part of the essential security kit of any company, being the 3-2-1 Backup rule one of the most used, as it allows to effectively address any failure scenario consisting of storing three copies of the data, in two different media and a copy of the offsite backup.

This Final Project will address the real current technological solutions that allow to guarantee the continuity of the service and of the business, providing a data backup and recovery system that complies with the 3-2-1 rule, robust and efficient, with a reduced RTO, making use of BaaS or DRaaS technology.

For this purpose, all the technologies involved in the backup process will be analyzed and the different tools will be selected for implementation based on a practical, pre-established framework consisting of:

- 3 site places interconnected through ipsec vpn tunneling between sites.
- Each site has a nas as Backup repository.
- Thus complying with the 3-2-1 backup.

With the intention of structuring all the information we will make use of the PMBOK project guide, which is overlapping and interacting along the realization of the project phases. Without forgetting a practical part as one of the objectives is to implement a Backup solution using different points of view.

Índice

Lista de Figuras

1. Introducción

1.1. Contexto y justificación del Trabajo

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.

Ante estas circunstancias, no cabe otra cosa que realizarse ciertas preguntas como son: ¿La organización es consciente del riego que supone la pérdida de las factura emitidas o recibidas?, ¿Es consciente de lo que puede suponer la pérdida de la justificación de cobros y pagos? Puesto que las consecuencias ante un desastre como es la perdida de datos no solo es de reputación de empresa no fiable de cara a los clientes, sino que además se puede producir una parálisis de la actividad, puesto que para la toma de decisiones la información debe ser integra, confidencial y estar siempre disponible.

Por este motivo se hace necesario, no solo tener un respaldo continuo, sino que además debemos contemplar el tiempo de recuperación de los sistemas y este no debe ser excesivo. Y he aquí que nos tengamos que preguntar ¿En cuánto tiempo puedo recuperar los sistemas en caso de desastre?, ¿Cuánto tiempo puede estar la empresa inactiva por no tener los datos disponibles? Y a partir de ahí determinar el alcance que puede tener este problema.

En este punto, debemos tener claro que las copias de seguridad adquieren una importancia supina, ya que en caso de catástrofe se cuenta con un respaldo de la información otorgándonos la capacidad de una oportuna recuperación llegado el caso, evitando de esta manera las grandes pérdidas económicas que supondrían la perdida de la totalidad de los datos.

No obstante, con solo una copia no es suficiente para garantizar el respaldo de toda organización, al existir eventos que pueden malograr esta copia, desde un incendio a un robo y en definitiva cualquier incidencia que se diera en el soporte de almacenamiento donde se encuentre dicha copia.

Ante esta problemática, se desarrolló la estrategia de almacenamiento Backup 3-2-1, básicamente esta norma, consiste en realizar 3 copias de seguridad de los datos, almacenar en al menos 2 medios diferentes y enviar 1 a un entorno offsite. Esta solución permite abordar de forma efectiva cualquier escenario de fallo. Ya que la posibilidad de que exista un fallo tal que afecte a la vez a tres entornos diferentes es prácticamente nula.

Dentro del Plan de recuperación de desastre y en lo que se refiere a la continuidad del servicio de la organización deberemos tener en cuenta el **Recovery Point Objective (RPO)** y **Recovery Time Objective (RTO)** para elegir un plan de respaldo de datos óptimo. Siendo RPO la cantidad de tiempo/datos que se pueden perder y seguir funcionando y el RTO se refiere al tiempo necesario para que todos los sistemas se reanuden con normalidad.

1.2. Objetivos del Proyecto

Los objetivos de este proyecto son los siguientes:

- Obtener una visión clara de la necesidad de tener un plan de recuperación ante desastres desde la perspectiva de las copias de seguridad.
- Cumplir norma Backup 3-2-1
- Conocer las diferentes estrategias de Backup
- Visualizar las diferentes ventajas/inconvenientes de los diferentes soportes/medios utilizados en Backup
- Asimilar el Cloud como parte de la estrategia de copias a nivel de repositorio
- Definir el RPO y RTO en base a las diferentes opciones de Backup elegidas.
- Aplicar las últimas innovaciones en sistemas de Backup.
- Aplicar todas las construcciones teóricas que se han ido adquiriendo en una solución práctica.

1.3. Método y enfoque realizado

Para poder iniciar el proyecto, debemos de crear unas premisas iniciales desde el punto de vista de la organización, a modo de punto de partida puesto si nos situamos a nivel organización, son varias las estrategias que se pueden seguir para alcanzar a implementar un entorno de copias de seguridad robusto.

Se puede delegar la implantación de este sistema a una empresa externa que a través de subcontratación del servicio y que esta se encargue de todas las tareas de copia, recuperación y gestión de backups. también se optar por un sistema hibrido en el que una empresa externa colabora con el personal cualificado de la organización encargándose de la implantación y formación del personal

Para este proyecto, ambas estrategias no tendrían cabida debido a que lo que se busca obtener es un amplio conocimiento para llevar a buen término la implantación de un sistema de Backup que respete la regla 3-2-1 y haga uso del Cloud.

Por lo que a nivel organización utilizaremos un enfoque en el cual será el personal cualificado quien se encargue buscar, implantar y realizar un protocolo de actuación en lo que a copias de seguridad de refiere.

La ventaja que nos dará esta elección es clara, al conocer todos los pormenores del proceso, seremos en un futuro capaces de delegar o no las partes más tediosas del mismo así como tener la capacidad de solucionar cualquier problema que nos encontremos al tener un conocimiento más profundo de las diversas herramientas utilizadas así como disminuir el coste directo al limitarlo a las licencias y el hardware necesario en contra partida, se aumentaran los gastos indirectos al dedicar personal interno al proyecto.

1.4. Planificación del proyecto

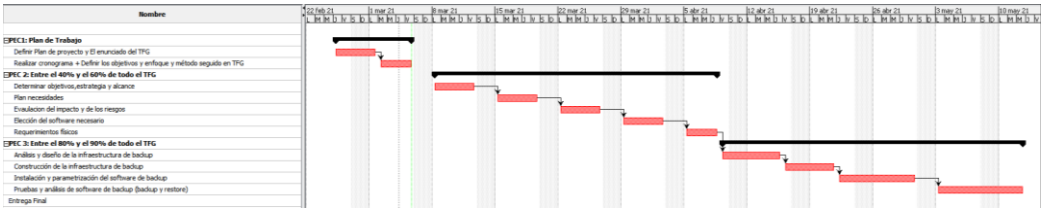

Figura 1.Diagrama de Grant

Actividad	Memoria	Inicio	Fin	días	Horas
Entrega PEC1:	**Plan de Trabajo**	**17/02/2021**	**06/03/2021**	**17**	**25,5**
Definir Plan de proyecto y El enunciado del TFG		25/02/2021	01/03/2021	4	6
Realizar cronograma + Definir los objetivos y enfoque y método seguido en TFG		02/03/2021	06/03/2021	4	6
Entrega PEC2:	**Entre el 40% y el 60% de todo el TFG**	**07/03/2021**	**08/04/2021**	**32**	**48**
Determinar objetivos, estrategia y alcance		07/03/2021	13/03/2021	6	9
Plan necesidades		14/03/2021	20/03/2021	6	9
Evaluación del impacto y de los riesgos		21/03/2021	27/03/2021	6	9
Elección del software necesario		03/04/2021	09/04/2021	6	9
Entrega PEC3:	**Entre el 80% y el 90% de todo el TFG**	**09/04/2021**	**12/05/2021**	**33**	**49,5**
Requerimientos físicos		09/04/2021	13/04/2021	4	6
Análisis, diseño y construcción de infraestructura de backup		12/04/2021	19/04/2021	7	10,5
Instalación y parametrización del software de backup		20/04/2021	30/04/2021	10	15
Pruebas y análisis de software de backup (backup y restore)		01/05/2021	12/05/2021	11	16,5
Entrega TFC y Presentación		**13/05/2021**	**06/06/2021**	**24**	**36**
Total, Proyecto:				92 días	138 Horas
Calificación final		**21/06/2021**	**21/06/2021**		

Figura 2.Tabla Explicativa diagrama de Grant

2. Desarrollo del proyecto

2.1. Estrategia, objetivos y alcance

Tradicionalmente, la copia de seguridad ha sido muy difícil de realizar correctamente. Los sistemas de respaldo no se ejecutan o los datos no se pueden restaurar y el problema que genera es la falsa sensación de seguridad, que es peor que no tener ningún sistema de seguridad. Y es que para algunas personas se aferran a la idea obsoleta de que la copia de seguridad es un asunto que se realiza una vez a la semana.

De ahí que la estrategia de respaldo sea tan importante, ya que nos marcara el objetivo y el alcance del sistema Backup, para definir una estrategia de protección de datos madura con sistemas de respaldo modernos, debemos tener en cuenta:

El "Backup Window" (Ventana de Backup) que consiste en el tiempo necesario para realizar la copia de seguridad, este tiempo va asociado normalmente a los soportes de almacenamiento, puesto que la velocidad de escritura de datos el soporte es determinante, por ejemplo, USB 2.0 tiene una velocidad de transferencia de 35 MBps, USB 3.0 tiene una velocidad de transferencia de 300 MBps, seleccionar uno u otro dispositivo puede aumentar o disminuir la ventana de Backup.

El Recovery Point Objective, RPO, siendo este simplemente la cantidad máxima de tiempo desde su última copia de seguridad, para hallar este dato debemos estimar cuanta información está dispuesta a perder la organización en caso de desastre, el objetivo es definir la periodicidad de las copias.

El Recovery Time Objective, RTO, nos indica el tiempo que se tarda en restaurar los datos más restablecer los sistemas como si el desastre no se hubiera producido. Este dato a nivel financiero es muy relevante, ya que cada minuto de inactividad en cualquier organización, tiene coste.

El último dato necesario para poder realizar la estrategia es la política de retención, de copias de seguridad, es decir establecer cuanto tiempo deseamos conservar las copias de seguridad, tenemos que tener en cuenta dos factores, que múltiples copias, nos permiten varios puntos de recuperación, no obstante, el espacio de almacenamiento, aunque hoy por hoy es muy amplio, también es limitado, con lo que no podemos guardar los datos para siempre.

En definitiva, debemos organizar el trabajo de tal manera en que el servicio de Backup, este lo más optimizado posible, Obviamente un proyecto de gestión de Backup, no va a depender de una sola persona, sino de un conjunto de responsables con lo que habrá que definir diferentes flujos de trabajo, donde cada una de las partes tenga clara su responsabilidad. Por supuesto, el escalado debe estar bien definido para poder reaccionar y adaptarse sin perder calidad ante el crecimiento de la organización.

Aunque el objetivo principal de la implantación de un sistema de respaldo es crear una copia de los datos que se puedan recuperar en caso de que se produzca una falla en los datos primarios devolviendo estos a un estado conocido consistente con una pérdida mínima de datos actualizados, existen también otros objetivos a alcanzar en este proyecto como puede ser el dimensionamiento de la solución asegurando el un rendimiento adecuado dentro de un coste moderado, para ello se debe realizar un estudio exhaustivo de las necesidades reales. Debiendo contemplar el crecimiento que pueda existir a corto, medio y largo plazo, sin olvidar cumplir la norma Backup 3-2-1 con la intención de tener el sistema más robusto posible y que tanto el RTO como el RPO no sean muy elevados y que la solución elegida, no tenga una ventana de Backup muy amplia.

En cuanto al alcance, será el cumplimiento de los objetivos anteriormente explicados cumpliendo la estrategia lanzada que en nuestro caso tendrá como resultado la implantación de un sistema Backup robusto y eficaz que haga uso del Cloud y el acta de constitución proyecto el asistente de dicho acuerdo, que marque en definitiva el alcance.

2.2. Análisis del impacto

Este proyecto nace de la necesidad de garantizar la continuidad del negocio. por eso debemos asegurarnos de que no se perturba la continuidad del negocio ni la del servicio, es decir que la herramienta Backup debe garantizar, que las apps y los datos de la organización, tiene una salvaguarda tal que permita la continuidad del servicio y por ende la mínima perturbación del negocio.
Para detectar aquellas aplicaciones y datos que son críticos para la continuidad de negocio, debemos realizar un análisis denominado Business Impact Analysis (BIA) este análisis consiste en un proceso sistemático para determinar y evaluar los efectos potenciales de una interrupción de las operaciones críticas como resultado de un desastre, accidente o emergencia.
Debemos tener en cuenta que este análisis, tiene como objetivo los efectos o consecuencias de la interrupción de las funciones críticas intentando cuantificar los costos financieros y no financieros asociados con un desastre, mientras la evaluación de riesgos identifica peligros potenciales.
Uno de los objeticos del BIA consiste en proveer una base para identificar los procesos críticos para la operativa de una organización, para ello, aunque no existe un estándar formal y la metodología puede variar según la organización, debemos
análisis de impacto empresarial

- Recolectar la información, realizar un proceso mediante reuniones y formularios internos que nos permitiría realizar un mapa conceptual de las codependencias entre proceso.
- Clasificar y Jerarquizar con los datos recopilados, debemos generar una tabla en las que introduciremos distintos RTO, MTD (Maximum Tolerable Downtime) y RPO. de esta manera establecemos las prioridades entre proceso para definir las consideraciones necesarias para proteger las partes más vulnerables de cada proceso.
- Despliegue de medidas, Una vez recopilada la información y clasificada, debemos validar con los distintos departamentos que la clasificación y jerarquización es correcta, así como evaluar los requisitos de recuperación de los sistemas involucrados.

En definitiva, este análisis nos permitirá determinar los sistemas y datos más cruciales, el personal y los recursos tecnológicos necesarios para que las operaciones funcionen de manera óptima y por último una ventana de tiempo dentro de la cual la funcionalidad debe recuperarse para minimizar el impacto de un desastre en la organización.

2.3. Análisis de riesgos

Durante el proceso de la gestión del proyecto, nos encontraremos mediante condiciones inciertas que pueden desembocar en un riego para la cumplimentación de los objetivos del proyecto sufriendo una desviación en el presupuesto aumentando costes o sufriendo una desviación en la planificación del proyecto implicando también aumento de costes o la perdida de la calidad o una reducción del alcance.
Es por esto por lo que nos preguntamos si es necesario realizar un Análisis de Riesgos, en sentido estricto, la respuesta es complicada puesto que siempre podrán aparecer riesgos debido a la condición de incertidumbre de todo proyecto, pero sí que debemos intentar identificar todos los riesgos que podamos prever de acuerdo a nuestra experiencia previa en la gestión de proyectos, teniendo en cuenta siempre el principio de Pareto aplicado a la gestión de proyectos, es decir que el 20% de los problemas consumen el 80% del tiempo.
A partir de la identificación de un riesgo debemos plantear una contramedida, que en definitiva logremos mantener los riesgos bajo control brindando tranquilidad y confianza en la gestión del proyecto, en este proyecto identificamos los siguientes riesgos y contramedidas

- **Riesgos derivados de la organización**, puede ocurrir que si los componentes del equipo de IT, son reticentes al cambio o no dedicamos el tiempo suficiente a analizar las diversas soluciones del mercado, el proyecto puede fracasar.
  Como contramedida, tendríamos que hacer partícipe a todo el equipo con reuniones periódicas de seguimiento de proyecto, involucrar en lo posible al equipo en la elección de la solución, la cual debe ser una elección más que meditada, de ahí que realicemos este trabajo.

- **Riesgos de acabar en un limbo**, si todos los componentes participan, pero ninguno toma decisiones la falta de llegar a un punto en común, genera incertidumbres sobre la información analizada.
  Como contramedida debemos asignar las responsabilidades dentro de este proyecto en función de la valía y es estrictamente necesario que las personas involucradas entiendan el alcance del mismo.

- **Riesgos provocados por problemas en la planificación**. Si la planificación no es metódica, si no tiene un seguimiento periódico mediante ToDo list, resulta inviable cumplir los hitos de las fases programadas, una planificación optimista, sin tener en cuenta la carga de trabajo que puede suponer una implantación de este tipo.
  Como contramedida debemos intentar visualizar la carga de trabajo, poner un enfoque pesimista y hacer reuniones de seguimiento semanales, diariamente actualizar hitos conseguidos.

- **Riesgos derivados de la solución**, existe una gran variedad de riesgos derivados del propio producto a implantar puesto que, al no conocerlo con exactitud, no es posible tener una idea real de la complejidad.
  Como contramedida, deberemos documentarnos lo mejor posible, a cerca de los puntos fuertes de las posibles soluciones, buscar opiniones en las comunidades de usuarios, información negativa del software, contactar si es posible con organizaciones similares a la nuestra que haya aplicado esa solución, para mejorar la percepción de la complejidad.
- **Riesgos derivados del presupuesto**, Los riesgos anteriores pueden derivar en una desviación presupuestaria de tal manera que el coste se puede incrementar, también el hecho de no valorar correctamente a nivel económico el proyecto puede llevar a la cancelación del mismo.

Una contramedida, puede ser analizar y definir correctamente cada una de actividades involucradas en el proceso, estimando tiempo y como inversión.

- **Riesgos de la pérdida de los apoyos de la gerencia de la organización**, debido a cualquier desviación sobre todo en lo que afecta a lo presupuestado, podemos perder el apoyo de gerencia, puesto que un proyecto de esta índole está compuesto de la tecnología, los procesos y las personas que muchas veces, no entienden la necesidad de cambio si hasta ahora ha cumplido.
  como contramedida debemos no subestimar los esfuerzos necesarios, para de esta manera adjudicar los recursos y el tiempo que sean necesarios a la hora de presentar el proyecto

- **Riesgos de Incompatibilidades**, la solución a implantar, debe convivir con un conjunto de hardware anterior con la intención de abaratar los costes de infraestructura, esto implica que aunque el software funcione en principio correctamente, sea incompatible, por ejemplo a nivel de drivers o de tecnología de tal manera que no reconozca por la cabina de discos o simplemente genere inestabilidad o problemas de rendimiento en el resto de sistemas.
  Como contramedida, trazar una matriz de compatibilidad para ello analizaremos bien el hardware con el que va a convivir la solución así como las métricas necesarias de carga, de tal manera que podamos reducir el impacto del cambio de tecnología.

- **Riesgos de desastres físicos**, Existen factores que no se van a poder controlar, como un incendio una inundación, una sobre tensión, etc.
  Como contramedida valorar el emplazamiento físico de los sistemas, por ejemplo, si tienen o no un SAI y de que tipo, existen medidas anti incendio, son para fuegos eléctricos de tipo co2.

- **Riesgos derivados debidos a los recursos humanos**, debemos contemplar el hecho que alguno de los miembros del equipo de implantación puede sufrir una baja ya sea por accidente o enfermedad.
  Como contramedida tendríamos que replantear la planificación y encontrar la manera de compensar las horas de trabajo, sin saturar al equipo para continuar avanzando hacia la consolidación del proyecto.

2.4. Normativa LOPD y RGPD

Una de las obligaciones a las que debemos tener en cuenta cuando la organización opera con datos de terceros, es que debemos seguir con directrices que marca, la ley orgánica de protección de datos (LODP) y con el Reglamento Europeo de Protección de Datos (RGPD).

En materia de las tecnologías de la información, debemos ser conscientes de que estas normas obligan realizar backups o copia de seguridad, de cara a salvaguardar los datos personales de los clientes, proveedores y de los trabajadores ante potenciales desastres. Al margen de esta obligación legal que regula la realización de estas copias de seguridad según los artículos 94 y 102 del RD 1720/2007 de 21 de diciembre.

El cumplimiento del RGPD tiene implicaciones en la evaluación del impacto de la privacidad, la administración del acceso a los datos, y la notificación y resolución de fugas de datos, para ello se creado la figura del Delegado de Protección de Datos (DPD). Quien tiene la obligación de conocer la ubicación de todas las copias de seguridad, debe categorizar está en función de los contenidos y gestionar que los nuevos datos se incorporen, eliminando los contenidos no actuales. Esta actualización se debe realizar de forma periódica, la naturaleza de los datos determinara la periodicidad de las copias, aunque se recomienda que sea mínimo semanal. En el caso de que la organización tome la decisión de subcontratar los servicios a terceros, debería existir un contrato firmado entre el DPD de la organización y la entidad proveedora.

La solución escogida debe cumplir con los siguientes requisitos:

- Control de la ubicación de almacenamiento de datos personales, debemos tener en cuenta dos lugares de almacenamiento: in situ (en la propia organización) y/o en un centro de datos específico de la Unión Europea.
- Se debe garantizar la posibilidad de realizar búsquedas a nivel granular en las copias de seguridad, para facilitar la localización de la información.
- Debe ser capaz de exportar los datos personales a un formato habitual.
- Debe ofrecer cifrado fuerte de los datos personales tanto para los datos en tránsito como en reposo siendo cifrado totalmente automatizado, el DPD debe ser el único conocedor de la clave.
- Debe tener la posibilidad de copiar, modificar y eliminar datos personales de estas copias de seguridad.
- Debe ser capaz de recuperar rápidamente datos personales de las copias de seguridad

A partir de este punto, los agentes implicados en el proceso de respaldo de la información deben:

- Generar copias de seguridad cifradas de todos los datos personales con seudodenomización de ficheros y carpetas, de manera totalmente automatizada.
- Verificar todas las copias, simulando procesos de restauración para garantizar la integridad de cada copia de seguridad.
- En caso de pérdida de datos deben almacenarse un histórico mínimo de 15 días de copias de seguridad.
- Cuando se detecte una violación de seguridad, como puede ser robos de documentos, robos de equipos informáticos etc., se restaurará toda la documentación a su estado original, simultáneamente se deberá generar todos los informes pertinente para demostrar ante la Agencia Española de Protección de Datos las evidencias del cumplimento del artículo 32 del GDPR.

2.5. Análisis de la Arquitectura de la solución

Como administrador Backup, las funciones que debemos desarrollar son la administración, implantación, realización de planes de optimización y tuning en plataforma Backups, por esta razón realizaremos una reunión con los operadores de Backup siendo estos los encargados de supervisar la realización de las copias de seguridad, así como realizar pequeñas restauraciones de ficheros comprobando además que no hay problemas ni de rendimiento que puedan aumentar la ventana Backup ni alcanzar cierto umbral de almacenamiento.

En este estadio realizamos una puesta en común que nos permita analizar el escenario actual para establecer el diseño de la solución futura, a partir de la solución existente, para ello recogeremos información evaluando el RTO y el RPO, El Backup Windows, el espacio consumido por las copias. Por último, definimos los datos que debemos salvaguardar y lo comparamos con la política actual. Con todo esto posiblemente tengamos acotado el escenario actual que nos servirá de punto de partida para el nuevo sistema de Backup.

Ahora es el momento de ver las infraestructuras que ofrecen las distintas soluciones, para poder decir el entorno de trabajo, actualmente, podemos decidir tener el sistema de Backup, tanto en local, como en la nube, como en un entorno hibrido entre ambas, por ello vamos a entrar en detalle en estas infraestructuras para poder seleccionar la más pertinente para la organización.

- **Infraestructura On-Premises**
  - Ventajas
    - En esta solución, la organización tendrá un control físico sobre las copias de seguridad
    - Se mantienen la privacidad de los datos de la empresa al no asociarse con terceros
    - Los datos no son accesibles desde internet (solo se debe de preocupar de cumplir la LPOD)
    - Se puede implementar un cifrado de datos de alta seguridad, controlado por el Administrador de Backup.
    - El proceso de recuperación de datos será mucho más rápido, teniendo un RTO más bajo.
  - Desventajas
    - Sistemas especialmente diseñados con hardware escalable un ejemplo de esto sería la cabina de cintas o cabina de discos.
    - Mayor inversión de capital en una infraestructura física y virtual.
    - Consumo de espacio dedicado para un rack de servidores, un armario o una habitación.
    - Se debe tener especial precaución, puesto que los datos debido a la ubicación son más susceptibles a desastres como incendios, inundaciones, terremotos, etc. y apagones asociados, con lo que deberemos tener un plan de contingencia para estos supuestos.
    - La escalabilidad se ve comprometida en parte, puesto que puede requerir inversiones en hardware

- **Infraestructura On-Cloud**
  - Ventajas
    - No existen costos asociado al hardware
    - Escalable según necesidad de la organización.
    - Modelo de facturación es pago por uso o cuotas de pago periódicas

    - El Backup Window es mucho menor que On-Premises
    - Protección contra la pérdida de datos, la pérdida de sistemas, la pérdida de aplicaciones y la pérdida de la ubicación comercial.
    - La recuperación de datos se puede iniciar de manera deslocaliza, utilizando cualquier dispositivo.
  - Desventajas
    - Se pierde el control completo de sus datos.
    - El entorno de almacenamiento de datos de múltiples inquilinos conlleva desafíos de seguridad y cumplimiento.
    - Se la capacidad de recuperación y de copia si hay una caída de internet.
    - La recuperación completa de datos puede llevar mucho más tiempo, que en una solución On-Premises
    - Costo continuo
    - Se debe confiar en un tercero para mantener la seguridad de los datos.
- **Infraestructura Hibrida**
  - Ventajas
    - Fusión de ambas infraestructuras puede aprovechar la escalabilidad y la seguridad de la nube sin comprometer el control local
    - maximizar la seguridad y la disponibilidad y minimizar la latencia.
    - permite a las organizaciones aprovechar la escalabilidad de la nube para garantizar que los recursos de almacenamiento se adapten a sus necesidades.
    - limita la necesidad de costosas compras de hardware adicionales y permite a los equipos liberar recursos locales.
  - Desventajas
    - Costo continuo
    - Se debe confiar en un tercero parcialmente para mantener la seguridad de los datos.
    - Coste de hardware, aunque menor que on-premises pero necesario.
    - Consumo elevado de ancho de banda de internet

Teniendo esto en mente debemos de seleccionar el tipo de infraestructura que necesitamos en la organización. Como ya hemos indicado con anterioridad, las necesidades son mejorar el sistema actual de copias, Mejorar el RTO y el RPO, respetar la legislación actual y las recomendaciones (por ejemplo, las que propone Incibe) y en general reducir la ventana de Backup sin descuidar cumplir la norma Backup 3-2-1.

2.6. Elección del del software de Backup

Mas allá de las infraestructuras a emplear para almacenar las copias de respaldo, debemos pensar el software que se encargara de esta tarea, Existes aplicaciones nativas de los sistemas operativos, también existen aplicaciones externas a los S.O. Existen opciones gratuitas, opciones de pago, también sistemas de Código abierto así como software propietario, tenemos aplicaciones locales y otras alojadas en la nube, y existe la opción de realizar la operación de respaldo manualmente aunque esta última opción deja de ser practica cuando el caudal de datos y la frecuencia con la que se actualizan es muy alta, debido a la complicación que existe para gestionar las copias, por esto mismo, nos centraremos en las diferentes opciones de software existentes.

A la hora de seleccionar el software de Backup nos centraremos en los siguientes puntos:

- **Capacidad de seleccionar manualmente la información** que queremos realizar el respaldo. Por razones obvias, no siempre debemos respaldar todo, hay archivos no se modifican o directamente que carecen de importancia, existen unos archivos más críticos que otros, si realizamos copias de BBDD de la organización también debemos tener en cuenta que el software a elegir, pueda realizar la tarea. Por lo tanto, debemos realizar una clasificación de los datos que vamos a respaldar. De esta manera podemos empezar a cribar las soluciones que no son compatibles con la arquitectura de la información de la empresa, aquí sería bueno contar con la experiencia de los operadores actuales del sistema de copia.
- **Capacidad de crear copias del sistema operativo entero y máquinas virtuales**, esta opción es más que interesante, debido a la criticidad de ciertos sistemas, nos podemos ver con la necesidad de reconstruir la maquina entera, si tenemos una copia entera de estos sistemas, el tiempo de recuperación es muchísimo menor permitiendo restaurar la operatoria mucho más rápido, que en definitiva es uno de los puntos críticos.
- **Capacidad de encriptación con contraseña para acceder a la información**. Ante todo, debemos asegurarnos de la confidencialidad de los datos que estamos salvaguardando, siendo esto además una exigencia de la normativa LOPD, concretamente el artículo 102.2 que exige mínimo un cifrado de 128 bits para los soportes que contengan información de carácter personal.
- **Capacidad de compresión de los archivos en el respaldo.** Esto es necesario, para ahorrar costes de almacenamiento, ya sea en la propia infraestructura o en el Cloud, además la comprensión y la descompresión debe ser rápida para no dilatar la ventana de Backup ni el RPO.
- **Capacidad de establecer la frecuencia de respaldo.** Este dato es importante de acuerdo a nuestra estrategia del proyecto, ya que uno de nuestros puntos claves de esta, es establecer una política de retención, ya que si sufrimos una pérdida de datos puede ser que la última copia no sea funcional y tengamos que buscar una versión anterior, además tenemos que marcar una periodicidad tal que permita recuperar los datos lo más actualizados posibles, es decir que la necesitamos para hacer copias recurrentes de la información y también para generar un histórico de versiones.
- **Capacidad de adaptación a la infraestructura pre existente**, este punto es uno de nuestros riesgos que deben quedar cubiertos puesto que se debe adaptar a los sistemas de hardware existentes, así como del software empresarial, ya que es la única manera de reducir costes y además de asegurarse de que todos los datos que queremos salvaguardar pueden ser salvaguardados.
- **Capacidad de realizar informes y notificaciones por correo**, ante cualquier problema la solución escogida debe notificar a los operadores y al administrador de Backup, que ha

habido un problema, los informes que nos aporte la solución deben ser claros y útiles para que podamos detectar donde puede estar el problema y darle solución, por otro lado, informes de calidad que aporten estadísticas, umbrales de almacenamiento también son más que necesarios.

- **Capacidad de certidumbre**, en todo momento debemos tener la seguridad de que lo que se respalda pueda ser restaurado con versatilidad, puesto que de ello depende la continuidad de la activad empresarial y el software que escojamos debe restaurar los datos de forma consistente.
- **Capacidad de adaptación facilidad de configuración,** IT cambia a un ritmo vertiginoso y necesitamos que, ante cualquier cambio o nueva necesidad de la organización, nuestro sistema de Backup sea ágil y de fácil configuración, permitiendo integrar rápidamente los cambios a nivel de software y hardware.

Con todas estas premisas presentes, es hora de analizar el mercado en busca de la solución que mejor se adapte a nuestras necesidades y como ya hemos indicado al principio de este punto, existen multitudes de opciones a la hora de escoger un software de Backup, por lo que nuestro siguiente paso, es documentarnos para saber que nos ofrecen y de esta manera poder elegir la aplicación idónea.

2.7. Repositorios de Backup

Uno los aspectos que será necesario considerar desde el momento en que se planifica la puesta en marcha de un sistema Backup, es la forma en la cual se almacenarán los datos que serán generados. siendo de vital importancia esta decisión, ya que cada tipo de repositorio tiene sus ventajas y desventajas.

- Almacenamiento físico
  - Unidades USB HDD/SDD, estos dispositivos, también denominado discos duros externos son un dispositivos de almacenamiento que te permiten introducir, transportar, o copiar de forma sencilla una gran cantidad de documentos y archivos de un equipo a otro. utilizando actualmente el bus de datos USB 3.0, que supone un aumento de la velocidad de transferencia 10 veces superior a la versión anterior de este bus (2.0), este aumento de velocidad, junto con el hecho de ser portable, así como el coste byte relativamente bajo ya que 1 TB está en torno a 45€, han convertido estos dispositivos en unidades de almacenamiento muy utilizados para realizar un respaldos de datos offsite.
  - Unidades RDX, la tecnología RDX proporciona un sistema de almacenamiento basado en disco con cartuchos extraíbles para obtener lo mejor del disco: rendimiento en el acceso aleatorio, alta velocidad de transferencia, fiabilidad de datos, capacidad escalable; y lo mejor de la cinta: portabilidad, larga durabilidad, automatización, robustez y bajo coste. Utiliza para formato el interno SATA III, para el formato externo USB 3.0, los cartuchos son discos duros recubiertos de una carcasa de plástico que los hace resistentes a caída, y transportables con total fiabilidad, los dispositivos RDX son universales e independientes de la capacidad del disco, con lo que es una tecnología de fácil escalado, ya que, si en el futuro hay un crecimiento de datos en la organización, basta con adquirir cartuchos de mayor capacidad.
  - Dispositivos de cinta (LTO), La tecnología LTO permite almacenar grandes cantidades de datos en soportes magnéticos de cinta con un coste muy bajo por GB, esta tecnología, es ampliamente utilizada para realizar copias de seguridad especialmente en entornos empresariales, donde las bases de datos y la

virtualización plantean necesidades de copia de seguridad de un cierto nivel. Con una duración estimada de cerca de 30 años, estos soportes son perfectamente adecuados para conservar los datos a largo plazo. Por esto mismo, esta tecnología continúa desarrollándose hoy en día. Actualmente nos encontramos en la octava generación a nivel comercial, que tiene capacidad de almacenar hasta 30TB por cartucho, con cifrado de datos de hardware y Con velocidades de transferencia de datos de hasta 300 MB/s nativos, desarrollado y pendiente de implantar la tecnología se encuentra en LTO-13 con una capacidad en raw de 384TB y 960TB y se está desarrollando el LTO-14 con una capacidad en raw de 768TB y 1920TB

- Dispositivos NAS, Un dispositivo NAS consiste en un dispositivo de almacenamiento conectado a la red (Network Attached Storage). Normalmente suele ser un ordenador con su propio sistema operativo y que está adaptado para estar todo el día funcionando, orientado para el almacenamiento en red. El precio de estos dispositivos va en función de la RAM y procesador que incorporen, así como el número de bahías de disco que pueda tener, otro aspecto para tener en cuenta es que la mayor parte de soluciones profesionales, no incluyen disco, aquí lo recomendado es utilizar discos duros preparados para rendir correctamente en dispositivos NAS.

Normalmente estos sistemas permiten varias configuraciones de RAID

- Raid 0 combina dos o más unidades para aumentar el rendimiento y la capacidad, pero no ofrece tolerancia a los fallos
- Raid 1 Se necesitan 2 o más unidades ya que los datos de las unidades se copian a la vez, proporcionando una tolerancia a fallos en caso de avería en las unidades.
- RAID 5 proporciona tolerancia a fallos y un mayor rendimiento de lectura, Se necesita un mínimo de tres unidades. En caso de producirse un fallo de unidad, los datos de la unidad averiada se reconstruyen a partir de la paridad guardada.
- RAID 6 es similar a RAID 5, con la diferencia de que proporciona una capa adicional de striping y puede tolerar el fallo de dos unidades. Se necesita un mínimo de cuatro unidades.
- RAID 10 combina los beneficios de RAID 1 y RAID 0. El rendimiento de lectura y escritura aumentan, pero solo la mitad del espacio total está disponible para almacenar datos. Se necesitan cuatro o más unidades

- Almacenamiento Cloud

El almacenamiento en la nube es un servicio que permite almacenar datos transfiriéndolos a través de Internet o de otra red a un sistema de almacenamiento externo que mantiene un tercero, estos sistemas sistemas de almacenamiento suelen ser escalables para adaptarse a las necesidades de almacenamiento de datos de una persona o una organización, accesibles desde cualquier lugar e independientes de aplicaciones para ofrecer accesibilidad desde cualquier dispositivo.

Los principales modelos de servicio son:

- Nube publica, El almacenamiento en la nube consiste en un servicio de almacenamiento mantenido por un proveedor de Cloud que es quien se encarga de la custodia, el almacenamiento y la accesibilidad de los datos contenidos. permiten el escalado hacia arriba y hacia abajo según las necesidades., en cuanto a la seguridad de los datos, la mayoría de los proveedores de almacenamiento en la

nube ofrecen medidas de seguridad básicas que incluyen control de acceso, autenticación de usuarios y cifrado de datos.

- Nube privada, El almacenamiento en la nube privada suele replicar el modelo nube pública, pero, las infraestructuras residen dentro de la red local, aunque también existe la posibilidad de contratar a un proveedor de almacenamiento en la nube para crear una nube privada dedicada a la que pueda acceder con una conexión privada.
- Nube híbrida, Este modelo de almacenamiento, combina elementos de nubes públicas y privadas, lo que brinda a las organizaciones la opción de elegir qué datos almacenar en qué nube.

En cuanto al almacenamiento en la nube disponemos tres tipos principalmente:

- Almacenamiento en bloque, en este modelo de almacenamiento, los datos se organizan en grandes volúmenes llamados "bloques", cada bloque representa un disco duro independiente. Los proveedores de almacenamiento en la nube utilizan bloques para dividir grandes cantidades de datos entre varios nodos de almacenamiento.
- Almacenamiento de archivos, el modelo de almacenamiento de archivos guarda los datos en la estructura jerárquica de archivos y carpetas, los datos conservan su formato, ya sea que residan en el sistema de almacenamiento o en el cliente donde se originan, y la jerarquía hace que sea más fácil e intuitivo buscar y recuperar archivos cuando sea necesario.
- Almacenamiento de objetos el modelo de almacenamiento de objetos se diferencia del almacenamiento de archivos y bloques en que administra los datos como objetos estos objetos incluyen los datos en un archivo más sus metadatos asociados y un identificador único. en cuanto al funcionamiento, hay que indicar que los objetos almacenan los datos en el formato en el que llegan y permiten personalizar los metadatos de manera que faciliten el acceso y el análisis de los datos. En lugar de organizarse en archivos o jerarquías de carpetas, los objetos se guardan en repositorios que ofrecen una escalabilidad prácticamente ilimitada. Dado que no existe una jerarquía de archivo y los metadatos se pueden personalizar, el almacenamiento de objetos le permite optimizar los recursos de almacenamiento de una manera rentable.

2.8. Optimización de la capacidad

Antes de analizar el mercado de las soluciones Backup, debemos entender bien las tecnologías que participan en la creación de backups y al analizar brevemente el mercado de estas soluciones, observamos que aunque tradicionalmente en software para la realización de respaldos, hacia uso de diferentes librerías de compresión para poder hacer un uso óptimo de la capacidad de almacenamiento, actualmente debido ingente cantidad de datos que las organizaciones manejan a día de hoy hacen necesarias tecnologías que optimicen tanto el envío, como el almacenamiento y la salvaguarda de la información.

Una de las tecnologías más utilizadas hoy día en casi todos los sistemas de Backup, consiste a parte de la comprensión, la de duplicación de datos y es que actualmente, las técnicas de deduplicacion han hecho posible optimizar al máximo los recursos empleados en estas tareas,

así como permiten una mayor adaptación a las particularidades de cada organización en este importante proceso de manera que hoy en día es imprescindible plantearse su uso en una estrategia adecuada de Backup. La razón por la que se utilizan estas técnicas es porque no solo mejoran la utilización del espacio de almacenamiento, sino que, además, se suele aplicar en las transferencias de datos de la red para reducir la cantidad de bytes que se deben enviar

Durante el proceso deduplicacion, se identifican, ficheros idénticos en diferentes ubicaciones, con lo que solo necesitamos almacenar una copia, sino que igualmente se identifican y almacenan fragmentos únicos de datos, o patrones de bytes, durante el proceso de análisis. cuando se produce una coincidencia entre fragmentos de diferentes ficheros, el fragmento redundante se reemplaza por una pequeña referencia que apunta al fragmento almacenado, como un mismo patrón de bytes puede ocurrir docenas, cientos o incluso miles de veces, la cantidad de datos que se deben almacenar o transferir se puede reducir considerablemente.

Esta técnica como acabamos de observar es muy diferente de la compresión, que consiste en identificar los datos redundad entes dentro de archivos individuales, codificando estos de manera eficiente. La deduplicacion puede ocurrir "en línea", a medida que fluyen los datos, o “postprocesar” después de que se hayan escrito.

Debemos destacar que la deduplicacion tiene dos variantes:

- Deduplicacion en origen

  Al realizar una copia de seguridad en un almacenamiento con deduplicacion, la solución de copia de seguridad calcula un hash de cada bloque de datos, verificado la unicidad de cada bloque en una “base de datos”. Los bloques únicos se envían al almacenamiento y se omiten los duplicados. Esta técnica, permite que la transmisión de información entre los sistemas de origen y destino sea mínima.

- Deduplicacion en destino
  Una vez que se completa una copia de seguridad en un almacenamiento con deduplicacion, el sistema de almacenamiento realiza la deduplicacion del lado del almacenamiento. se almacenan primero en el dispositivo de almacenamiento y luego un proceso en un momento posterior analizará los datos en busca de duplicaciones. La ventaja que aporta esta técnica es que no es tiene la necesidad de terminar de calcular los hash para empezar el proceso de almacenamiento, con lo que la ventana de Backup puede ser menor, además de ofrecer unas tasas mayores de deduplicacion.

Ambos métodos suelen ser objeto de un intenso debate, pero sobre todo conforme ha ido creciendo el binomio de deduplicacion de datos y el Cloud. Siendo así porque la mayoría de los proveedores de nube pública cobran por el almacenamiento de datos por gigabyte almacenado. Las técnicas de deduplicacion de datos son importantes para reducir los costos de la nube en virtud de la reducción del volumen de datos respaldados en los sistemas de la nube, siendo esencial para minimizar los costos ocultos asociados con la realización de copias de seguridad de sus datos mediante los servicios de nube pública.

2.9. Políticas de Backup

Una política de Backup establece la importancia de los Backups de datos y del sistema, define las reglas básicas para planificar, ejecutar y validar Backups e incluye actividades específicas para garantizar que los datos críticos se respalden en un medio de almacenamiento seguro. El esquema de protección predeterminado de la política garantiza la capacidad de recuperación

de servidores, componentes de red y otros dispositivos de infraestructura, así como aplicaciones críticas, bases de datos y archivos importantes.

Las políticas de copia de seguridad también deben incluir la métrica del objetivo de punto de recuperación (RPO) que define cuánto tiempo se deben almacenar los datos (por ejemplo, antigüedad) antes de que se deba realizar una copia de seguridad nuevamente. Los valores de RPO, por lo general un período de tiempo como segundos o minutos, los definen los propietarios de los datos y el sistema empresarial, y la alta dirección puede revisarlos y aprobarlos. Cuanto menor sea el tiempo de almacenamiento de los datos de la copia de seguridad antes de que se necesiten para una situación de recuperación, mayor será el costo de la copia de seguridad y el almacenamiento.

Esto significa que se deben utilizar tecnologías como la deduplicacion, en el caso de repositorios en LAN o WAN, debe tener capacidad de red de alta velocidad y baja latencia para lograr los objetivos de RPO.

En general, un proceso de referencia de la política de Backup especifica la captura de un Backup completo inicial de datos, seguido de una serie de Backups diarios incrementales o diferenciales intermedios, entendamos que una copia de seguridad incremental es una copia de los datos creados y modificados desde la última ejecución de la copia de seguridad, tanto en copias incrementales como completas mientras que las copias diferenciales, son una copia de los datos creados y modificados desde la última copia de seguridad completa.. Independientemente del método que se utilice, debemos tener en cuenta el método 3-2-1 Backup, esta estrategia de Backup consiste en tener 3 copias totales de sus datos, dos de las cuales son locales, pero en diferentes medios (lea: dispositivos), y al menos una copia offsite.

Lo primero que debemos tener claro para realizar una política de Backup, es que queremos respaldar ya que existen archivos de datos, las bases de datos, los programas de utilidades, máquinas virtuales, etc. y casi cualquier software de la organización debe respaldarse, una vez tenemos claro que queremos respaldar, según la criticidad, la variabilidad de la información podremos definir cuando realizar las copias es decir con cuanta periodicidad realizar las copias. De la misma manera podremos definir cuanto tiempo debemos conservar los datos, es decir aplicar una política de retención, que no es más que definir cuantos puntos de restauración serán mantenidos en una cadena de Backup, para asegurar que contemos con el periodo de retención necesario requerido por la compañía.

En definitiva, el propósito de las políticas de Backup es asegurar que exista un método consistente y confiable para recuperar datos, por ello se debe determinar qué información se respalda, cuándo y con qué frecuencia, también describe cómo se administran y mantienen las copias de seguridad y detalla los responsables de su gestión.

Los puntos que tener en consideración a la hora de elaborar esta política son:

- Que tecnologías utilizadas para realizar copias de seguridad, recuperar y restaurar datos y sistemas
- Que tipos de datos y sistemas que se necesita respaldar
- Que requisitos de infraestructura para garantizar que se puedan completar las copias de seguridad
- Que personal profesional es encargado de realizar copias de seguridad y recuperaciones.
- Establecer procedimientos de emergencia si las copias de seguridad de los datos se ven comprometidas.

- Establecer procedimientos para garantizar que los datos críticos se almacenen de forma segura en caso de corrupción de datos, ataque de ransomware u otro evento de ciberseguridad.

A partir, de ahí se generará un documento en el que se tengan en cuenta las métricas (RPO, RTO, Etc), el nivel de granularidad, el propósito y el alcance, verificación del cumplimiento de la política así como sanciones por incumplimiento, debe presentarse al departamento legal (si existiese) y de recursos humanos, así como gerencia de la organización.

2.10. Soluciones de respaldo Opensource

En cuanto al open source tenemos dos modelos diferentes de soluciones muy diferenciados, uno sería el software tradicional construido a partir de un conjunto de herramientas de respaldo, que, si bien otorgan la capacidad de realizar la tarea de Backup a equipos en redes ip utilizando la arquitectura Cliente servidor, no está enfocado a ser un servicio Cloud propiamente dicho, como ejemplo de este tipo de software tenemos Amanda, BackupPC, Bacula, Etc. estos sistemas son los sistemas de Backup más tradicionales. Por otro lado, hay una nueva corriente en cuanto a soluciones de respaldo que son soluciones orientadas a Cloud que gracias a su interfaz web permite la gestión de las copias de seguridad a través de internet, de manera deslocalizada, como ejemplo de estas soluciones tenemos Urbackup y también Duplicati.
Para este punto vamos a analizar un sistema de los llamados tradicionales como es Bacula para después entrar en analizar Urbackup y por último veremos la solución Duplicati, al aportar cada uno un enfoque en los sistemas de Backup diferente

2.10.1. Bacula

Bacula más que un software, es un conjunto de herramientas que permiten gestionar las copias de seguridad, la recuperación y la verificación de los datos informáticos, entre sus características principales, esta su diversificación, ya que está dividido en varias partes interrelacionadas entre sí. esas partes, no tienen por qué encontrarse en la misma máquina.
Principalmente existen 4 partes cada cual tiene su propio programa de instalación, una parte se denomina file, siendo esta la maquina cliente que es donde se encuentra la información que necesitamos respaldar otra parte es el storage que se encarga de almacenar la información, otra parte se denomina Catalog que es la BBDD donde se almacenan los registros de las operaciones realizadas, otra parte se denomina Director que es la parte que se encarga de gestionar todo el proceso y por ultimo esta la consola Bacula, que permite la comunicación entre director y el usuario siendo este desde el administrador de Backup como los operadores de Backup, para operar con el sistema.
Existen interfaces web o Gui como BWeb Management Suite es una aplicación web que ofrece sencillez a la hora de supervisar y administrar Bacula a través de una interfaz web, pero no deja de ser una interface limitada que actúa sobre director.

Para poder realizar el proceso de copia se hace uso de demonios y cada parte tiene su propio demonio teniendo así Bacula-director, Bacula-fd (file-Daemon) y Bacula-sd (storage-Daemon), estos demonios, se configuran mediante ficheros donde se definen cada uno de los componentes del demonio, los puertos a la escucha, el comportamiento durante los procesos que lleva acabo, etc. Hay que mencionar que toda la información del proceso como pueden ser los eventos, volúmenes y clientes se almacena una base dados y esta puede ser MySQL, SQLite y PostgreSQL.
Uno de los puntos fuertes de este sistema es la seguridad ya que cada cliente, cada storage y cada director que instalemos tiene su propia clave, que será utilizada para cifrar la información y aunque se permite configurar esta clave de manera manual cada programa genera una de

forma aleatoria de 30 caracteres. además del propio cifrado, Bacula también admite las conexiones seguras TLS, añadiendo una capa más de seguridad, al generar certificados y claves únicas ssl para cada máquina.
El almacenamiento, se puede realizar sobre unidades de cinta, unidades de discos, permitiendo además el Cloud storage para un sistema hibrido de Cloud, al permitir utilizar el almacenamiento en Amazon S3 mediante plugins.

ARQUITECTURA TÍPICA DE BACULA:

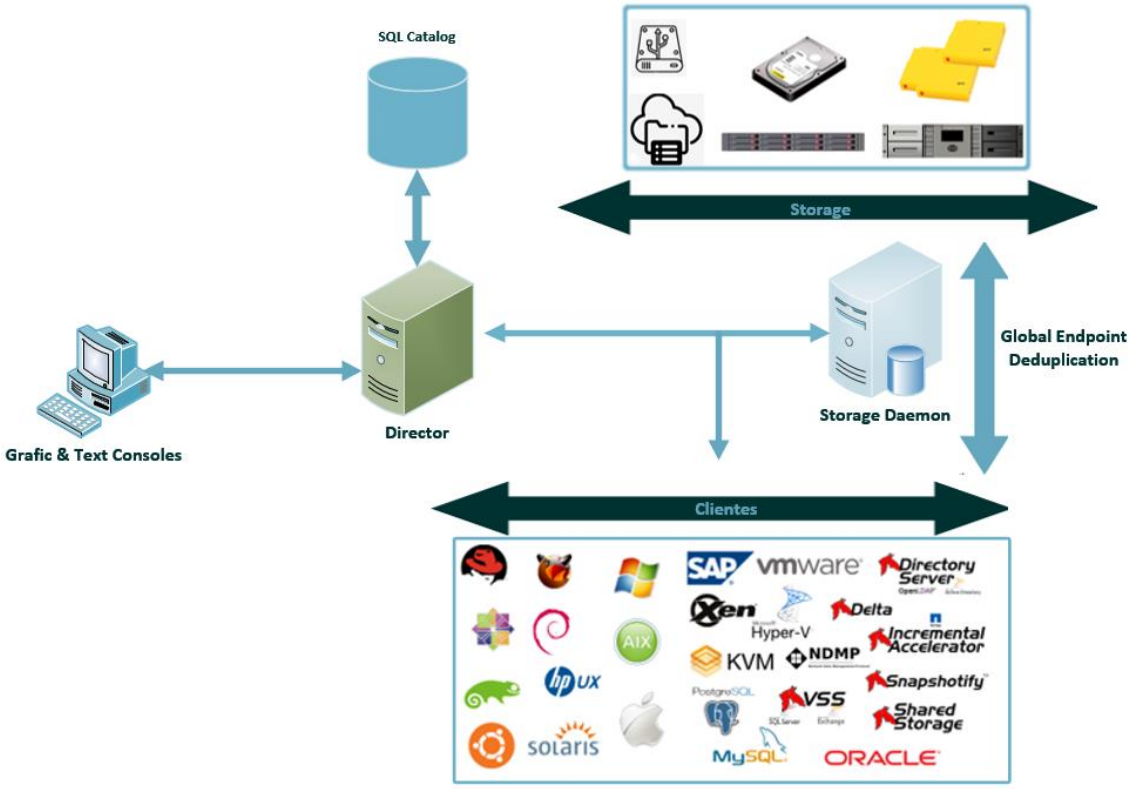

Figura 3. Arquitectura Bacula

Como suele ocurrir en el software open source, existen dos ediciones, una versión Community Opensource y otra Enterprise bajo licencia propietaria. La versión Community puede ser vista como la base funcional de la Enterprise ya que las funcionalidades primeramente se desarrollan en esta versión.

Luego de ser probadas por un gran número de usuarios se trasladan hacia la Enterprise donde son atendidas directamente por el desarrollador, además de ofrecer una serie de servicios de valor añadido, en la siguiente tabla vemos una comparativa entre ambas versiones.

Visión general	Community	Enterprise
Código libre	SI	NO
Parches	NO	SI
Apoyo	NO	SI
Binarios certificados	NO	SI
Certificación y prueba	NO	SI
Soporte y servicios		
Centros de formación certificados por Bacula	SI	NO
Consultoría de Bacula Systems y socios certificados	NO	SI
Foros comunitarios en línea	SI	SI
Soporte técnico profesional	NO	SI
Asistencia remota (para instalación / configuración, diseño, resolución de problemas, optimización)	NO	SI
Acceso a documentación profesional	NO	SI
Opción de soporte técnico 24/7	NO	SI
Acceso inmediato a correcciones de Bacula completamente probadas	NO	SI
Visibilidad e influencia de la hoja de ruta	NO	SI
Ciclos de lanzamiento administrados	NO	SI
Derecho a nuevas funciones y actualizaciones	NO	SI
Características avanzadas		
Tecnología de instantáneas	NO	SI
Gestión de instantáneas	SI	SI
Restauración de un solo archivo para VMware	NO	SI
Recuperación de buzón único para Exchange	NO	SI
Copia de seguridad iniciada por el cliente	NO	SI
SD de Windows	NO	SI
Soporte de Windows EFS	NO	SI
Cambio de dispositivo de almacenamiento	NO	SI
Reiniciar trabajo fallido	SI	SI
Estadísticas de la línea de comunicación	NO	SI
Mejora del rendimiento del catálogo	NO	SI
Estadísticas periódicas para ejecutar trabajos en Director	SI	SI
Comando truncar	SI	SI
Replicación de SD a SD	SI	SI
Replicación de SD a SD con deduplicación	NO	SI
Compresión de la línea de comunicación	NO	SI
Directiva de unidad de solo lectura	SI	SI
Esquema de catálogo de alto rendimiento	NO	SI
Deduplicación global de endpoints	NO	SI
Formato de volumen alineado	SI	SI
Protección de datos continua	NO	SI
Cliente detrás de NAT	NO	SI
Complementos		
LDAP y Active Directory	NO	SI
VMware	NO	SI
Virtualización de Red Hat	NO	SI
KVM	NO	SI
Hyper-V	NO	SI

Xen	NO	SI
Proxmox	NO	SI
Estibador	NO	SI
Kubernetes	NO	SI
Complemento para SAP	NO	SI
Windows VSS	NO	SI
Recuperación completa de Windows	NO	SI
Recuperación completa de Linux	NO	SI
Complemento NDMP	NO	SI
Acelerador incremental para el complemento Netapp	NO	SI
Complemento de Oracle con SBT	NO	SI
Complemento de PostgreSQL	NO	SI
Complemento MySQL Percona	NO	SI
Complemento de SAP HANA	NO	SI
Complemento SAP (Sybase) ASE	NO	SI
Complemento para servidor MSSQL	NO	SI
Complemento delta	NO	SI
Complemento de almacenamiento compartido de San	NO	SI
Complemento de Azure Cloud	NO	SI
Complemento de nube de AWS	SI	SI
Complemento de Google Cloud	NO	SI
Complemento de Oracle Cloud	NO	SI
Complemento Glacier Cloud	NO	SI
Instrumentos		
Herramienta administrativa de Bacula	Limitado	SI
Suite de gestión BWeb	NO	SI
Servicio BCloud	NO	SI
Opciones de restauración del complemento BWeb	NO	SI
API REST	SI	SI

Figura 4.Tabla Comparativa Comunity Vs Enterprise Bacula

BACULA	
Capacidad de seleccionar manualmente la información	Bacula le ofrece la posibilidad de restaurar archivos individuales a partir de una copia de seguridad completa, también permite realizar copias de seguridad de bbdd SQL server, tanto a nivel completo como a nivel de transaccional, con lo que si tiene esta capacidad
Capacidad de crear copias del sistema operativo entero y máquinas virtuales	Bacula Enterprise Edition proporciona herramientas para realizar copias de seguridad de imágenes de máquinas virtuales a través de sus API de copia de seguridad de hipervisor y permite el clonado de equipos completos. Con lo que tiene esta capacidad.
Capacidad de encriptación con contraseña para acceder a la información	Bacula permite el cifrado de datos de archivos y la firma dentro del File Daemon (o Cliente) antes de enviar datos al Storage Daemon. Tras la restauración, las firmas de los archivos se validan y se informa de cualquier discrepancia. Con lo que tiene esta capacidad
Capacidad de compresión de los archivos en el respaldo	A nivel de compresión utiliza LZO, que proporciona una relación de compresión muy alta con un buen rendimiento al admitir compresión superpuesta y descompresión in situ que le hacen uno de los algoritmos de compresión y descompresión más rápidos que existen. con lo que tiene esta capacidad
Capacidad de adaptación a la infraestructura pre existente	Tiene compatibilidad con casi todos los SO utilizados en la organización a implementar y a nivel de hardware es compatible con el Hardware pre existente cumpliendo de esta manera con este requisito
Capacidad de realizar informes y notificaciones por correo	Si que tiene la capacidad de envío de notificaciones según los diversos estados, advertencias, problemas, para pada poder tener un servicio de reporting simple y claro, debemos utilizar aplicaciones de terceros como pandorafms que conecten con el sistema Bacula
Capacidad de certidumbre	Bacula compara los atributos del archivo actual con los atributos que se han almacenado previamente en el Catálogo de Bacula, dotándole de la capacidad de detectar cambios en archivos de manera muy similar a lo que realiza Tripwire cuando verifica la integridad de los archivos, el uso de comandos de Pipe Nominado permite que se realicen copias de seguridad consistentes, con lo que esta funcionalidad es cumplida
Capacidad de adaptación, facilidad de configuración	Este es el punto más débil de este conjunto de software, como es altamente configurable y muy versátil, también puede ser difícil de configurar para gente que no tenga experiencia en sistemas unix, puede resultar complicado configurar el director, al ser este quien se encarga de realizar la coordinación de todo el sistema, aunque una vez configurado se convierte en un sistema robusto

Figura 5. Tabla de elementos comparativos de Bacula

2.10.2. UrBackup

UrBackup consiste en una herramienta de copias de seguridad Opensource para clientes y servidores, que permite realizar respaldos de seguridad consistentes, utilizando una combinación de archivos e imágenes mientras el sistema se encuentra en ejecución, sin interrumpir los procesos que se están realizando.

De esta manera tenemos un sistema que logra la seguridad de los datos con un tiempo de restauración rápido sin sobrecargar los equipos que son respaldados, para realizar estas tareas, monitoriza las carpetas que se desea respaldar para encontrar diferencias realizando así copias incrementales realmente rápidas.

Para ser más eficiente, en el caso de querer respaldar los mismos archivos en diferentes clientes, UrBackup es capaz de detectar esta condición, realizando una única copia, haciendo un menor consumo de espacio de almacenamiento, al tener una interfaz web intuitiva integrada, permite que la gestión de copias sea sencilla, por otro lado, esta interfaz muestra información acerca del estado de los diferentes clientes, así como las actividades actuales permitiendo monitorizar toda la infraestructura de Backup utilizando estadísticas e informes intuitivos.

Para poder restaurar los archivos, se puede utilizar tanto la interfaz web, como a través del propio cliente además de permitir el uso de CD o un USB de restauración. En cuanto, al servidor, este es multiplataforma, con lo que se puede ejecutar tanto en Windows, GNU/Linux, FreeBSD permitiendo el valor añadido de ser ejecutado directamente en algunos sistemas operativos de algunos NAS.

Para realizar le compresión y el cifrado, se apoya en diferentes sistemas de archivos con los que es compatible NTFS, Btrfs, ZFS, el motivo por el que no utiliza un cifrado durante el proceso de copia, se debe principalmente a dos motivos, el primero es por eficiencia en el almacenamiento, la deduplicacion, el hecho de que al encontrar dos ficheros idénticos, solo se guarde uno y almacene un enlace simbólico del resto le permiten hacer un consumo moderado del espacio, pero si se cifran los datos dos archivos idénticos dejan de serlo, perdiendo esta funcionalidad perdiendo a su vez la capacidad de compresión. Si aun así deseamos tener un sistema de compresión adicional, el desarrollador recomienda utilizar como he indicado antes ZFS o Btrfs como sistema de ficheros ya que estos permiten compresión desde su propia concepción y si se monta el servidor en un sistema Windows podemos utilizar el seguimiento de bloques de cambios para rastrear que bloques cambian entre si reduciendo tiempo y espacio en las copias incrementales, si se requiere cifrar la información UrBackup recomienda para el caso de Windows cifrar la unidad ya sea usando BitLocker en el caso de Windows o dmcrypt si se utiliza Linux.

Utilizando Infscape AWS o Azure UrBackup Appliance obtenemos un dispositivo basado en Linux que integra UrBackup en un entorno completamente Cloud, lo cual nos proporciona un sistema de respaldo robusto, completamente Cloud que para almacenar las copias utilizara o bien escritura diferida utilizando la cache local utilizando Direct o almacenamiento Cloud en nubes como la de Amazon S3, Backblaze B2 , daDup , permitiendo además comunicación con diferentes softwares Opensource de almacén de objetos como son OpenStack Swift , Ceph o Minio y por lo tanto capacidad de utilizar las diferentes nubes que utilicen estos softwares.

ARQUITECTURA TÍPICA DE URBACKUP:

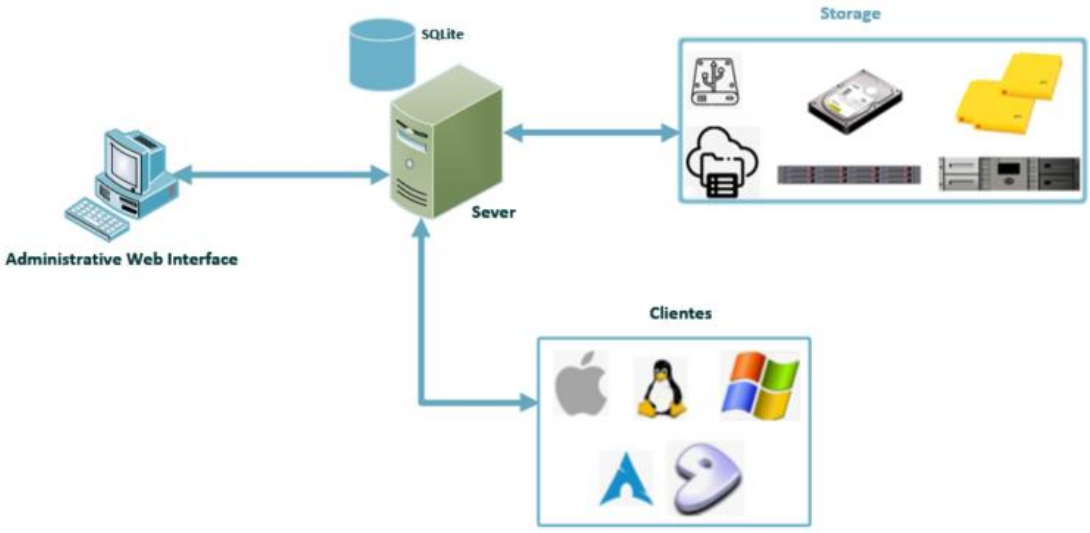

Figura 6.Arquitectura de UrBackup

UrBackup	
Capacidad de seleccionar manualmente la información	UrBackup permite el respaldo de imágenes enteras de equipos, así como la selección de archivos. con lo que tiene la capacidad de seleccionar la información a respaldar.
Capacidad de crear copias del sistema operativo entero y máquinas virtuales	Como se ha indicado en el punto anterior, UrBackup tiene la capacidad de realizar imágenes de equipos enteros con lo que está capacitado.
Capacidad de encriptación con contraseña para acceder a la información	UrBackup, no hace uso del cifrado ni de archivos ni de imágenes por temas de rendimiento y gestión de espacio, no obstante, el desarrollador delega esta tarea en el uso de soportes cifrados que hacen uso de la tecnología BitLocker en el caso de Windows o dmcrypt si se utiliza Linux.
Capacidad de compresión de los archivos en el respaldo	De la misma manera que no hace uso de cifrado, tampoco comprime los archivos, lo que si hace es hacer un uso eficiente del disco en copia, copiando únicamente bloques de información que se hayan modificado, así utilizar técnicas avanzadas de deduplicacion. No obstante, como valor adicional se puede utilizar sistemas de ficheros que hacen uso de compresión.
Capacidad de adaptación a la infraestructura pre existente	En cuanto a la capacidad de adaptación UrBackup, es multi-plataforma tanto a nivel de servidor como de cliente, a nivel de hardware es compatible con todo tipo de infraestructura, con lo que cumple con esta condición.
Capacidad de realizar informes y notificaciones por correo	El servidor de respaldo tiene una interfaz web integrada que muestra el estado de los clientes, las actividades actuales y las estadísticas, así como notificaciones de alertas y estados.
Capacidad de certidumbre	UrBackup realiza una copia de seguridad de los archivos abiertos, aunque estén en uso, la consistencia es su mayor objetivo y al analizar a bajo nivel los datos, resulta un sistema confiable con alta certidumbre.
Capacidad de adaptación, facilidad de configuración	El hecho de que sea un sistema abierto, orientado a cloud es decir que la infraestructura puede estar deslocalizada, hace que sea un sistema adaptable. Por otro lado, una de sus premisas de desarrollo, es que sea fácil de configurar, permitiendo configurar los clientes desde el servidor, no haciendo fala utilizar la interface del cliente, centralizando todo el proceso.

Figura 7.Tabla de elementos comparativos de UrBackup

2.10.3. Duplicati

Duplicati es un sistema de respaldo multiplataforma Opensource diseñado para copias de seguridad online que tiene la capacidad de almacenar la información segura y consistente mediante respaldos encriptados, incrementales y comprimidos en almacenamiento local, servicios de almacenamiento en la nube y servidores de archivos remotos. Surgido en una primera versión con una funcionalidad similar a Duplicity, evoluciono hacia una versión 2 utilizando un nuevo modelo más eficiente de almacenamiento.

La solución de copia de seguridad que propone está basada en bloques. Los archivos se dividen en pequeños fragmentos de datos (bloques), que opcionalmente se cifran y comprimen antes de enviarlos a la ubicación de la copia de seguridad. Lo que le dota de una excelente capacidad de Deduplicacion, ya que analiza el contenido de los archivos de tal manera que es capaz de encontrar archivos duplicado o con contenido similar almacenando una sola vez estos bloques, de esta manera tenemos un consumo eficaz de los repositorios de almacenamiento.

Utiliza un fuerte cifrado AES-256 para proteger los archivos de respaldo siguiendo el principio TNO, al trabajar con bloques realiza inicialmente una copia completa de los archivos a respaldar para posteriormente realizar copias incrementales agregando los bloques modificados ahorrando tiempo y espacio y el tamaño de la copia de seguridad.

Aparte de esto todos los datos de la copia de seguridad, se comprimen antes de realizar el cifrado y se puede parametrizar para utilizar zip o 7z.

Entre las muchas características que dispone tiene la capacidad de utilizar *Volume Shadow Copy Services* en Windows y *Logical Volume Management* para realizar instantáneas coherentes, aunque el archivo este en ejecución además de poseer un sistema de verificación online excelente, al descargar aleatoriamente un conjunto de archivos de respaldo verificando después su integridad, con lo que podemos detectar cualquier problema existente en los archivos de respaldo, antes de necesitarlos.

Obviamente consiste en un sistema de copias de seguridad diseñado para gestionar todo tipo de problemas, problemas de rede, interrupción de Backup, sistemas de almacenamiento no disponibles o corruptos, para hacernos una idea de la capacidad de esta solución si los archivos de Backup se corrompen, si los originales están disponibles, este software va a intentar reconstruir la copia lo máximo posible.

Con interface web intuitiva para agilizar la gestión de las copias de seguridad y con un sistema de línea de comandos para realizar respaldos de seguridad en una ventana de terminal incorporando estas características a los scripts que desarrollemos, por ultimo y no menos importante permite la instalación directamente en ciertos NAS, que para el caso de pequeñas infraestructuras es más que funcional.

Los repositorios que puede utilizar van desde una carpeta compartida hasta un USB pero además puede utilizar protocolos estándar como FTP, SSH, WebDAV y apoyarse servicios Cloud de forma nativa como son Backblaze B2 , Tardigrade , Microsoft OneDrive, Amazon S3, Google Drive, box.com, Mega, hubiC, permitiendo al administrador de copia mantener la regla 3-2-1 Backup de manera sencilla, ya que a partir de una copia, podemos distribuirla fácilmente en dos soporte y uno offsite.

ARQUITECTURA TÍPICA DE DUPLICATI:

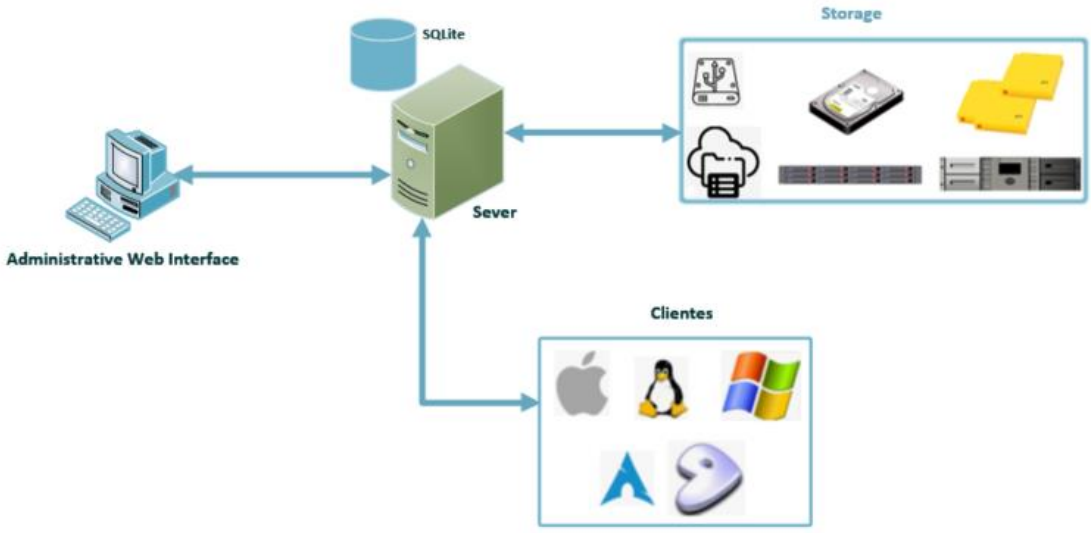

Figura 8. Arquitectura de Duplicati

Duplicati	
Capacidad de seleccionar manualmente la información	Entre sus características esta la capacidad de realizar copias de seguridad de archivos y carpetas, es decir que tiene la capacidad de seleccionar manualmente la información y esta puede ser desde ficheros y carpetas hasta BBDD de MSSQL
Capacidad de crear imagen sistema y máquinas virtuales	Este Software, puede realizar puede hacer una copia de seguridad de los archivos y carpetas seleccionadas, pero no tiene la capacidad de realizar un archivo de imágenes, para esta tarea, el desarrollador recomienda utilizar Clonecilla y mediante Duplicati actualizar los datos.
Capacidad de encriptación con contraseña para acceder a la información	la solución que aporta un fuerte cifrado AES-256 para proteger sus copias de seguridad, pudiendo utilizar instancias GPG locales.
Capacidad de compresión de los archivos en el respaldo	Duplicati admite compresión Zip|Deflate o 7z| LZMA2 y esta tarea la realiza en un paso anterior al cifrado, con lo que si dispone de esta capacidad.
Capacidad de adaptación a la infraestructura pre existente	Este sistema aparte de ser multiplataforma, tanto a nivel de servidor como de clientes, también es compatible con todo tipo de repositorios y protocolos de comunicación, si nos centramos en sistemas Cloud, de forma nativa hoy en día es compatible con más de 19 proveedores de almacenamiento en Cloud
Capacidad de realizar informes y notificaciones por correo	Si tiene un completo sistema de reporting en un dashboard y además de enviar las notificaciones de estado de cada tarea por correo, si aun así se precisara algo más especifico, podemos utilizar la herramienta Duplicati Monitoring que es gratuita y brinda la posibilidad recibir informes periódicos por correo, así como un nuevo panel de monitorización de las copias.
Capacidad de certidumbre	Duplicati realiza de manera aleatoria verificaciones de consistencia sobre los archivos de respaldo y si detecta algún bloque corrupto, intenta recuperar la información, de tal manera que, en caso de restauración de los datos, estos sean consistentes.
Capacidad de adaptación, facilidad de configuración	Una de las motivaciones del proyecto Duplicati es mantener lo más simple posible el sistema de copias, por ello la implementación es sencilla.

Figura 9. Tabla de elementos comparativos de Duplicati

Como ya detectamos en este punto, las soluciones tipo URbackup o duplicati, carecen de la madurez necesaria para un entorno empresarial, quizás sean válidos para microempresas y entornos no profesionales, pero no alcanzan a cumplir los requerimientos que un entorno profesional requiere, No obstante es justo indicar también, que la solución que propone Urbackup, es la que con el tiempo si madura, pueda alcanzar a ser competitiva en entornos más exigentes.

Por lo que para lo que este proyecto precisa, solo tendremos en cuenta Bacula en cuanto a OpenSource se refiere.

2.11. Soluciones de respaldo software propietario

2.11.1. Acronis Cyber Backup

Consiste en una solución de copia de seguridad multiplataforma compatible con servidores y máquinas virtuales Windows y Linux además de dispositivos móviles iOS y Android, Está pensada para empresas de cualquier tamaño, tanto para entornos físicos, virtuales e incluso en Cloud, permitiendo la gestión centralizada de copias de seguridad en entornos híbridos, ya que permite realizar los respaldos, tanto si los datos se encuentran localmente, en sistemas remotos, en nubes privadas o públicas. La solución garantiza una escalabilidad ilimitada, protege cualquier carga de trabajo futura. utiliza una consola de administración web diseñada para facilitar la supervisión y programación de las copias de seguridad, Realizando todas las tareas de protección de datos con una consola de copia de seguridad y recuperación multiinquilino, sin tener que conectar con los servidores locales a través de RDP, compatibilizando tanto el valor de los datos como los costes de la infraestructura.

Entre sus características más notables, es que posee un módulo de prevención contra el ransomware. Este módulo denominado *Acronis Active Protection* utiliza tecnologías basadas en IA y ML defendiendo los datos de forma proactiva contra los ataques, además de esto, identifica vulnerabilidades evaluado el riesgo de los sistemas, mitigando de esta manera las amenazas potenciales. El objetivo, en definitiva, es conseguir evitar la alteración de los archivos de respaldo.

Además del módulo anterior, utiliza una tecnología basada en Blockchain para evitar el daño o alteración de los archivos de copia, todo esto con el objetivo de reducir al máximo el RTO utilizando una tecnología llamada runVM por el desarrollador, que básicamente monta una máquina virtual a partir de la imagen de maquina original, sin importar si esta es física o virtual. De esta manera si se produce un fallo total del sistema, podemos continuar el trabajo con la maquina arrancada de manera virtual, mientras se solucionan los problemas existentes.

Para evitar consumir los recursos existentes realiza validación de copias de seguridad fuera del host y para minimizar el consumo de datos ofrece deduplicacion de múltiples niveles. Garantiza las normativas de protección de datos al utilizar tanto en tránsito como en reposo, AES-256 y permite opciones flexibles de almacenamiento de copia tanto en físico en la red local como almacenamiento listo para utilizar de Google Cloud Storage, Microsoft Azure Storage , AWS S3, etc. utilizando para esto el componente de *software Acronis Backup Gateway* ofreciendo en caso de ser necesario la opción Acronis Cloud Storage que es almacenamiento en centros de datos homologados por Acronis, compatibles con ISO 27001 y respaldan el cumplimiento de la Ley de protección de datos, firmando un acuerdo de responsabilidad comercial, para aquellos casos en que los datos, sean muy confidenciales y críticos.

ARQUITECTURA TÍPICA DE ACRONIS CYBER BACKUP:

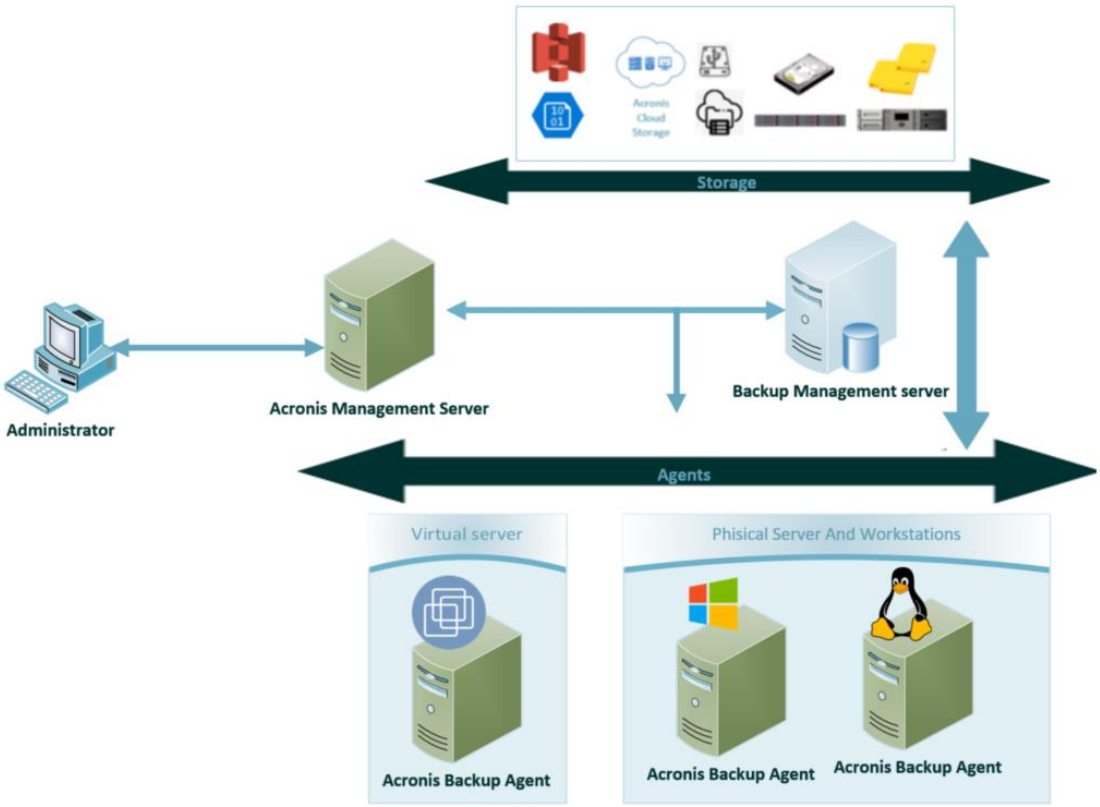

Figura 10. Arquitectura de Acronis Cyber Backup

Acronis Cyber Backup	
Capacidad de seleccionar manualmente la información	Dispone de opciones flexibles de copia de datos, permitiendo la copia de discos/volúmenes, así como la selección de archivos o carpetas específicos, permitiendo respaldar el estado del sistema y la copia de máquinas virtuales.
Capacidad de crear imagen sistema y máquinas virtuales	Como se indica en el punto anterior ofrece diversos tipos de copia y entre estos tipos, tenemos las máquinas virtuales y el sistema completo, además de permitir arrancar la maquina en virtual en caso de ser necesario runVM
Capacidad de encriptación y contraseña	Posee un sistema de cifrado de datos AES-256 tanto para los datos en tránsito como en reposo, con contraseña.
Capacidad de compresión de los archivos en el respaldo	Ofrece tecnología de deduplicacion eliminando bloques de datos duplicados, cuando se realizan copias de seguridad y se transfieren datos, además de ofrecer compresión utilizando las librerías zlib, zstd y el algoritmo de compresión de Acronis.
Capacidad de adaptación a la infraestructura pre existente	Es compatible con más de 20 plataformas diferentes desde Windows 2003 o incluso el Xp hasta Windows server 2019 o Windows 10 pasando por cualquier Linux con Kernel 2.6.9 o superior. así como todo tipo de sistemas de almacenamiento de red, aunque no admite cabinas de cinta.
Capacidad de realizar informes y notificaciones por correo	Permite la notificación del estado de la copia por correo, ofreciendo todo tipo de informes y estadísticas en la consola central de tipo web.
Capacidad de certidumbre	Su herramienta de prevención antimalware, le da un extra de protección a los datos respaldados, a esto hay que sumarle la capacidad de realizar tareas de verificación periódicas.
Capacidad de adaptación, facilidad de configuración	Al ser un software con arquitectura multinivel y multiinquilino en la nube ofrece una capacidad de adaptación fuera de lo común. Por otro lado, Acronis a diseñado este producto con la mayor simplicidad posible, para facilitar las tareas de mantenimiento y supervisión de las copias.

Figura 11. Tabla de elementos comparativos de Acronis Cyber Backup

2.11.2. Commvault Backup & Recovery

Commvault Backup and Recovery es una plataforma unificada y centralizada para la protección mediante archivos de respaldo, con carga de trabajo tanto local como en la nube. entre sus capacidades, tenemos el respaldo de datos, generación de instantáneas, replicación, archivado, migración y protección de en la nube permitiendo a su vez la recuperación granular, utilizando para ello una indización que le permite realizar búsquedas dentro del contenido respaldado, ofreciendo de esta manera una solución con capacidad de recuperación de desastres a nivel granular monitorizada y auditada mediante informes de re.

A nivel de Arquitectura, existen tres componentes principales que son:

- CommServe (CS), proporciona control y monitoreo de una implementación de respaldo y recuperación completa de Commvault.
- MediaAgents (MA), responsables de mover datos del origen a los distintos repositorios
- Intelligent Data Agents (iDA), interactúan con hipervisores, sistemas operativos y aplicaciones para proporcionar protección granular, recuperación y deduplicacion del lado de la fuente.

Indicar que además de estos tres componentes, tiene subcomponentes, como son librerías (que serían los repositorios e incluyen desde cabinas de discos hasta el storage Cloud) y los clientes que son los equipos de los que se desea el respaldo, debiendo de contar con el Virtual Server Agent (VSA), que aunque se trata de un agente como los IDA, realmente se le tiene una consideración especial, puesto que es utilizado para interactuar con vCenter de VMware dando de esta manera capacidades especiales para el respaldo de las máquinas virtuales.

Como solución de copias de seguridad, ofrece capacidad de realizar backups tanto de máquinas físicas como virtuales soportando multitud de hipervisores como: VMware, Nutanix, Hyper-V. A través de agentes, es capaz de realizar copias de seguridad de todo tipo de aplicaciones como: Oracle, SAP, Exchange, SQL, etc. Posee tecnologías avanzadas de deduplicacion y gestión cuya finalidad es reducir la cantidad de datos que se almacenan en el destino de Backup. Permite montar diferentes entornos de test, donde realizar pruebas sin afectar a la produccion. Incorporando la capacidad de utilizar flujos de trabajo cuya finalidad es automatizar todo tipo de acciones relacionadas con el entorno de Backup.

Permitiendo el cifrado extremo a extremo tanto para los datos en tránsito como en reposo, con descubrimiento automático de los conjuntos de datos recién agregados, con políticas de retención y procesos de instantáneas automatizado, con una interfaz de usuario en web, optimizado para los sistemas híbridos o directamente Cloud, con deduplicacion, así como cobertura de respaldo de datos para sistemas de archivos, aplicaciones, bases de datos, VM, contenedores, SaaS Cloud nativo y endpoints.

ARQUITECTURA TÍPICA COMMVAULT BACKUP & RECOVERY:

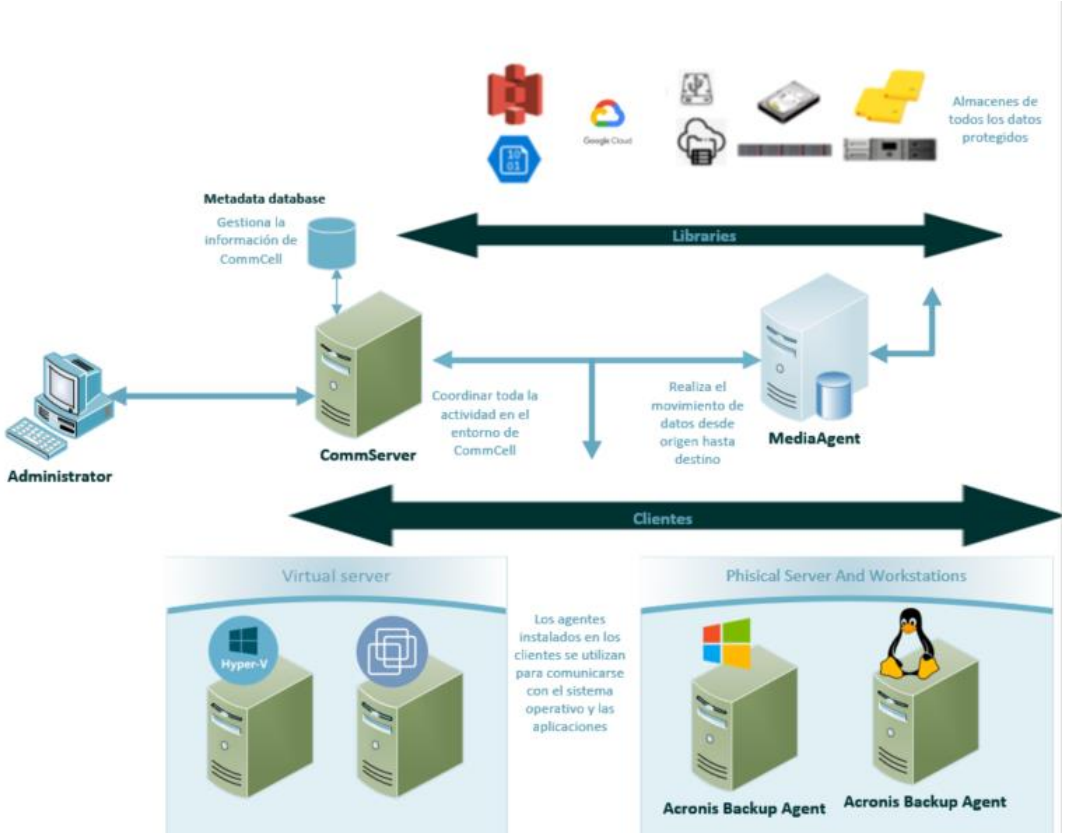

Figura 12. Arquitectura de Commvault Backup & Recovery

Commvault Backup & Recovery	
Capacidad de seleccionar manualmente la información	Recuperación y backup de todo el sistema, instancia, aplicación o archivo único granular, con lo que si tiene esta capacidad.
Capacidad de crear imagen sistema y máquinas virtuales	Como se indica en el punto anterior, permite realizar backups del sistema entero, así como VM's, con lo que si disponemos de esta capacidad.
Capacidad de encriptación y contraseña	Commvault genera una clave aleatoria diferente de 128 o 256 para cada fragmento de datos que escribe. Cada trabajo puede contener varios fragmentos, por lo que cada trabajo de respaldo puede tener varias claves generadas aleatoriamente. de esta manera se alcanza una fuerza de cifrado muy elevada
Capacidad de compresión de los archivos en el respaldo	Utiliza tanto la librería de compresión LZO como GZIP, siendo esta ultima la predeterminada, con lo que si cumple con este requerimiento. Además de esto utiliza un sistema de deduplicacion multinivel, muy eficiente.
Capacidad de adaptación a la infraestructura pre existente	Acepta múltiples arquitecturas como infraestructuras, aceptado desde la virtualización VMware, hyper-V, Citrix Xen, Oracle Vm, todo tipo de plataformas de almacenamientos, desde cabinas de discos hasta cabinas de cintas, como almacenamiento Cloud basado en objetos, es compatible con sistemas de tipo Unix (linux, Bsd,etc) así como sistemas Windows, con lo que si cumple con este requerimiento.
Capacidad de realizar informes y notificaciones por correo	Con notificación por correo de estado, además de un todo tipo de reportes que nos muestran la salud de la infraestructura de copias, así como un resumen al final de la copia/restauración que nos aporta información del rendimiento de la misma, con todo esto podemos afirmar que cumple con esta característica.
Capacidad de certidumbre	Como permite la realización de verificaciones de integridad periódicas para comprobar el estado de los archivos de recuperación, generando una solución de Backup confiable y robusta.
Capacidad de adaptación, facilidad de configuración	Al encontrarnos con un sistema multiplataforma, con habilidad de integración con casi todos los sistemas Enterprise orientado al Cloud, permite adaptarse con facilidad, por otro lado, se trata de una solución compleja en lo que a la administración se refiere.

Figura 13. Tabla de elementos comparativos de Commvault Backup & Recovery

2.11.3. Veeam Backup

Veeam Backup, es una solución multiplataforma flexible e integral que proporciona una capacidad de recuperación de alta velocidad, que combina las réplicas y snapshots, con el objetivo de reducir el RTO a menos de 15 minutos permite la realización de copias de seguridad de sistemas tanto físicos como virtuales, de tal manera que en un momento de necesidad se puedan recuperar en un entorno virtual para poner en productivo el sistema con la mayor celeridad posible apoyándose en una tecnología denominada Instan Recovera que como se ha indicado permite recuperar cualquier imagen, en entorno Vmware o en hyper-v además de esto permite recuperar así como a nivel de archivo lanzando un browser que no es más que el árbol de directorios de los volúmenes de la imagen realizada. Dispone asimismo verificación automatizada configurada de tal manera que verifica la integridad de las copias con la periodicidad marca, por otro lado dispone de recuperación de bbdds, al permitir un sistema de respaldo completo de objetos como Exchange, SharePoint, active directory y SQL, tiene la capacidad de recuperar directamente el objeto utilizando un sistema de búsqueda granular es decir, que permite recuperar un correo en el caso de Exchange, un documento en SharePoint, un usuario o pc en Active directory, etc.

Provee de un entorno de copia de seguridad, tanto para infraestructuras onpremise, como para sistemas Cloud como para sistemas híbridos, siendo compatible al mismo nivel en entornos físicos y en entornos virtuales ofreciendo conjuntamente una protección adicional contra el ransomware al permitir realizar Backup inmutables por un lado y en el caso de utilizar la nube de AWS se apoya en el bloqueo de objetos de S3, brindando una consistencia mayor a laos ficheros de copia, de esta manera, añadiendo un sistema potente de cifrado se garantiza que se cumplen los requisitos de seguridad de los datos, ya sea a nivel normativo como de privacidad exigidos por la ley de protección de datos.

En la última versión permite realizar respaldos directamente de archivos disponibles en red sin la instalación de agentes, de esta manera puede realizar copias de fichero accediendo mediante NFS o SMB con lo que aquellos sistemas incompatibles debido a su antigüedad o simplemente incompatibles por su propósito o funcionalidad, puedan llegar a tener un respaldo de los datos continentes en las carpetas compartidas. Es compatible con múltiples Cloud como son AWS, Azure y Google Cloud permitiendo realizar copias de la propia infraestructura de estas redes Cloud, así como migrar los sistemas locales a estas nubes Cloud para arrancarlas desde ahí, para ir poco a poco a un sistema Hibrido y terminar en un sistema deslocalizado en Cloud.

Otra de sus características más reseñables es un sistema de duplicación muy eficiente que incorpora una tecnología de seguimiento de bloques modificado para aumentar la velocidad y eficiencia de los backups incrementales, intentando reducir la ventana de Backup lo máximo posible. Como podemos observar de acuerdo con lo anteriormente mencionado entre los objetivos de este software esta reducir tanto el RTO, RPO y la Ventana Backup.

Este software ofrece un novedoso sistema denominado Reverse Incremental Backup aparte del ya tradicional copia de seguridad incremental, este sistema lo que realiza es un sistema de respaldo completo en el repositorio para después en los siguientes trabajos “inyectar” los bloques de datos que han cambiado desde la última copia de seguridad mientras los datos que son reemplazados se almacenan en un archivo incremental inverso, de esta manera siempre tendremos una copia full con el estado más reciente y varios incrementales inversos con los estados anteriores, la ventaja de este sistema de copia es la drástica reducción del RTO.

En caso de ser necesario y con la intención de reducir la infraestructura física, ofrece servicios de BasS (Backup as a Service) y DRaaS (Disaster Recovery as a Service) para poder gestionar y realizar todo el trabajo de Backup de manera totalmente deslocalizada.

ARQUITECTURA TÍPICA VEEAM BACKUP:

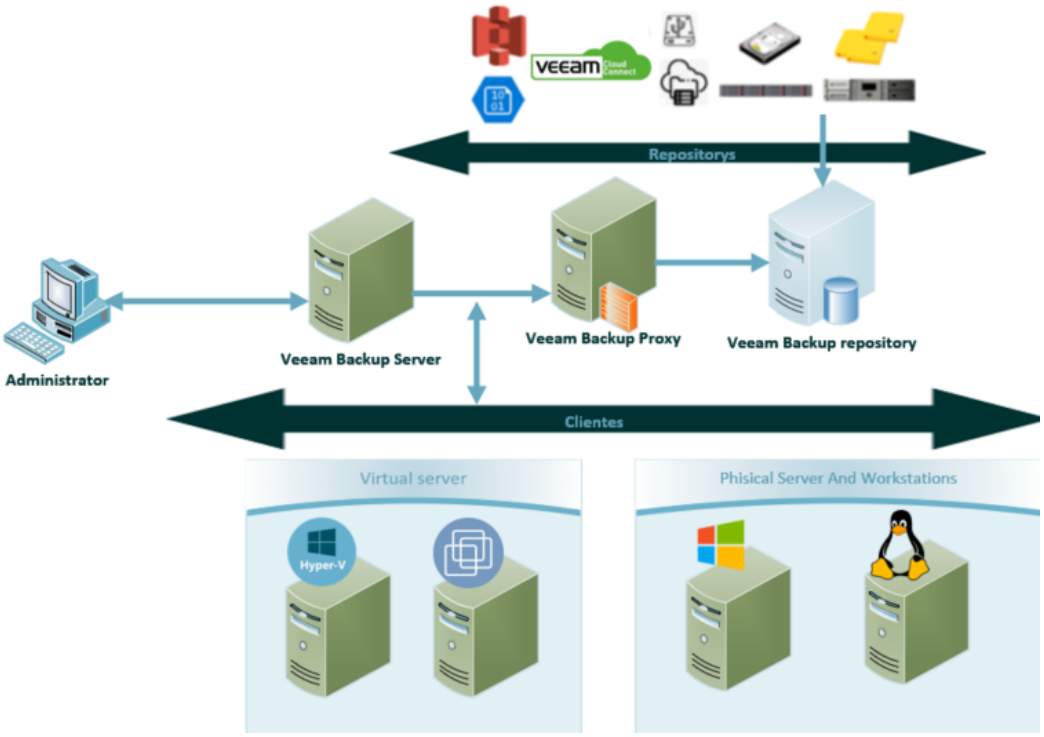

Figura 14. Arquitectura de Veeam Backup

Veeam Backup	
Capacidad de seleccionar manualmente la información	Entre las múltiples opciones de copia, dispone de capacidad de selección de ficheros, de Backup de volumen, así como de la maquina entera, incluso puede hacer Backup de distintas ubicaciones de red sin agentes, luego si dispone de esta capacidad.
Capacidad de crear copias del sistema operativo entero y máquinas virtuales	Como se ha indicado en el punto anterior, si se puede realizar copia del sistema completo, también realiza copia de las máquinas virtuales, permitiendo incluso migración o arranque puntual de máquinas físicas a Backup mediante el archivo Backup.
Capacidad de encriptación con contraseña para acceder a la información	Cada archivo de Backup de Veeam se cifra por una clave de encriptación generada aleatoriamente, Cada Backup cifrado de Backup posee dos contraseñas. Una es definida en el Job de Backup y es generada por el administrador y por otro lado se genera una clave pública automáticamente que se distribuye a todos los servidores de Backup en segundo plano, utilizando AES 256 a nivel de encriptación
Capacidad de compresión de los archivos en el respaldo	Hace uso de compresión y deduplicacion de datos para disminuir el tráfico de red y el espacio de almacenamiento requerido, con lo que si dispone de esta característica.
Capacidad de adaptación a la infraestructura pre existente	Es compatible con Microsoft Windows, Linux, Mac, IBM AIX, Oracle Solaris en físico, VMware vSphere, Microsoft, Hyper-V y Nutanix AHV en virtual en Cloud AWS, Microsoft Azure y Google Cloud Platform, con capacidad de realizar backups directamente sobre recursos compartidos, con lo que es adaptable casi a cualquier infraestructura.
Capacidad de realizar informes y notificaciones por correo	Tiene un dashboard muy potente que analiza la eficiencia de la protección de datos además de analizar permitiendo enviar estos reportes por correo periódicamente, en conjunto a la notificación el estado del Backup de cada trabajo realizado
Capacidad de certidumbre	Posee un sistema con capacidad de hacer verificaciones periódicas, de tal manera que, si el Backup se realizó correctamente, el respaldo no se ha corrompido, otro modulo muy interesante a este repuesto, es que tiene un sistema de Backup inmutables para detectar cualquier modificación en los archivos de copia, que le protegen tanto del ransomware como de la corrupción de ficheros.
Capacidad de adaptación, facilidad de configuración	Uno de sus puntos fuertes es precisamente esto, tiene una facilidad de configuración elevada, gestionando todo desde el servidor hacia los clientes sin archivos de configuración.

Figura 15.Tabla de elementos comparativos de Veeam Backup

Al comparar cual quiera de las soluciones que ofrece el software propietario entre sí, en cuanto a parámetros de: Calidad, Escalabilidad, Redundancia, Exhaustividad de la documentación, Compatibilidad con otras herramientas, capacidad Encriptación, etc...

Vemos que todas las soluciones están muy parejas, si incluimos Bacula en esta lista al estar al mismo nivel en cuanto a cantidad, nos vemos con la necesidad de para poder tomar decisiones que eliminen candidatos, debemos centrarnos en los costes de licenciamiento.

2.12. Análisis de licenciamiento

Como hemos indicado a la hora de seleccionar un software u otro, debemos analizar los costes de licenciamiento o costes de suscripción, para este punto, no vamos a incluir los costes de infraestructura, en este punto ya que se abordará en un apartado posterior y tomaremos como premisa inicial que el coste será idéntico para todas las soluciones analizadas, por simplificar la casuística.

Tampoco vamos a añadir coste de instalación y puesta en marcha en un principio, se presupone una situación ideal en el que las horas de instalación, parametrización y puesta en marcha son iguales para todas las soluciones. Aunque esto no es para nada real ya que cada solución tiene una curva de aprendizaje y una dificultad inherente de cada una en este proceso.

Por último, tampoco vamos a analizar los costes en Cloud, puesto que este punto es común para todas las soluciones y se abordara en un punto concreto en el cual se analizarán los servicios y costes específicos de cada Cloud

Procedemos pues a analizar suscripción y licenciamiento

Existen principalmente dos modelos de licenciamiento:

- Licenciamiento Perpetuo: En este modelo se realiza la compra la licencia de uso de una versión particular de software, pagando el valor completo de dicha licencia. En la mayoría de los casos es necesario adquirir un contrato de soporte para tener acceso a correcciones o parches para resolver problemas técnicos o solucionar vulnerabilidades de seguridad
- Suscripciones de software: En este modelo se paga de manera recurrente por la licencia de uso del software. El pago de la suscripción contiene el acceso a la última versión del software incluyendo correcciones a vulnerabilidades de seguridad y normalmente incluye también el acceso a soporte técnico.

Si analizamos el caso de Bacula, existe un modelo Community y un modelo Empresarial, para este punto nos centraremos en la versión Enterprise, por los servicios de valor añadido que ofrece, como pueden ser como la certificación de binarios, las opciones de soporte 24/7, Asistencia remota, etc. Dentro de esta versión, nos hemos encontrado un modelo de suscripción de 1 año con las siguientes características y precios:

	Estándar	Bronce	Plata	Oro	Platino
Bacula Enterprise Edition (1 director)	6.370 €	€ 10,76	37.120 €	80 915 €	171.550 €
Número de máquinas	11 hasta 50	51 - 200	201 - 500	501 - 2000	2.001 - 5.000
Número de contactos autorizados	1	2	3	5	5
Soporte de acceso de asistencia técnica	Web	Web	Tel y Web	Tel y Web	Tel y Web
Número de plataformas del sistema	4	todas	todas	todas	todas
Prioridad incidentes 'Severidad 1'	1	6	4	1	1
Deduplicacion global de terminales	NO	NO	Si	Si	Si
Formato de volumen alineado empresarial	NO	NO	Si	Si	Si
Complemento de Kubernetes de	NO	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de Docker de	NO	4.240 €	4.240 €	4.240 €	4.240 €
Complemento Amazon Glacier	NO	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de interfaz de Oracle Cloud	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de interfaz de Google Cloud	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €

Complemento de interfaz de Azure Cloud	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de interfaz Cloud S3	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento SAP Hana	23.760 €	23.760 €	23.760 €	23.760 €	23.760 €
Complemento SAP de	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de servidor de directorio	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento DB2	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento Sybase (ASE)	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento MySQL	4.240 €	4.240 €	4.240	4.240 €	4.240 €
Complemento PostgreSQL de	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de Oracle de	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento Incremental Accelarator para Netapp	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento Swift OpenStack	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de virtualización Red Hat	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento Proxmox	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento XenServer	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento KVM de	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de Hyper-V de	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento de VMware empresarial de Bacula	NO	4.240 €	4.240 €	4.240 €	4.240 €
Complemento Delta	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento SAN	NO	NO	4.240 €	4.240 €	4.240 €
Complemento Bare Metal Recovery para Linux	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento Bare Metal Recovery para Windows	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento VSS File Daemon	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento para MS SQL Server	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
Complemento NDMP de	4.240 €	4.240 €	4.240 €	4.240 €	4.240 €
BWeb Management Suite	3.430 €	3.430 €	3.430 €	3.430 €	3.430 €
Servicio BCloud	3.430 €	3.430 €	3.430 €	3.430 €	3.430 €

Figura 16. Tabla de coste licenciamiento Bacula Enterprise

Después de ver el caso de Bacula, Nos centramos en el modelo de licenciamiento de Acronis Cyber Backup que tiene dos versiones, la Standard Edition y la Advanced Edition, se adjunta tabla comparativa, indicando coste anual en función del dispositivo a respaldar.

	Standard	Advanced
Server	349 €	539 €
Workstation	55 €	75 €
Virtual Host	409 €	729 €
Windows Server Essentials	199 €	
Office 365	89 €	99 €
G Suite	89 €	
Tecnología de creación de imágenes de disco patentada	Si	Si
Almacenamiento: discos, NAS, SAN, Acronis Cloud Storage	Si	Si
Consola de gestión web táctil centralizada y remota	Si	Si
Paneles personalizables	Si	Si
Acronis Active Protection	Si	Si
Copia de seguridad compatible con la aplicación	Si	Si
Deduplicacion del almacenamiento en disco centralizado	No	Si
Compatibilidad con unidades de cinta, cargadores automáticos y bibliotecas	No	Si
Gestión de grupos basada en directivas	No	Si

Acceso administrativo basado en funciones	No	Si
Acronis Notary	No	Si
Informes avanzados	No	Si
Operaciones de administración de copia de seguridad fuera del host	No	Si

Figura 17. Tabla de coste licenciamiento Acronis Cyber Backup

Seguimos con la información que nos facilita Commvault, que ofrece dos modelos de licenciamiento el licenciamiento perpetuo y el licenciamiento de suscripción, dentro de esta modalidad existen diferencias en cuanto periodicidad de 1,2 o 3 años y de volumen 1Tb o 2Tb, por instancias, por usuario, etc... Puesto que vamos a realizar una comparativa de precios y en los anteriores hemos seleccionado 1 año de licenciamiento por suscripción, vamos a centrarnos en 1 año hasta 1 TB que es la opción que más se asemeja a las presupuestadas en las anteriores opciones:

CommVault Backup & Recovery for Virtual Machines (10 VM)		
CV-BKRC-VM10-11	104 €	1 front end TB
CommVault Backup & Recovery For Non-Virtual and File		
CV-BKRC-FT-11	157 €	1 front end TB

Figura 18. Tabla de coste licenciamiento CommVault Backup & Recovery

Por último, en el caso del Veeam Backup, aunque posee licenciamiento perpetuo, nos encontramos que ofrece un modo de licenciamiento denominado Veeam Backup Essentials Universal, que se agrupa en pack de 5 instancias, estas instancias no tienen en consideración si es un entorno server, si es físico o virtual, es un licenciamiento mucho mas equilibrado que todos los anteriores.

Veeam Backup Essentials Universal		
V-ESSVUL-0I-SU1YP-00	348 €	5 Instancias
	69,6 €	1 instancia

Figura 19. Tabla de coste licenciamiento Veeam Backup

Analizando los precios de las 4 soluciones vemos que en Bacula tenemos la opción en principio con un precio más elevado, aunque si bien es cierto, podemos optar por la Community que no tiene coste de licenciamiento, en contraposición tendrá un coste en mayor en cuanto a horas de implantación, parametrización y puesta en marcha.

Si los equipos a respaldar son solo estaciones de trabajo o Workstation, la solución más económica seria Acronis, con un precio de 55€ al año por máquina, en el caso de incluir un servidor o un host Virtual, el precio se eleva con la que consecuencia de quedarse fuera de precio al existir soluciones más económicas, por ejemplo aunque la licencia de Host virtual (VSphere - Hyper-V) de Acronis tiene un coste de 409€ año con ilimitados equipos, la opción que ofrece Commvault de 10 equipos virtuales por 104€ al año es más competitiva simplemente con tres licencias de este tipo, seguiría siendo más económica (312€) y permitiría dar solución a 30 equipos virtuales independientemente del host, esta solución es particularmente ventajosa si nuestra infraestructura es completamente virtual, puesto que el coste por máquina virtual de 10,4€ al año. Mas económico que la opción Veeam, cuya oferta recibida es de 348€ por 5 instancias/año, es decir que el precio por instancia será 69.6€ al año independientemente de si esta es virtual, Workstation o servidor. Esta solución es la más indicada si nuestra infraestructura es mixta, es decir tenemos como mínimo dos servidores físicos, varias instancias virtuales, ya que el precio se mantiene constante no como en Commvault que el coste de servidor no virtual asciende a 157€

En Resumen, en función de la arquitectura de hardware y las infraestructuras, nos decantaremos por una solución u otra. siendo Veeam la solución más equilibrada, Acronis ideal para equipos de trabajo en exclusiva y Commvault si la infraestructura es completamente virtual, aunque esto es bastante difícil puesto que en la mayoría de las organizaciones suelen estar provistas de un entorno hibrido, razón por la que en la mayor parte de las ocasiones con los precios actuales, nos decantaremos por Veeam.

2.13. Análisis de costes infraestructura Cloud

De la misma manera que hemos analizado los diferentes precios de licenciamiento, vamos a analizar los diferentes costes del Cloud, según tecnología y de acuerdo al Cloud que utilicemos, actualmente han surgidos dos enfoques diferentes en cuanto al servicio que puede proporcionar un Cloud estos son:

2.13.1. Backup as a Service (BaaS)

Es un servicio, que permite a las organizaciones, realizar copias de seguridad de archivos, carpetas y repositorios de datos completos en un centro de datos seguro offsite

BaaS normalmente es gestionado por un proveedor de servicios administrados (MSP) de terceros, lo que en la práctica se traduce en que la administración, mantenimiento y almacenamiento de las copias de seguridad son responsabilidad del MSP en lugar del departamento de IT.

Entre las muchas ventajas que ofrece este servicio tenemos:

- La seguridad. Debido a que sus datos se almacenan en BaaS, no está sujeto a las amenazas típicas de piratas informáticos, desastres naturales y errores de usuario, normalmente los datos que se almacenan en BaaS están encriptados, lo que minimiza los riesgos en los que pueden incurrir sus datos.
- Conveniencia. BaaS es automático: una vez que se configura, la información se guarda automáticamente a medida que ingresa. No es necesario que guarde, etiquete y realice un seguimiento de la información de manera proactiva.
- Facilidad de recuperación. Debido a los múltiples niveles de redundancia, si los datos se pierden o eliminan (con mayor frecuencia debido a un error o eliminación de un usuario individual), las copias de seguridad están disponibles y se localizan fácilmente.

2.13.2. Disaster Recovery as a Service (DRaaS)

La recuperación ante desastres como servicio (DRaaS) es un modelo de servicio de computación en la nube que permite a una organización realizar copias de seguridad de sus datos e infraestructura de TI en un entorno en un Cloud de terceros y proporcionar toda la gestión de recuperación del desataste, todo a través de una solución SaaS, para recuperar el acceso y funcionalidad a la infraestructura de TI después de un desastre. El modelo como servicio significa que la organización en sí misma no tiene que poseer todos los recursos o manejar toda la administración para la recuperación de desastres, sino que depende del proveedor de servicios. para ser funcional, esta tecnología debe reflejar la infraestructura completa en modo a prueba de fallos en servidores virtuales alojados en el cloud proveedor, esto permite a la organización en caso de desastre reducir el RTO al poseer una redundancia deslocalizada.

Existen tres modelos de DRaaS principalmente

- Managed DRaaS en un modelo de DRaaS administrado, un tercero asume toda la responsabilidad de la recuperación ante desastres. La elección de esta opción requiere que una organización se mantenga en estrecho contacto con su proveedor de DRaaS para asegurarse de que se mantiene actualizado sobre todos los cambios de infraestructura,
- Assisted DRaaS el proveedor de servicios ofrece su experiencia para optimizar los procedimientos de recuperación ante desastres, pero el personal de la organización es responsable de implementar parte o la totalidad del plan de recuperación ante desastres, esta opción es recomendable, si se dispone de aplicaciones únicas o personalizadas que podrían ser un desafío para que un tercero se haga cargo.
- Self-service DRaaS esta es la opción más económica, aunque la organización en última instancia es la responsable de la planificación, realización de pruebas y la gestión de la recuperación ante desastres, al ser un servicio sin asistencia, se requiere personal experimentado en recuperación de datos.

2.13.3. Ejemplo: Veeam Backup Servicios Cloud

Como vimos en el punto anterior, la solución más equilibrada y económica bajo el contexto de todo tipo de arquitectura, que es lo más habitual em cualquier organización, es Veeam Backup, por eso vamos a centraremos esta solución y lo que ofrece en cuanto a tecnología Cloud, aunque podríamos reemplazar este software por cualquier otro ya que todos los analizados tienen capacidades similares en cuanto a Cloud

Veeam Backup ofrece 3 servicios cloud

- Dos de ellos mediante proveedores certificados VCSP o Veeam Certified Service Providers
  - Backup como servicio (BaaS):
    Veeam ofrece este servicio mediante VCSP que utilizando un servicio denominado Cloud Connect realiza a conexión segura encriptada por SSL mediante el componente de Cloud Gateway, que permite conectar el espacio que nos facilita el proveedor con el servidor de Veeam Backup local y configurar en él, los trabajos como si se tratara de un repositorio local de manera transparente. la única diferencia con respecto a un repositorio local es que la copia no está físicamente en la red local, es offsite y es el proveedor de servicio quien se encargara de la custodia y la retención, un valor añadido que ofrecen, insider protection, que evita la eliminación, accidental o no, de cualquiera de sus respaldos por un tiempo, dando una protección adicional en caso de que la seguridad del sistema se vea comprometida.

  - Recuperación ante desastres como servicio (DRaaS)
    En este caso, igual que en el anterior, Veeam, ofrece este servicio mediante los mismos VCSP que para el servicio BaaS, a nivel arquitectura se utilizará además un *Tenant Backup server* y en lugar de tener una imagen comprimida, poseerá una copia tal cual, es decir mantendrá una réplica de la infraestructura a salvaguardar clonando completamente las VM y sincronizando los cambios incrementalmente cada cierto tiempo. para aliviar el consumo de disco, existe la posibilidad de aprisionar los disco en thin, que consiste en un disco virtual que consume solo el espacio que necesita inicialmente y crece con el tiempo según la demanda.

los VCSP se encargan de proporcionar los hosts VMware o HyperV, a los que dotaran de cierta cantidad de CPU, memoria y disco, para realizar sus réplicas en forma rápida y segura.

Si comparamos uno y otro, podemos deducir que la opción de DRaaS tiene más sentido cuando hay algún imperativo de requerimientos de recuperación muy agresivos en cuando a continuidad del negocio ya que RPO que usualmente se asocian con DRaaS son más agresivos, pueden llegar a ser del orden de minutos, obviamente para mantener este servicio, se debe sacrificar espacio de disco en el Cloud y mayor ancho de banda ya que la réplica no se comprimen ni se deduplican los datos, además, el DRaaS al necesita consumir CPU y memoria con lo cual va tener una tarificación mayor.

Hay que indicar que los proveedores VCSP ofrecen la posibilidad de restaurar las copias realizadas con BaaS en su propia infraestructura, en un RTO mayor que utilizando sistema DRaaS, pero un RTO menor que descargándolo a nuestra infraestructura y a un coste menor que el DRaaS en caso de necesidad.

Adjuntamos precio del Servicio BaaS, en un VCSP, indicamos el capacidad de 2Tb, para establecer un real que nos sirva de referencia a la hora de evaluar el resto de los servicios de almacenamiento en Cloud.

Cloud Connect de Veeam			
	Cantidad	Importe mensual	Total
Equipos virtuales	1	6 €	6,00 €
Equipos Físicos	1	8 €	8,00 €
Espacio (Tb)	2	100 €	200,00 €
TOTAL			214,00 €

Figura 20. Tabla de coste del Cloud Connect de Veeam

**Los costes de equipo físico y virtual vienen determinado por las licencias que factura Veeam

- El tercer servicio que ofrece es el de extender los repositorios locales haciendo el uso del *Capacity Tier* tecnología que tiene la capacidad de utilizar almacenamiento orientado a objetos como Blob de Microsoft o S3 de Amazon, esta tercera vía es la más económica de todas las opciones, ya que solo tiene el coste de almacenamiento orientado a objetos en dichas nubes, mucho más económicas que las opciones de BaaS. La manera de utilizar esta vía puede ser llevar cierto histórico de copias al repositorio orientado a objetos o llevar la copia al repositorio de objetos en el momento se realice la copia, de tal manera que poseeremos una copia local que será idéntica a la copia en Cloud, a la hora de restaurar, la copia Cloud se realiza como si la copia es local.

2.13.4. Proveedores Cloud

Vamos a analizar varios proveedores de servicios cloud y como estos interaccionan con las soluciones que propone Veeam:

- IBM Cloud
  - BaaS

    IBM ofrece un completo servicio de Backup as server, permitiendo asimismo extender y migrar rápidamente IaaS dedicado y alojado dentro de IBM Cloud.

- DRaaS

  La solución propuesta por IBM es encargarse de la gestión de la infraestructura hasta el hipervisor, incluidas las responsabilidades de copia y replicación, además de incluir soporte para upgrades, parches en el sistema Backup en nombre del cliente.

- Repositorio basado en objetos

  Permite almacenamiento en cintas virtuales VTL en conjunto con el IBM Cloud Object Storage, que se utiliza un sistema de almacenamiento de objetos en la nube.

- Microsoft Azure
  - BaaS

    Azure ofrece un sistema BaaS, Al ofrecer Cloud Connect dentro de los SaaS que ofrece en su Marketplace, lo cual dota al sistema Backup de la capacidad de gestionar y traslada de forma eficiente las copias de seguridad de Veeam a los repositorios de Azure.

  - Repositorio basado en objetos

    Utilizado las capacidades de Cloud Tier permite integración nativa en Microsoft Azure Blob.

  - Portabilidad a Cloud

    Podemos Utilizar un repositorio de Veeam y restaurarlo y ponerlo en marcha en el cloud de Azure, razón por la que ofrece también DRaaS.

  - Backup IaaS y SaaS

    Por último, se dispone de la capacidad de realizar copias de los documentos de SharePoint online, así como del Exchange incluyendo la infraestructura desplegada en el cloud, permitiendo superar cualquier interrupción en cuestión de minutos.

- AWS De Amazon
  - Repositorio basado en objetos

    Utiliza Amazon S3 para obtener una capacidad ilimitada de retención de datos a largo plazo al mismo tiempo que ofrece soporte de Virtual Tape Library (VTL).

  - Portabilidad a Cloud

    Podemos Utilizar un repositorio de Veeam y restaurarlo y ponerlo en marcha en el cloud de AWS EC2, razón por la que ofrece también DRaaS, además de ofrecer migración a EC2.

  - Backup IaaS y SaaS

    Por último, se dispone de la capacidad de realizar copias de los documentos de SharePoint online, así como del Exchange de 365 como objeto en S3, permitiendo además realizar respaldos de la infraestructura desplegada en el cloud EC2.

Tanto en el caso de IBM Cloud, como de Amazon, ofrecen soporte de VTL (virtual tape library), esta es una tecnología de virtualización de almacenamiento de datos que se utiliza normalmente con fines de copia de seguridad y recuperación, simulando o virtualizando unidades de cinta o bibliotecas de cinta, lo que permite una mejor consolidación del almacenamiento, así como proceso de restauración más rápidos.

Ejemplo precios mensuales De VTL Amazon

- Respaldo

	Datos escritos por GW	S3	S3 Glacier	cintas eliminados anticipadamente	Importe
Datos en (TB)	1	0	2	1	20,52
Datos en (TB)	1	2	0	0	51,51

Figura 21. Tabla coste VTL Amazon

- Recuperación

	Transferencia de datos	S3	S3 Glacier	Importe
Datos en (TB)	2	0	2	52,38
Datos en (TB)	2	2	0	52,38

Figura 22. Tabla comparativa coste S3 y S3Glacier

En contra posición. sí utilizamos la tecnología Veeam Cloud Connect para la empresa en Azure, dependiendo de la máquina que Utilizamos y del tiempo que este encendida tendrá un coste u otro:

Plan de precios Azure Veeam Cloud Connect

Tipo	Categoría	Núcleos	RAM	Espacio	importe/hora	Importe/mes
A4	Estándar	8	14 GB	605 GB	0,405 €	303,75 €
A3	Estándar	4	7GB	285 GB	0,202 €	151,50 €
A2	Estándar	2	3,5 GB	135 GB	0,101 €	75,75 €

Figura 23.Plan de precios Azure Veeam Cloud Connect

Ahora ya solo nos queda analizar los precios de varios proveedores de almacenamiento orientado a objetos IBM Cloud, Azure y AWS:

	Amazon S3 Glacier	Amazon S3	IBM Cloud Object Storage	Azure Storage Blop
Región	Europa (Fráncfort)	Europa (Fráncfort)	eu-de	LRS West Europe
Precio (GB)	0,00380 €	0,02100 €	0,01110 €	0,00844 €
Operaciones de escritura (1k)	N/A	N/A	0,00840 €	0,08440 €
Solicitudes PUT, COPY, LIST (1k)	0,03100 €	0,00460 €	N/A	0,04560 €
Solicitudes GET, SELECT (1k)	0,00036 €	0,00360 €	0,00840 €	0,00850 €
Solicitudes de transición ttl (1k)	0,03100 €	N/A	N/A	
Recuperaciones de datos por GB	0,01000 €	0,03100 €	0,00840 €	0,00850 €
Índice de blob	N/A	N/A	N/A	0,02530 €
Ámbito de cifrado	N/A	N/A	N/A	1,09630 €
Ancho de banda de salida público	N/A	N/A	0,07590 €	

Figura 24.Tabla Comparativa diferentes proveedores cloud

Para realizar una comparativa más eficaz, establecemos una capacidad de almacenamiento para todas las opciones de 2 TB con lo que tenemos el siguiente cuadro

	Amazon S3 Glacier	Amazon S3	IBM Cloud Object Storage	Azure Storage Blop
Precio (2TB)	7,7824	43,008	22,7328	17,28512
Operaciones de escritura (1k)			0,00840 €	0,08440 €
Solicitudes PUT, COPY, LIST (1k)	0,03100 €	0,00460 €		0,04560 €
Solicitudes GET, SELECT (1k)	0,00036 €	0,00360 €	0,00840 €	0,00850 €
Solicitudes de transición ttl (1k)	0,06200 €			
Recuperaciones de datos por GB	20,48000 €	63,48800 €	17,20320 €	17,40800 €
Índice de blob				0,02530 €
Ámbito de cifrado				1,09630 €
Ancho de banda de salida público			155,4432 €	

Figura 25. Tabla comparativa proveedores Cloud con las mismas condiciones.

Con lo que si agrupamos importes en almacenamiento tenemos:

	Amazon S3 Glacier	Amazon S3	IBM Cloud Object Storage	Azure Storage Blop
Precio Almacenamiento	7,81€	43,01€	22,74€	17,42€
	Amazon S3 Glacier	Amazon S3	IBM Cloud Object Storage	Azure Storage Blop
Recuperación	20,54€	63,49€	172,65€	18,54€

Figura 26.Tabla comparativa proveedores cloud gastos agrupados.

Ya tenemos toda la información necesaria para evaluar los diferentes proveedor de Cloud, obviamente hay muchos proveedores de Cloud, pero nos hemos centrado en los más populares actualmente. Como podemos observar existen varios servicios que podemos utilizar en cloud, en función de la utilización de recursos, pagaremos más o menos importe, si utilizamos un VCSP debemos pagar tanto el licenciamiento por equipo almacenado, como el espacio en disco almacenado, si además utilizamos un sistema DRaaS, a lo anterior deberemos añadir el coste de mantener de la réplica de la infraestructura y si escogemos la opción de VTL a los costes deberemos añadir los costes de almacenamiento de objetos y en definitiva la elección más económica, es utilizar simplemente almacenamiento de objetos, con encriptación y con el respaldo encriptado. de esta tecnología la más económica, será S3 Glacier. No obstante, puede suceder que el servicio que ofrece no sea suficiente debido a la criticidad de los datos, así como la necesidad de disminuir el RTO al mínimo, en cuyo caso en función del tiempo máximo que podamos permitirnos de RTO escogeremos un servicio BaaS o un servicio DRaaS.

2.14. Escenarios de implantación

Tras analizar las soluciones existentes en el mercado en lo que a copia de seguridad se refiere, debemos analizar el tipo de organización en el que se va a implantar el sistema de copias de seguridad, puesto que una de nuestras tareas es implantar la solución más adecuada para cada entorno. Ya que no es ni eficiente ni eficaz instalar un sistema muy sobredimensionado, por los sobrecostes a nivel de infraestructura y licenciamiento que se generan y la elevada complejidad que puede generar. De la misma manera un sistema infra dimensionado también puede generar problemas de rendimiento, de espacio, puede llegar a bloquearse la realización de las copias de seguridad generando un sistema completamente errático, no funcional e inconsistente, que sería peor que no tener un sistema de copia de seguridad, ya que no podemos confiar en el sistema.

Por esto mismo vamos a entrar a analizar los diferentes tipos de organizaciones empresariales que podemos encontrar en función de su tamaño, nos centramos en la ejemplificación de empresa ya que es extrapolable a casi cualquier tipo de organización o sociedad (ONG, Partido político, sindicato, agrupación, entidad deportiva, etc). Y las analizamos en función del tamaño puesto que el volumen de información, esta intrínsecamente asociado al tamaño de la empresa, a más personal, más información es producida y a la vez más información es necesaria para la toma de decisiones.

2.14.1. Microempresa

Una Microempresa, Según el Reglamento Nº 651/2014 de la Comisión Europea, define el concepto de microempresa, como aquellas empresas con menos de diez trabajadores y cuyo volumen de negocios anual no superará los dos millones de euros.

Este tipo de sociedades normalmente tienen dos niveles jerárquicos principales, que son el jefe y los trabajadores, con una facturación limitada por ende limitados beneficios, normalmente subcontratan servicios que no son su core de negocio como la asesoría fiscal online o la logística o el servicio IT. para un escenario asi, la criticidad no se encuentra en el volumen de sistemas a respaldar puesto que seguramente conste de un servidor con redundancia en el mejor de los casos o directamente haga uso de una arquitectura Cloud, si su infraestructura es física, la opción más económica, podría decantarnos hacia una solución Opensource, que, aunque Opensource no significa gratis de las soluciones analizadas, si son mucho más económicas. En el supuesto de que los datos a respaldar no fueran muchos unos pocos gigas podríamos utilizar UrBackup ya que estamos buscando un sistema sencillo y rápido, un ejemplo de este tipo microempresa podría ser una tienda de proximidad, cuyo volumen de información a respaldar es muy pequeño pero necesario. pero si deseamos tener algo más profesional debido a la criticad de los datos Utilizamos Bacula, que si bien el tiempo de implementación es mayor al tener una arquitectura sencilla, la parametrización y configuración va ser más sencilla y como consecuencia tendremos un sistema más robusto y fiable, con cifrado y compresión, un ejemplo de este escenario, sería una clínica puesto que los datos que utilizan son muy sensibles, y al estar bajo el amparo de la ley de protección de datos debemos de añadirle una capa extra de seguridad a las copias y además debido a los archivos que utilizan, es más que necesario utilizar compresión.

Si la infraestructura actual de la organización es completamente en Cloud, si este Cloud AWS, Azure, Google, lo lógico seria apoyarse en software propietario, compatible al 100% con estas nubes, este tipo de organización ya estará acostumbrada a utilizar un modelo de pago por suscripción con lo que aunque pueda parecer excesivo para el volumen de negocio que genera, el pago por uso, puede ser una opción.

2.14.2. Pequeña Empresa

Una pequeña empresa según el reglamento indicado en el punto anterior es aquella que cuenta con un número de trabajadores menor a 50 y su facturación anual y balance general no supera los 10 millones de euros,

En este tipo de sociedades, nos podemos encontrar una infraestructura consistente de red es decir distribuida, con vlans o subnetings, si la infraestructura de software es On-premises, tendrá varios servidores que gestionaran varias aplicaciones para obtener ciertos registros, aquí nos podemos encontrar una arquitectura bastante critica porque podemos encontrarnos entornos en los que diferentes tecnologías ocupan un espacio y podemos tener un sistema por ejemplo que haga uso de un sistema Linux y de Oracle SQL o una App que se apoye en MySql o en MSSQL, aparte de un cierto número de ficheros compartidos de ofimática, la infraestructura en este tipo de empresa puede ser muy variada, suelen tener sistemas obsoletos.

En este escenario podemos apararnos en herramientas Opensource, pero las versiones Enterprise con un buen partner que nos agilice la implantación del sistema debido a su adaptabilidad lo más recomendable es utilizar Bacula teniendo en cuenta que es un software que una vez implantado el mantenimiento y la gestión es sencilla.

Si la empresa utiliza una infraestructura hibrida o en Cloud en este caso dependiendo de la infraestructura podemos optar por un software propietario, estas soluciones tienen experiencia de trabajo en entornos Cloud como son AWS Elastic Compute Cloud (EC2), Azure Virtual Machines y Google Compute Engine, en el caso de que se esté usando IaaS (Infraestructura como servicio) o en el caso de PaaS (Platform-as-a-Service). debemos tener en cuenta que este tipo de empresas no suelen tener una estructura homogénea en cuanto a infraestructura se refiere, utilizando una amalgama de tecnologías, ya que normalmente suelen tener un responsable de IT, pero no un departamento, la mayoría de las implantaciones suelen realizarse por proveedores extornos y el responsable, se encarga de realizar las tareas de mantenimiento. En definitiva, deberemos analizar la infraestructura que utilice y ver la compatibilidad con las diversas soluciones del mercado para decirnos por una o por otra.

2.14.3. Empresa mediana

Una mediana empresa es un término utilizado para referirse a aquellas que, aun teniendo un tamaño moderado, no se situarían en la categoría de pequeñas empresas y, por este mismo motivo, tampoco en las de gran tamaño. En la Unión Europea según la normativa de 2014, la mediana empresa es aquella que posee entre 51 y 250 empleados, factura como máximo 50 millones de € y tiene un inmovilizado no superior a 43 millones de €. Este tipo de empresa suele tener un departamento de IT, que se encarga tanto de gestionar proyectos con el apoyo de diferentes partners o de manera autónoma poder llegar a implantar y mantener sus propios proyectos. En este escenario podemos encontrarnos siendo parte del equipo Cliente o del Partner, dependiendo del lado en que nos encontremos tomaremos unas decisiones o otras, en la toma de decisiones acerca de la solución tecnológica a implantar, normalmente estaremos en el lado del cliente existen ciertos criterios a evaluar, como son el coste tanto en precio como

en tiempo por parte del personal involucrado en lleva adelante este proyecto. Aquí podemos utilizar software tipo Bacula, pero a no ser que tengamos experiencia con la herramienta podemos perder mucho tiempo parametrizado y en definitiva realizado la implantación. Mientras que, en el caso de los softwares propietarios detallados en el punto anterior, tienen una curva de aprendizaje pequeña, además de estar orientado a la escalabilidad, además de modalidades de pago por uso, que lo pueden hacer más que competitivo.

Como en el punto anterior, si la empresa actualmente ya está utilizando una a infraestructura hibrida o en Cloud, deberemos adaptarnos a esta con soluciones de respaldo compatibles con la arquitectura disponible. Si la infraestructura está en AWS, Azure o Google, las soluciones de software privativo, tiene mejor rendimiento actualmente, debido también a las inversiones que estas empresas hacen en estos clouds.

2.13.4. Empresa grande

En la organización de tipo de empresa según su tamaño, cuando una entidad cuenta con 250 trabajadores o más pasa a ser considerada una gran empresa. Así mismo, en los criterios económicos, si la compañía supera los 50 millones de euros en el negocio anual y también supera los 43 millones de euros en el balance general, es decir, en ambos criterios supera los límites de las pymes, se considerará gran empresa.

En este escenario, Conforme la especialización tanto de los recursos de infraestructura como de aplicaciones aparece en el mercado, la externalización de los servicios de TI empieza a cobrar una importancia mayor, y el departamento de TI de estas organizaciones pasa a tener un papel de controlador y gestor de los servicios recibidos. En este caso se realizara un estudio de las diferentes soluciones del mercado con diferentes partners tecnológicos, de entre todas, se seleccionará la solución más adecuada al problema y tras elegir entre las diversas soluciones hay que decidir un partners, si es de confianza podemos decantarnos directamente por el, sino, lo más lógico sería realizar un breve concurso con tres posibles partners que nos den un presupuesto, así como un plan de acción en el que se nos detalle cómo van abordar la necesidad. a partir de ahí decidir cuál es la mejor solución.

En este escenario, mayoritariamente, se utiliza software propietario y en el caso de utilizar una infraestructura hibrida o en Cloud, normalmente harán uso de las nubes más populares como son AWS, Azure y Google, por lo que las soluciones estudiadas en el punto anterior, serian serias candidatas al ser el software de respaldo de una gran empresa, ahora habría que contactar como se ha indicado con un partner de Acronis otro de Commvault y otro de Veeam, para que nos proyecten y presenten las diferentes tecnologías que aportan cada una de las soluciones. tras decidirnos habría que buscar dos partners más para evaluar más allá del licenciamiento que será el mismo, el coste de los servicios de configuración y puesta en marcha.

3. Implantación

3.1. Establecimiento del Marco

Tras analizar los diferentes escenarios posibles así como una breve reseña de las soluciones más relevantes en cuanto a copias de seguridad, debemos, encuadrar nuestro proyecto de tal manera que podamos evaluar una solución real y funcional, para ello estableceremos las premisas que nos permitan identificar un entorno en el que situarnos, así como definir una arquitectura a nivel de sistemas, de esta manera seleccionaremos una solución de las analizadas procediendo a su implantación para ver los problemas y funcionalidades técnicas que vamos a encontrarnos.

Viendo los posibles escenarios, seleccionaremos una posición intermedia entre mediana y gran empresa, ya que nos va a generar una arquitectura anterior que deberemos respetar y así probaremos la compatibilidad de las soluciones, además de al ser una empresa de este tipo, tendremos diferentes sedes, en distintas ubicaciones y ver cómo afecta esta problemática a las diferentes soluciones, esta empresa que estamos enmarcando constara de tres sedes:

- Sede A, una sede principal siendo esta la sede más grande con el mayor cantidad de información
- Sede B, otra sede esta vez secundaria en cuanto a volumen, pero independiente en cuanto a datos y documentos.
- sede C independiente en cuanto a documentos, pero no en cuanto datos que depende de las sede B.

Hay que indicar que el departamento RRHH, el departamento de mantenimiento y el departamento de IT, se encuentran centralizado y ubicados en la sede A.

Estas tres sedes estarán conectadas por fibra óptica de la siguiente manera:

Sede A: 2 líneas de fibra óptica de 300MB simétricos con un WiMAX de Backup

Sede B: 1 línea de fibra óptica de 300MB simétricos, 1 línea de fibra óptica de 100MB simétricos y un WiMAX de Backup

Sede C: 2 líneas de fibra óptica de 100MB simétricos y un WiMAX de Backup

Para controlar el acceso a internet utilizan un firewall next gen que aparte de realizar las funciones de filtrado de dispositivos de red, también utiliza la inspección profunda de paquetes, inspeccionando el tráfico cifrado, permitiendo la gestión del ancho de banda mediante QoS, entre las características de estos firewall asimismo posee la capacidad de ofrecer un servicio de interconexión entre si mediante túneles VPN IPSec entre las 3 sedes además de un grupo de conmutación por error con el enlace secundario por si acaso hay caída de la fibra principal.

En cuanto a la red interna:

- **Sede A** , contiene varias Vlans, dispone de 6 racks distribuidos por toda la empresa, cada uno con 2 switches uno poe otro sin poe, igualmente tiene una red wifi por toda la organización, los switches están interconectados entre si mediante maya de fibra de 10Gb con puertos Giga Ethernet. Está a nuestra disposición además un NAS Synology de 10TB

- **Sede B**, contiene varios Vlans, dispone de 3 racks distribuidos por toda la empresa, cada uno con 1 switches con poe, interconectados entre si mediante maya de fibra de 10Gb con puertos GigaEthernet, además posee una red wifi por toda la organización. Está a nuestra disposición además un NAS Synology de 4TB.
- **Sede C**, dispone de 3 racks distribuidos por toda la empresa, cada uno con 1 switch con poe interconectando entre los racks fibra de 10Gb y con puerto de GigaEthernet, existe una red wifi por toda la organización. Está a nuestra disposición además un NAS Synology de 1TB.

Tras realizar un análisis BIA detectamos una serie de datos y sistemas críticos que debemos salvaguardar en las sedes.

Sede A

- Diferentes bbdd Sql server, alojadas en diferentes servidores garantizando siempre la alta disponibilidad.
    - 2 servidores MSSQL BBDD's Software de nóminas, control de presencia 1 principal y uno secundario con replicación para la redundancia de datos
    - 2 servidores oracle SQL BBDD's ERP
    - 2 servidores MSSQL software de control de producción, toma de datos en planta y cálculo de OEE
    - 2 servidores Mysql para el GMAO que además es utilizado por el inventario y un sistema de Tickets del departamento de tecnologías de la información.
- 2 servidores de ficheros DFS en conjunto a Active Directory

Sede B

- Diferentes bbdd Sql server, alojadas en diferentes servidores garantizando siempre la alta disponibilidad.
    - 2 servidores oracle SQL BBDD's ERP
    - 2 servidores MSSQL software de control de producción, toma de datos en planta y cálculo de OEE
- 2 servidores de ficheros DFS en conjunto a Active Directory

Sede C

- 2 servidores de ficheros DFS en conjunto a Active Directory

De acuerdo con este marco, con la intención de abaratar costes, no se hace necesario implantar un sistema DRaaS, un Sistema BaaS sería suficiente además, si existe la posibilidad de replicar el entorno de produccion en el Cloud, como sucede en este marco, este supuesto es el ideal, puesto que en el caso de que tengamos la pérdida total de todos los sistemas como pudiera ser ante un incendio, existe la posibilidad de recuperar el entorno de produccion a una nube IaaS que permita continuar con la operativa de la organización con un RTO no muy elevado.

3.2. Análisis de los requisitos físicos

Independientemente del escenario de trabajo, hay ciertas necesidades a nivel físico que deben estar cubiertas, se presupone que, de acuerdo con el marco anteriormente descrito, las necesidades están cubiertas, no obstante, vamos a analizarlas y verificar si están cubiertas o no.

- Espacio físico
  Deberemos tener un espacio no inflamable por construcción ni penetrable, este espacio, no debe poseer ventanas ni situarse ni por encima ni por debajo de elementos de riesgo como cañerías, tuberías, desagües..., la altura mínima libre de obstáculos debe estar en torno a los 2,5m entre el suelo técnico y los elementos del techo, debe poseer un área de acceso biométrico, que permita el acceso solo a personal autorizado.

En definitiva, debe ser un espacio que proporcione estanqueidad contra agua, polución y gas, seguridad antivandálica y resistencia contra el fuego, es recomendable tener suelo técnico

- Sistema eléctrico
  Debemos contar un sistema redundante N+1 con caminos diferentes en todas las canalizaciones, con el fin de tener puntos únicos de fallo, deberemos que utilizando los SAIs se abastecerá a los sistemas de CCTV, Control de Accesos, Antiincendios e incluir el sistema Backup, este punto es importante puesto que mediante el binomio PDU-SAI Intentaremos controlar la situación de corte prolongado de la corriente eléctrica mientras se están realizando los backups o se están publicando en la nube. resulta obvio que para minimizar las fugas de corriente y controlar los problemas del disparo diferencial, debe existir en este espacio un mallado de tierras equipotenciales cumpliendo la normativa EN 50310 para sistema de tierras y equipotencialidad.

- Sistema de detección y extinción de incendios
  Se debe contar con un buen sistema de detección y extinción de incendios para prevenir, detectar y extinguir incendios en las diferentes zonas que lo componen (Falso techo, suelo técnico, ambiente), que además sea independiente del resto del edificio. por eso deberemos comprobar que se cuenta un sistema por aspiración de alta sensibilidad, formado por un conjunto de tuberías que permitan identificar un fuego incipiente en el área cumpliendo las Normas NBE-CPI/96 y UNE 23007. Como sistema de extinción deberá contar un sistema de extinción para fuego eléctrico que elimine el fuego, pero además no dañe los elementos.

- Sistema de Seguridad y Control de Accesos
  Como la información contenida en las contenida en las copias de seguridad es de carácter sensible, según la GDPR, debemos tener controlado el acceso físico a los equipos que almacenan estos backups con métodos anti-passback, de tal manera se pueda asegurar la integridad, confidencialidad y consistencia física de los equipos.

- Cableado Estructurado
  Es importante que las instalaciones en las que se ubica cuenten con un cableado estructurado, de tal manera que sea flexible ante el crecimiento de la organización, permitiendo adaptarse a nuevas exigencias facturas, es decir que el sistema Backup tenga acceso de manera estable y robusta con los equipos a respaldar.

Como hemos indicado al principio de este apartado, se cumple con todos los criterios de este punto en todas las sedes, en caso de no ser así, pediríamos los presupuestos necesarios que en definitiva permitan poder poner a salvo el dato.

3.3. Análisis de infraestructura necesaria

Tras establecer el marco de trabajo, ya podemos realizar un análisis de la infraestructura existente y a partir de ahí definir que infraestructura necesitaríamos adquirir para llevar a buen término la implantación del servicio de respaldo. Sin olvidar que el objetivo último de este proyecto consiste en garantizar la continuidad del negocio y del servicio, con lo que intrínsecamente, debemos obtener un sistema que sea capaz de ofrecer Alta disponibilidad del dato de negocio mediante el servicio de Backup.

El análisis de la infraestructura existente se debe abordar desde dos puntos de vistas, el punto de vista lógico en el que detallaremos que unidades de negocio queremos salvaguardar, es decir que queremos copiar. Y un punto de vista físico, en el que analizaremos la electrónica existente, estado y capacidad, ya que de poca fiabilidad al sistema nos puede dar un NAS, cuyos discos den errores en un test de S.M.A.R.T, o el cableado entre switch es deficiente.

Tras revisar todos los componentes que intervienen en la copia, Estado de los NAS, de los Discos, la electrónica de redes, el acceso a internet, reemplazaremos los sistemas deficientes. obviamente, para este ejercicio teórico-practico vamos a suponer que los sistemas se encuentran mantenidos correctamente y la infraestructura pre existente es óptima.

El siguiente paso, seria localizar la parte más deficiente e intentar mejorarla, intentando a la vez los costes bajos. para el marco de estudio del punto 3.1, un posible punto débil puede ser el espacio en disco de los NAS, puesto que al tener una infraestructura de túneles VPN interconectadas entre sí, podemos utilizar esta interconexión, para enviar las copias entre sedes, de tal manera que tengamos siempre una segunda copia offsite pero intra organización. para ello podemos ampliar el espacio de disco dejando todas las sedes con un espacio de almacenamiento de 10Tb y que todas las sedes compartan los mismos backups, esta replicación se puede realizar utilizando el software incluido en los propios NAS o realizar trabajos específicos y aplicarle diferentes políticas de retención a las copias locales. Otra mejora plausible, es ampliar el ancho de banda de la sede de 100MB a 300MB simétrico, de esta manera, intentaremos paliar lo máximo posible el cuello de botella que puede ser la VPN.

También hemos de tener en cuenta si existe un equipo con la capacidad suficiente para gestionar todo el sistema de Backup o si debemos adquirir uno para este menester, este equipo en principio será único para las tres puesto que Veeam, ofrece una solución para los backups deslocalizados. Utilizando un equipo de las redes deslocalizadas (Sede B y Sede C) instala un agente Proxy que se encarga de gestionar la copia en LAN, es decir Es el equipo proxy quien rece la información del trabajo a realizar y el que se encarga de realizar el trabajo de manera local, de esta manera por ejemplo un servidor con poca carga de trabajo en la sede B, puede hacer de proxy, hacer una copia de una maquina en su entorno local (dentro de la propia sede B) y enviarla a un almacenamiento NAS de su propia Red (dentro de sede B). de esta manera ahorramos ancho de banda y limitamos el coste de licencias e infraestructuras, sin ver comprometida la continuidad del negocio.

Por esto mismo simplemente, necesitaríamos adquirir Discos de alta capacidad que generen reducidas vibraciones para trabajar en sistemas RAID y con reducción efectiva de ruido y calor preparados para sistemas 24/7, deberemos además tener la misma capacidad en todas las sedes y esta, ser suficiente para poder alojar el espacio necesario de las copias de acuerdo con

el plan de copias, aunque nos podemos adelantar un poco a este paso sobredimensionando los disco alcanzando 30TB por sede.

3.4 Análisis del plan de Copia

Como ya hemos indicado con anterioridad, los datos son cruciales y no podemos permitirnos su pérdida. Los backups son como una póliza de seguros para los datos, en el supuesto de tener que usarlos, es fundamental que funcionen correctamente y que puedan restaurar lo que se necesite. Los fallos no son una opción cuando se trata de recuperar datos. Si el método principal de recuperación falla de alguna manera, necesita un plan de Backup.

Dado que muchas organizaciones no suelen probar habitualmente la recuperabilidad de sus backups, pueden encontrarse en una situación en la que necesite un plan b o, incluso, un plan c para recuperar los datos que se han perdido.

La regla 3-2-1 garantiza poder contar con múltiples opciones de restauración de los datos. Funcionando de la siguiente manera:

Tener al menos tres copias de los datos (esto significa que debería tener al menos dos backups adicionales además de los datos en producción). Si algo sucede con un Backup, existirá otro al cual poder recurrir.

Guardar las copias en dos tipos de medios diferentes, asegurando que un problema o fallo en uno de los dispositivos no afectará a la integridad y capacidad de recuperación del otro. Por ejemplo, puede guardar un Backup en cinta y otro en disco o cualquier otro destino, tal como un proveedor de nube, dispositivo USB, SAN/NAS, etc.

Conservar una copia de Backup remota, impidiendo que un evento local como un incendio o una inundación impida el acceso a los datos principales y a todas las copias al mismo tiempo. Se pueden hacer backups secundarios sobre unidades de cinta u otros dispositivos extraíbles, replicar a otra oficina o incluso a la nube, pero asegurándose siempre de la existencia de una copia remota, manteniendo una separación física suficiente entre los entornos de Backup.

En el marco que hemos establecido, hemos indicado que existen tres sedes, conectadas por VPN y cada uno tiene un NAS, para aprovechar este hecho, podemos mandar los backups entre sedes y al cloud, de esta manera cumpliríamos con la regla 3-2-1, teniendo dos copias en dos medios diferentes (infraestructuras de red diferentes) y una copia off-site fuera de la organización en uno de los proveedores anteriormente descritos, por coste, lo mas aconsejable seria depositarlos en S3 Glacier, ya que nos ofrece suficiente con el menor coste, de acuerdo al marco de estudio.

3.4.1. Periodicidad y tipo de copias de seguridad

Tras una copia completa inicial de la totalidad de las máquinas virtuales y equipos físicos, se plantea una copia sucesivas incremental diaria.

Adicionalmente, el último día de cada mes y el último día del año se realizarán copias completas de la totalidad de máquinas virtuales.

3.4.2. Retención de las copias de seguridad

Se deberán mantener durante el año en curso, con objeto de recuperación y auditoría de la información, al menos:

- 1 copia completa semanal del mes en curso
- 1 copia completa mensual
- 1 copia completa anual

3.4.3 Registro y comprobación de copias de seguridad

Aunque el software de Backup dispone de la funcionalidad de verificar la correcta realización de la copia y la integridad de la misma, se deben realizar con una periodicidad máxima de 3 meses, pruebas de recuperación aleatorias de máquinas virtuales desde las copias de seguridad a un entorno de laboratorio aislado.

Con este procedimiento, además de verificar la integridad de las copias, se permitirá el establecer y consolidar los protocolos y procedimientos de restauración de sistemas de cara a un incidente real.

De igual forma, se debe mantener un registro anual de realización de copias de seguridad, pudiendo ser mediante el propio de la aplicación o a través de un registro externo, para que en cualquier momento verificar la correcta realización de la copias en caso de auditoría interna y externa.

3.5. Instalación y parametrización del software.

De acuerdo con el análisis realizado en los puntos 2.10,2.11 y especialmente en el 2.12, debido a los costes de licenciamiento así como las features disponibles, la solución más idónea para un entorno como el establecido en el marco de trabajo, donde existen sistemas físicos conviviendo con sistemas virtuales en idéntica proporción, es Veeam Backup.

Ya que nos garantiza cumplir con la política de copia establecida, al menor coste posible, por este motivo procedemos a realizar a modo de ejercicio práctico, la parametrización y puesta en marcha de esta solución incluyendo pruebas de respaldo y recuperación

3.5.1. Instalación del software

Tras cumplir con los requerimientos físicos y lógicos, procederemos a la instalación del software ofrecido por Veeam, en primer lugar debemos entender un poco como es la arquitectura de Veeam Backup a nivel de software puesto que estas arquitectura nos va a condicionar en cuanto a rendimiento y configuraciones., cuando le damos a instalar, lo que se va instalar es el Veeam Backup server, que sería el director, originador, de todo el sistema de copias, para ello además de este software, se van instalar otros servicios, otros componentes que serán utilizados por la herramienta sin los que no se podrán realizar los trabajos, estos componentes son el proxy y el repository.

El repository, no es más que el almacenamiento, que puede ser un disco, un NAS un espacio en cloud.

El proxy es el servicio que realiza el 'Trabajo', es el que realiza la lectura de bloques, la deduplicacion, la comprensión la recuperación igualmente es realizada por este servicio en definitiva es el encargo de realizar todas las actividades de copia en la infraestructura de produccion comandadas por el server.

En el momento de instalación, se instalan en la maquina local un default proxy y default repository, pero se podrá instalar en diferentes maquinas varios proxys (uno por maquina) y varios Repository.

Procedemos pues a descargarnos el software desde la web del Veeam y una vez descargado el software instalación, le damos doble click y procedemos a instalar, como suele ocurrir en este tipo software, aparece la información en cuanto a las aceptaciones de uso o EULA, le damos a siguiente:

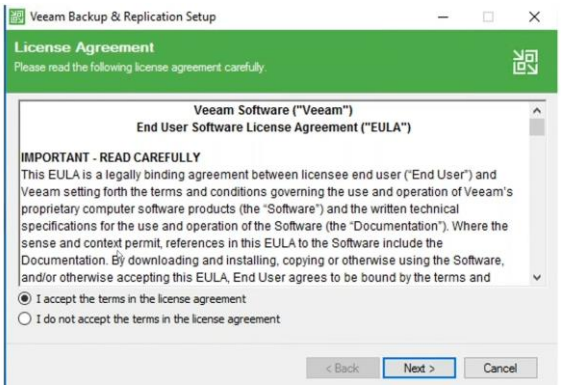

Figura 27. Aceptaciones de uso o EULA

El siguiente paso consiste en asignarle la licencia de aunque podremos utilizar licenciamiento trial o prueba por un periodo determinado, la licencia consiste en un fichero lic, que puede ser agregado en este paso o ya con el software instalado.

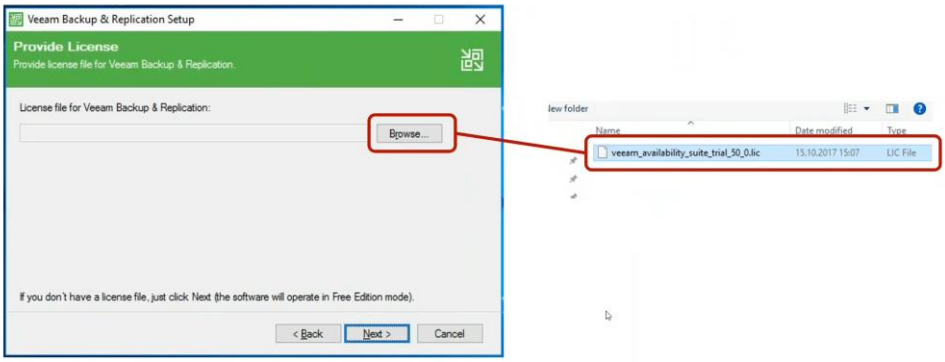

Figura 28. Inclusión del archivo licencia en la instalacion

Tras la asignación de la licencia, el instalador ofrece la posibilidad de seleccionar que componentes deseamos instalar, estas tres opciones consisten en

- Veeam Backup & Replication, consiste en el servidor propiamente dicho.
- Veeam Backup Catalog, que contiene los datos de servicio
- Backup & Replication Console, consiste en la interfaz web que permite conectar con el servidor

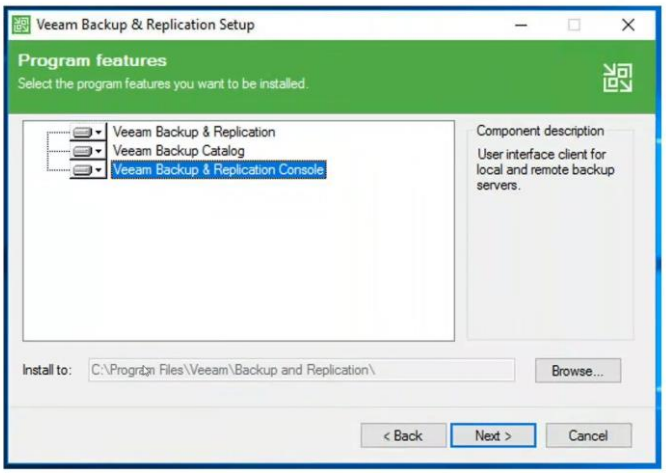

Figura 29.Características del programa

Ahora nos aparece la configuración por defecto de instalación que podremos cambiar al dejar marcada la opción *Let me specify different settings*

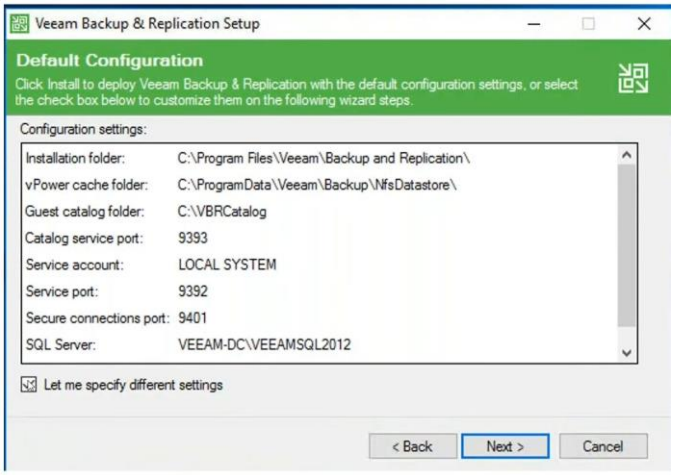

Figura 30. Configuración por defecto

Como la intención del proyecto es formativa, vamos investigar, que opciones podremos seleccionar, para empezar nos permite seleccionar toda la información relativa al servidor de SQL puesto que este software hace uso de una BBDD de SQL server que puede estar o no en el equipo donde se va instalar el software, para almacenar toda la información de configuración, del catálogo , mensajes históricos, etc. Como vemos se nos da la opcion de especificar una

cuenta con permisos, tambien,nos da la capacidad de instalar una nueva instancia o usar conistente, asi como permitir especificar credenciales para la conexión SQL

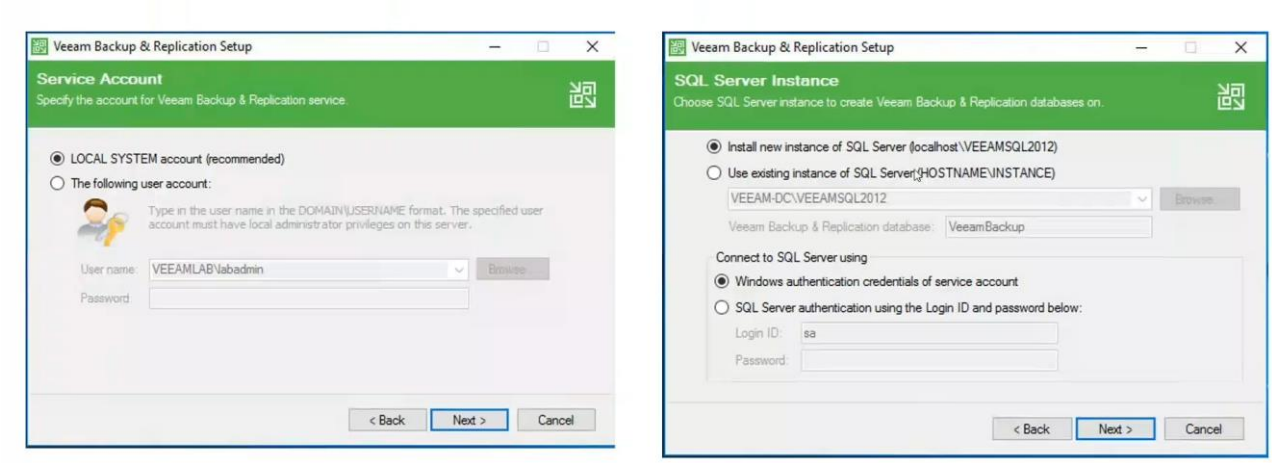

Figura 31. Conexión a SQL Server

Tras la pertinente revisión de las opciones generales salimos de este modo de configuración avanzada y continuamos dándole al botón Next; para llegar al punto donde debemos de especificar las carpetas que utilizara el sistema

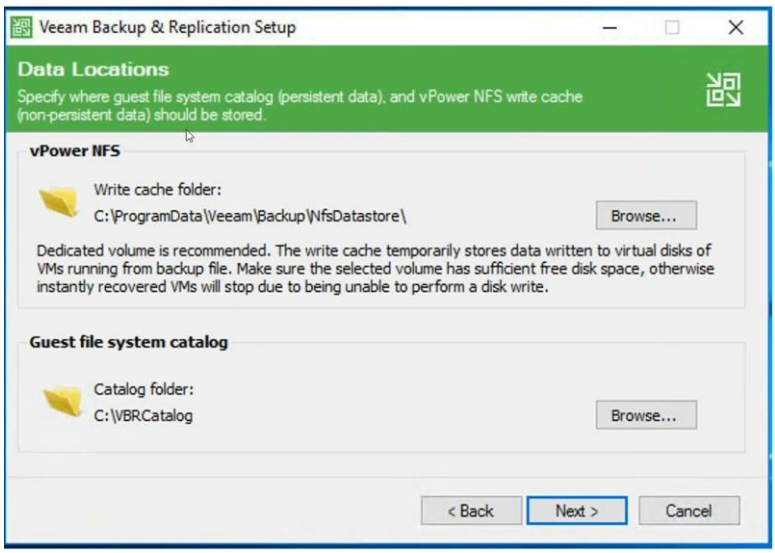

Figura 32. Especificación carpetas del sistema

Estas carpetas son:

- *Guest file system Catalog*, que como su nombre indica consiste en las carpetas donde se van a almacenar los archivos índice del SO huésped de máquina Virtual.
- *vPower NFS*, esta ruta, consiste en un directorio especial donde se almacena el archivo VMDK que se genera al iniciar una máquina virtual desde una copia de seguridad, recordemos que este software, permite arrancar a partir de una copia completa tanto maquinas físicas como virtuales, en un entorno virtual. asimismo se utiliza para almacenar el cache de la copia cuando estamos explorando el contenido de las unidades en el archivo de copia.

Al continuar aparece el resumen de la configuración seleccionada, procedemos a instalar:

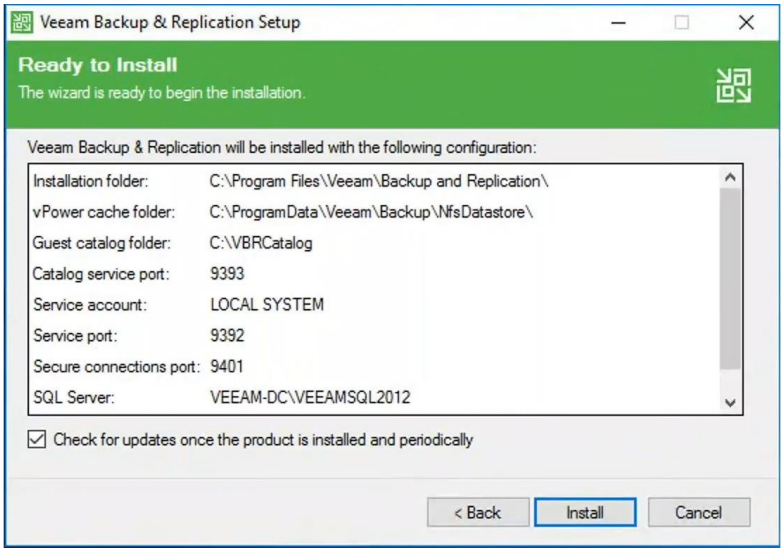

Figura 33. Resumen de la configuración seleccionada.

Durante la instalación se comprobará los componentes necesarios como son el SQL server, el .net Framework 4.7, PowerShell 5.1, Microsoft Universal C Runtime, etc. En caso de no encontrarlos procederá a instalarlos.

Con esto ya habríamos realizado la instalación del software, ahora vamos a analizar la parametrización de este.

3.5.2 Parametrización

Para poder realizar la parametrización, debemos entender la arquitectura disponible en Veeam Backup. Al ser un software que en origen se creó con la filosofía de dar un soporte eficaz a Backup de infraestructura virtual, mucha de su funcionalidad está enfocada a esta tarea.

Veamos cómo se comporta software a nivel de inventario, en el que añadiremos la infraestructura que deseamos respaldar. Para VMware vSphere protección podemos añadir hosts ESXi individuales y también se permite añadir vcenter server con todos los Host a los que este tenga acceso. Para Hyper-V podemos añadir System Center Virtual Machine Manager SCVMM server y Hyper-V clusters. Como infraestructura física los añadiremos como Standalone host. Recordemos que también se puede añadir carpetas compartidas, tanto en servidores como NAS, que utilicen SMB o NFS.

Tras realizar el inventario de la infraestructura a respaldar, añadiremos los proxys de Backup que son un componente de arquitectura de Veeam que se encuentra entre el servidor de Backup y otros componentes de la infraestructura de Backup. Mientras que el servidor de Backup administra las tareas, el proxy procesa los trabajos y entrega el tráfico de respaldo.

Estos proxys, se utiliza en infraestructura de virtualización y entre sus tareas básicas, se incluyen:

Recuperar datos de VM del almacenamiento de producción

- Compresión
- Deduplicacion
- Encriptando
- Enviarlo al repositorio de Backup (por ejemplo, si ejecuta un trabajo de Backup) u otro proxy de Backup (por ejemplo, si ejecuta un trabajo de replicación)
- Un proxy de Backup puede funcionar como transportador de datos en el Backup del NAS y transferir datos desde el recurso compartido de archivos de origen al repositorio de Backup.

Si analizamos como funciona este proxy para VMware ESXi y vSphere en cuanto al transporte de datos tenemos 3 modos:

- **Acceso directo al almacenamiento (Direct Storage Access)** En el modo de acceso directo al almacenamiento, Veeam Backup & Replication lee o escribe datos directamente desde o hacia el sistema de almacenamiento donde se encuentran los datos de VM o las copias de seguridad, permite SAN y NFS

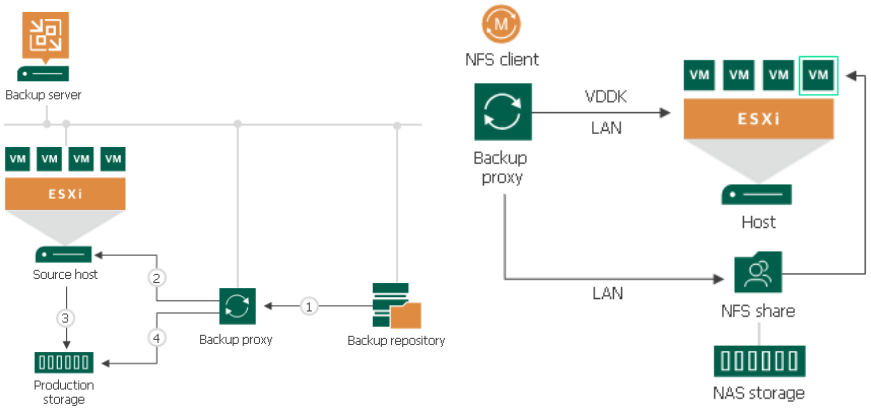

Figura 34. Diagrama proxy de Backup modo acceso directo al almacenamiento

- **Virtual Appliance (HotAdd)** En este modo, Veeam Backup utiliza la capacidad VMware SCSI HotAdd que permite conectar dispositivos a una VM mientras la VM está en ejecución. Durante la copia de seguridad, los discos de replicación o restauración de la máquina virtual procesada se adjuntan al proxy de copia de seguridad. Los datos de la VM se recuperan o escriben directamente hacia o desde el almacén de datos, en lugar de pasar por la red. Este modo no es tan eficiente como el modo de acceso directo al almacenamiento, pero proporciona un mejor rendimiento que el modo Network

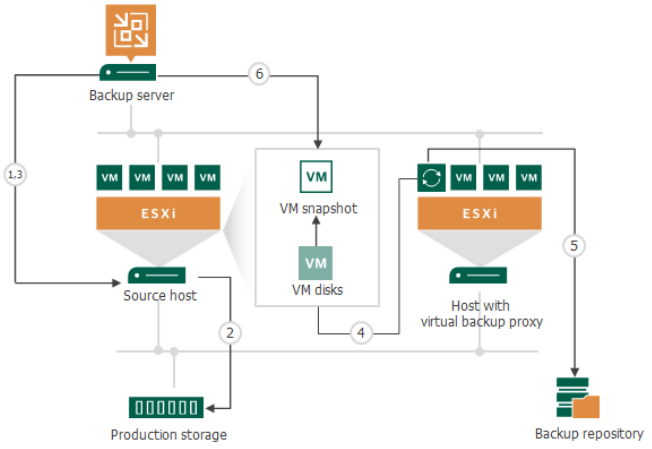

Figura 35. Diagrama proxy de Backup modo virtual Appliance

- **Network** Este modo se puede utilizar con cualquier configuración de infraestructura. En este modo, los datos se recuperan a través del host ESXi a través de la LAN mediante el protocolo de dispositivo de bloque de red (NBD). el modo Network es el único modo aplicable cuando el rol de proxy de Backup se asigna a una máquina física y el host usa almacenamiento local. Además, el modo Network puede ser la mejor opción si tiene un entorno virtual grande con cientos de máquinas virtuales pequeñas, con redes Ethernet de 10 Gb y con una tasa de cambio pequeña.

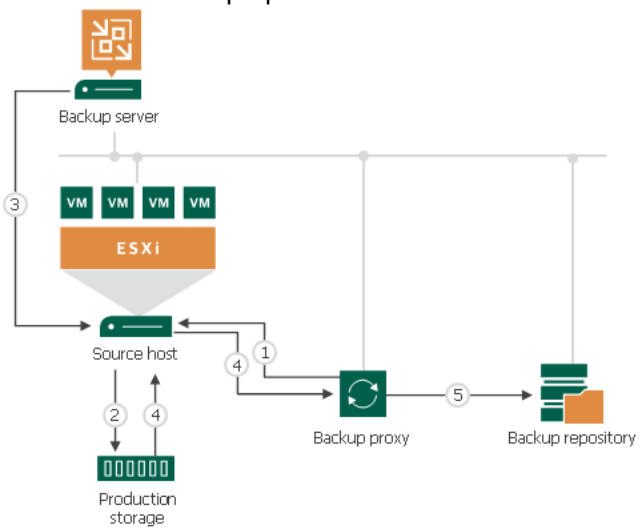

Figura 36. Diagrama proxy de Backup modo Network

Otro tipo de proxy es el Proxy CDP VMware que es básicamente es un componente que funciona como transportador de datos y transfiere datos entre los hosts de origen y destino. Normalmente se utiliza para interconectar la infraestructura en produccion con la infraestructura de recuperación ante desastres, normalmente se configurará como mínimo un proxy en origen y otro en destino que se encargaran en sincronizar los cambios que se produzcan en el host en productivo con la infraestructura de recuperación.

Tras analizar cómo funciona la solución con máquinas virtuales VMware procedemos a analizar el comportamiento del software en servidores de Hyper-V. Básicamente, existen dos tipos de proxies, los off-hosts y los On-hosts, el caso de los proxies On-host, se instalan en el host de origen de Microsoft Hyper-V donde residen las máquinas virtuales que desea realizar una copia de seguridad o replicar. Todas las operaciones de procesamiento se realizan directamente en este host de origen. mientas que el proxy off-host se utiliza para intentar eliminar la posible sobrecarga no deseada en el host Hyper-V de producción, el proceso es más lento que en un proxy On-host.

Como vemos el servidor proxy es un elemento que consigue hacer eficaz el proceso de Backup en equipos virtuales, aliviando la carga de trabajo al servidor de Veeam Backup.

Otro componente muy importante durante la realización de la copia mediante Veeam Backup es el Gateway server

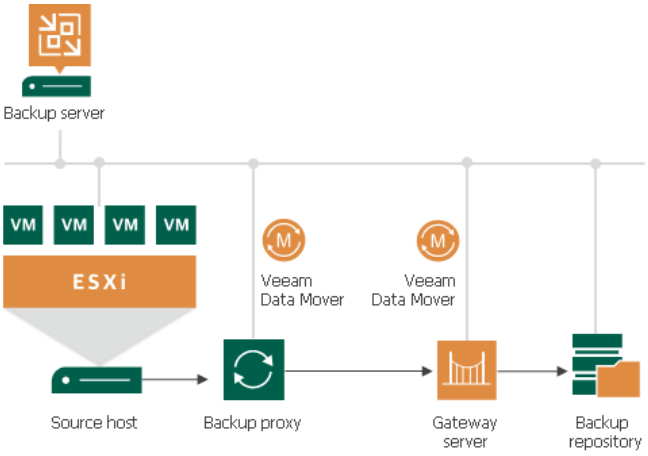

Figura 37. Diagrama Gateway server

Este componente se sitúa a la entrada del repositorio y es el que se encarga de realizar la escritura de datos en el repositorio, se utiliza especialmente en entornos descentralizados y cuando no se puedan albergar el agente de transporte de Veeam, se debe seleccionar una pasarela de repositorio, esta recibirá datos de los proxies en su camino al repositorio, opcionalmente descomprime los datos, construye los archivos de respaldo y los escribe en el almacenamiento.

Existen multitud de componentes y servicios disponibles en Veeam Backup. No obstante para entender el funcionamiento de la herramienta a nivel básico, debemos comprender bien el funcionamiento de un componente denominado repositorio Backup:

Un repositorio de Backup o un Backup repository es una ubicación de almacenamiento donde Veeam guarda archivos de respaldo, copias de VM y metadatos para VM replicadas.

Para configurar un repositorio de respaldo se pueden utilizar los siguientes tipos de almacenamiento:

- **Direct attached storage**, permite agregar servidores virtuales y físicos como repositorios de respaldo, tanto de Windows como de Linux y utilizar el almacenamiento basado en disco como un disco duro USB o un iSCSI

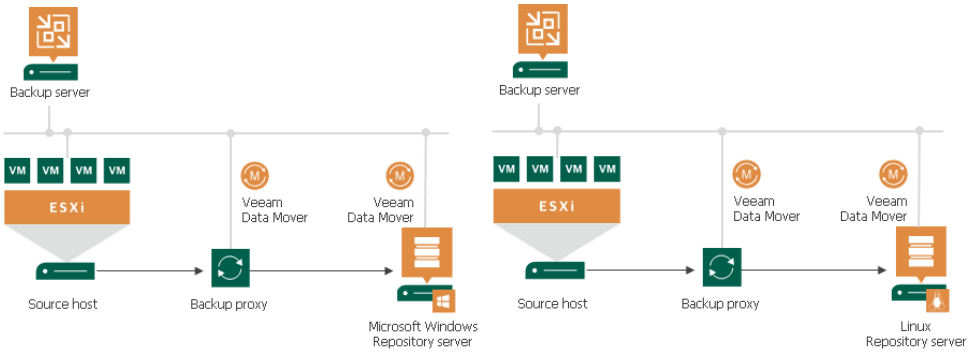

Figura 38. Diagrama repositorio de respaldo del tipo Direct Attached Storage

- **Network Attached Storage**, permite agregar recursos compartidos de red del protocolo SMB(CIFS) y del protocolo NFS, como repositorios de Backup

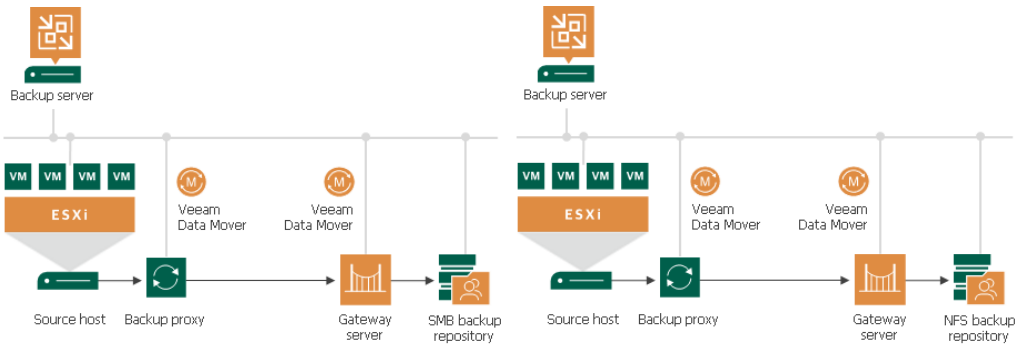

Figura 39. Diagrama repositorio de respaldo del tipo Network Attached Storage

- **Deduplicating Storage Appliances**, permite agregar dispositivos de almacenamiento con deduplicacion como repositorio y estos pueden ser los que ofrecen Dell EMC Data Domain, ExaGrid, HPE StoreOnce y Quantum DXi

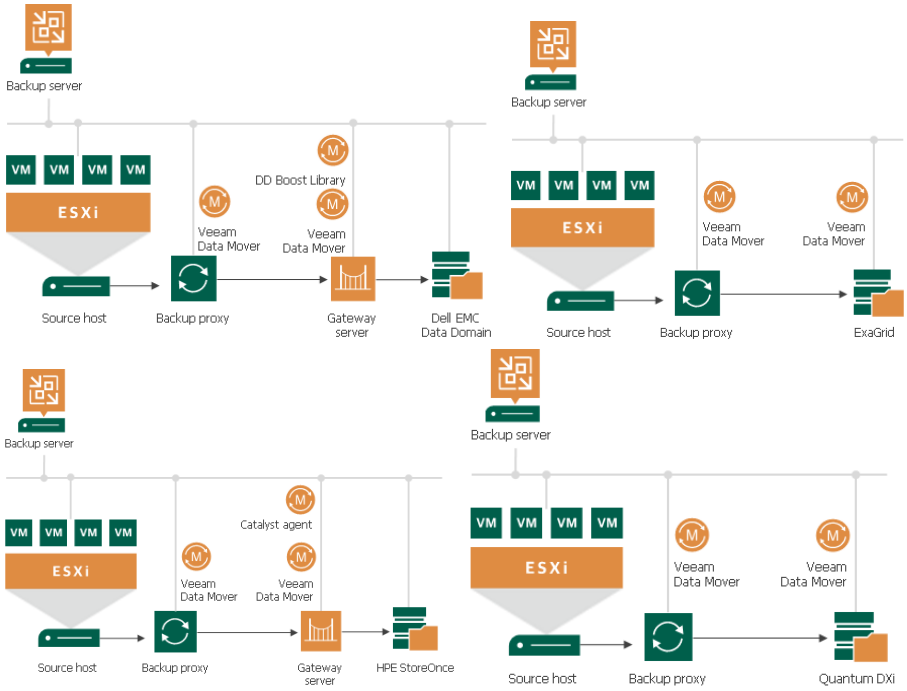

Figura 40. Diagrama repositorio de respaldo del tipo Deduplicating Storage Appliances

- **Object Storage**, permite utilizar el almacenamiento en la nube de objetos como repositorio de Backup, estas nubes pueden ser S3 y compatibles, Google Cloud, IBM Cloud, Microsoft Azure Blob.

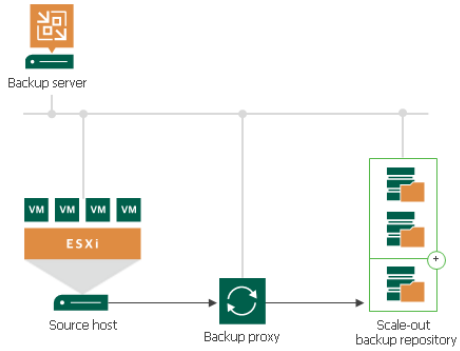

Figura 41. Diagrama repositorio de respaldo del tipo Object Storage

El último punto para comentar, son los métodos de Backup, actualmente Veeam ofrece tres métodos

- Forever forward incremental (FFI)
  Este método crea una cadena de Backup que consta del primer archivo de Backup completo (VBK) y un conjunto de archivos de Backup incremental hacia adelante (VIB) que lo siguen, es decir solo habrá un Backup Full y el resto de los respaldos serán incrementales. Este método de Backup permite a ahorrar espacio en el almacenamiento, pero en contraposición, produce una sobre carga de E/S adicional en el almacenamiento, puesto que se tendrá que inyectar los incrementales antes de eliminarlos de acuerdo con la política de retención.

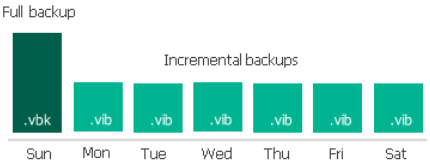

Figura 42. Gráfico método de Backup Forever Forward Incremental

- Forward incremental (FI)
  Este método, crea una cadena de Backup que consta de varios archivos de Backup completo (VBK) y conjuntos de archivos de Backup incremental hacia adelante (VIB) después de cada full, este método de respaldo requiere más espacio de almacenamiento que otros métodos porque las cadenas de respaldo contienen múltiples archivos de respaldo completos, pero es el más rápido

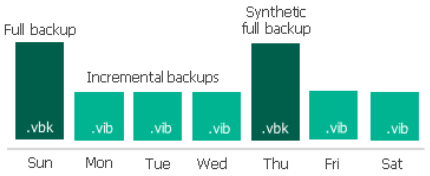

Figura 43. Gráfico método de Backup Forward Incremental

- Reverse incremental (RI)
  Este método, crea una cadena de respaldo que consta del archivo de respaldo completo (VBK) y un conjunto de archivos de respaldo incremental inverso (VRB) que lo precede. La restauración al último punto de restauración a partir de archivos de copia de seguridad creados con el método RI es la más rápida en comparación con otros métodos porque el punto de restauración más reciente es siempre una copia de seguridad completa y se actualiza después de cada ciclo de copia de seguridad. en contraprestación, este método produce el mayor impacto de E/S en el almacenamiento

en comparación con otros métodos de Backup puesto que las variaciones en bloques de información se deben inyectar y reemplazar en la copia completa, los bloques reemplazados se utilizan para generar archivos incrementales inversos, esta operación puede generar una fragmentación en el archivo de Backup completo, razón por la que se debe además realizar periódicamente una operación de compactación del archivo de Backup full, con la sobrecarga que esta pueda provocar.

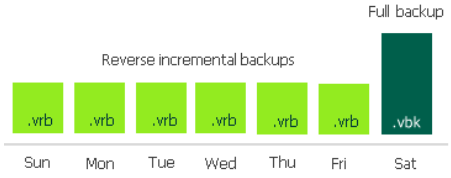

Figura 44. Gráfico método de Backup Reverse Incremental

Después de entender las opciones claves de configuración que ofrece la tecnología Veeam Backup, debemos de acuerdo con el plan de copia que se ha establecido según el marco de estudio, configurar y parametrizar la solución.

Lo primero que vamos a configurar, son las opciones de envío de mail, puesto que es una de las opciones más importantes, ya que nos permite detectar que todas las copias se están ejecutando correctamente, sin tener que entrar en el software todos los días, para su configuración accedemos al menú y en General Options

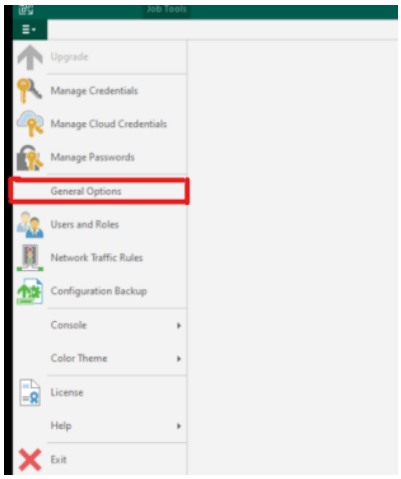

Figura 45. Menú de opciones

En la tercera pestaña, introduciremos los datos válidos, de una cuenta SMTP, así como definiremos la cuenta de correo del operador de Backup que, en definitiva, es quien debe recibir las alertas.

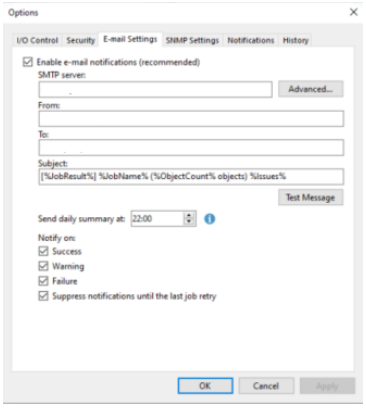

Figura 46.Opciones de configuración de email

Entre las opciones marcadas para envío de mails, dejaremos todas las opciones, Success, Warning, Failure, suppress notifications until the last job retry, escogemos estas opciones porque debemos de detectar que el sistema de notificación es correcto o si falla, además de realizar un registro diario verificando que todas las copias se han realizado correctamente.

Otro punto de este menú a revisar es el configuración Backup, ya que este nos permite configurar una copia de seguridad de la configuración del Veeam

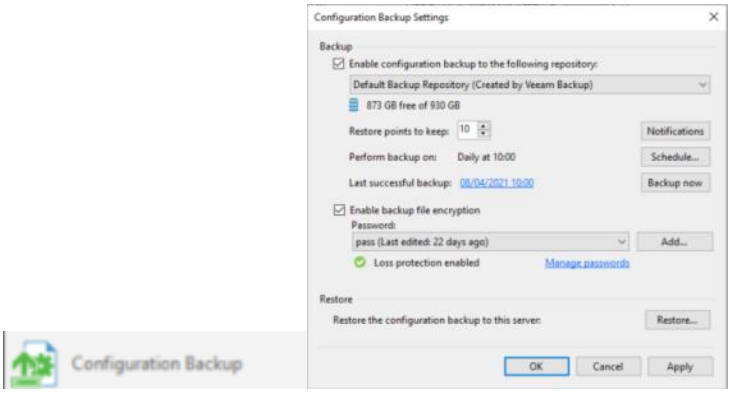

Figura 47. Pantalla de copia de la configuración

Esta configuración es más que prioritaria, en caso de desastre en la propia máquina de Veeam o por una migración de Hardware, solo tendremos que restaurar la última copia de la configuración, pudiendo recuperar todo el sistema de Backup.

El último punto a tener en cuenta de este menú es el administrador de credenciales, ya que el Manage Credentials, administraremos y almacenaremos las credenciales de acceso a los diferentes hosts a los que realicemos conexión, recordemos una vez más, que las credenciales a utilizar en todo proceso Backup, deben ser independientes a las utilizadas en el resto de la red y con privilegios de administrador, y las crearemos exprofeso. Esto nos permitirá poner un poco más a salvo el sistema Backup.

3.6. Respaldo utilizando la solución

Para realizar las pruebas de respaldo, vamos a explicar cómo se realizan los diferentes Jobs empezando por un Job de una máquina virtual, en home, donde pondremos hacer diferentes trabajos, trabajo de Backup, trabajo de replicación, aplicar una política CDP, realizar una Backup copy establecer un plan de failover o realizar una restauración. clicamos en Backup job, puesto que es el que necesitamos para el marco que nos hemos fijado.

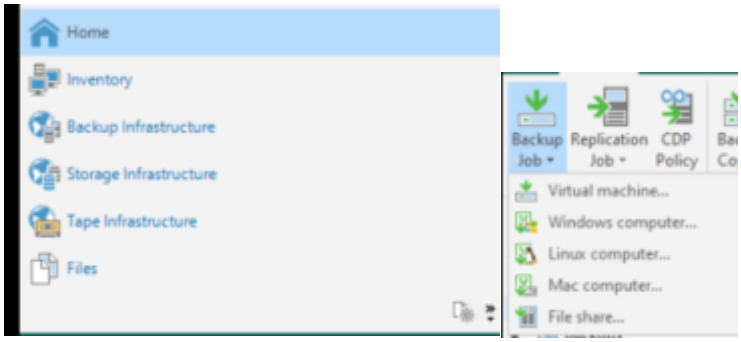

Figura 48. selección del tipo de Backup Job a realizar.

Como vemos nos aparecen diversas opciones de trabajo, a modo de prueba, vamos a realizar un Backup de una máquina virtual y después de un equipo físico de Windows para que veamos las opciones existentes, similitudes y diferencias.

En la ventana que se nos abre, podemos seleccionar el nombre del job, así como una descripción de este.

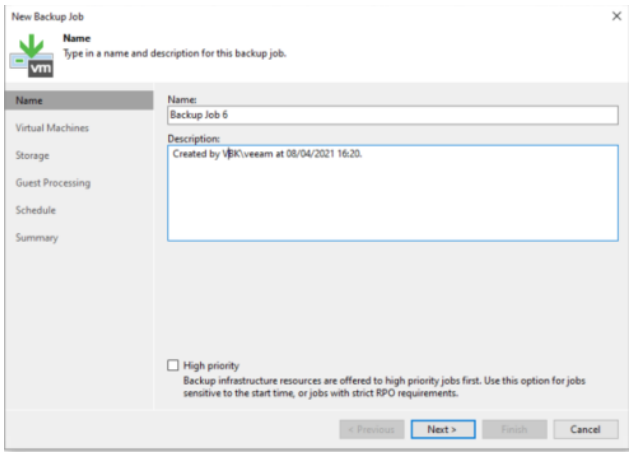

Figura 49. Nombre en nuevo trabajo de copia

Al darle a Next deberemos seleccionar a que maquinas va a realizar el respaldo, es recomendable realizar un Job por Maquina en lugar de agrupar varias, puesto que en caso de fallo podremos identificar fácilmente cual ha sido la que ha fallado.

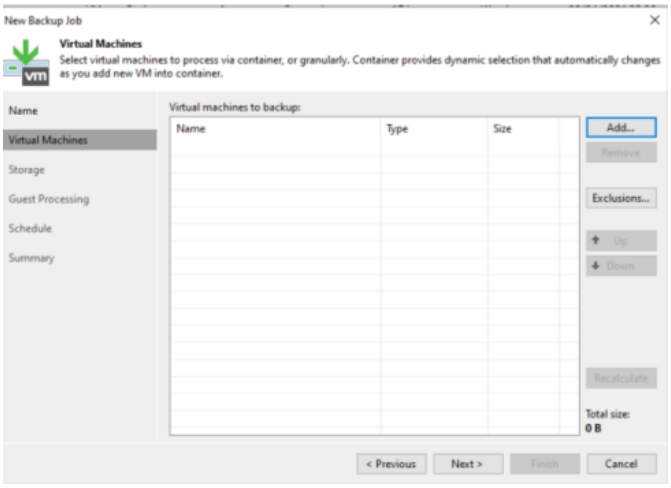

Figura 50. Pantalla de selección de equipo en el que se va a realizar el nuevo trabajo de copia

Al darle al botón de Add, aparecerá un popup con la infraestructura que hayamos agregado y agregaremos una maquina

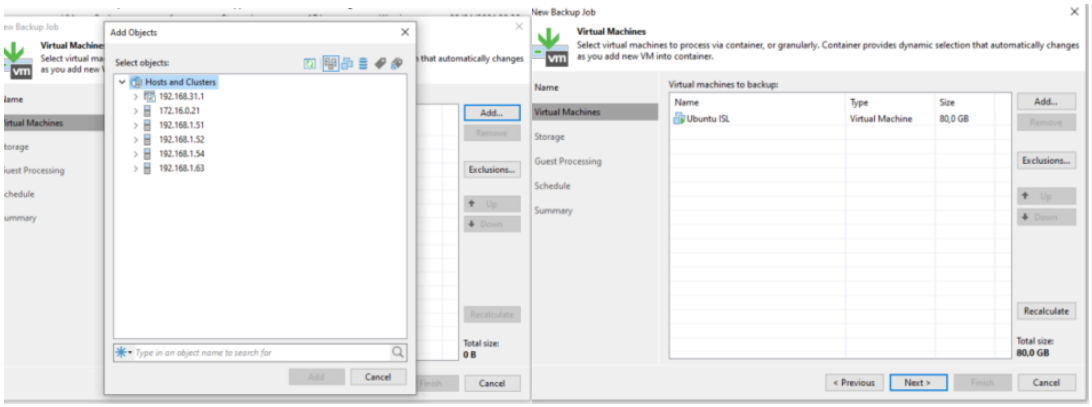

Figura 51. Añadir maquinas al nuevo trabajo.

Al darle a Next, aparecerá las opciones de configuración

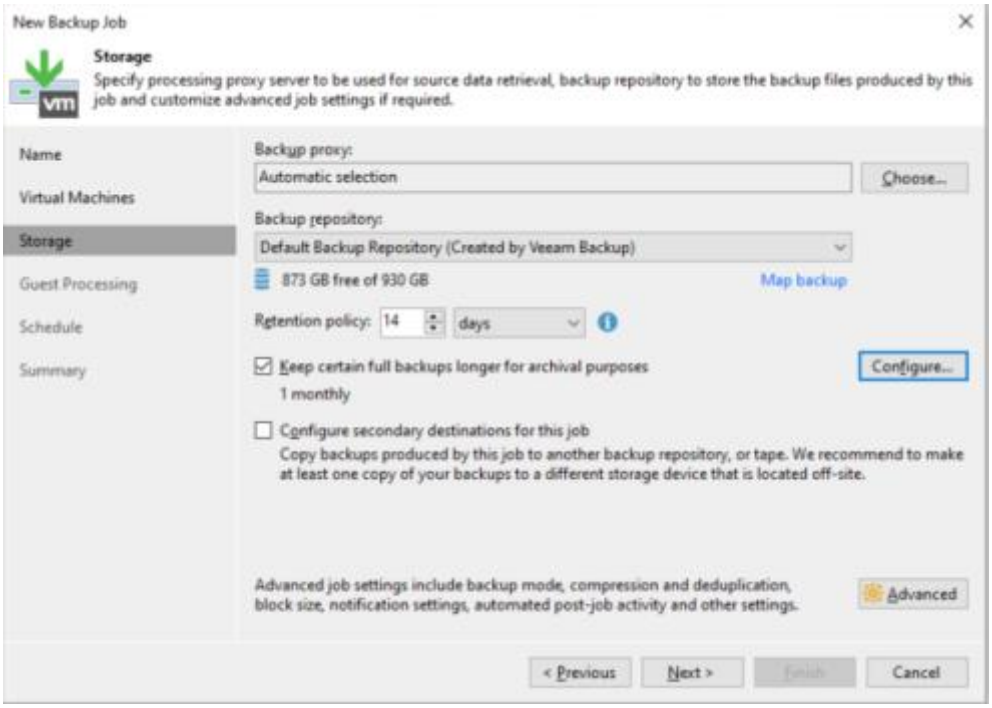

Figura 52. Opciones de configuración del trabajo de copia

Aquí hay varias tareas a realizar, la primera es seleccionar el Backup proxy y el Backup Repository que vamos a utilizar, el Backup proxy si lo dejamos en automático, el server Veeam, seleccionara el óptimo para la infraestructura y con menor carga de trabajo. El Repository por defecto es el disco del propio server. Ahora ya, empezamos a aplicar la política de retención, es decir cuánto tiempo deseamos conservar una copia, hemos fijado 14 días, aunque parece poco y es un mínimo, nos parece suficiente para la casuística planteada, teniendo en cuenta que además hemos marcado la opción de mantener una copia full durante un mes, con lo que tendremos una full de una antigüedad máxima de un mes más 14 días de retención

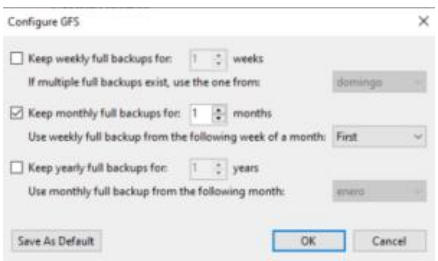

Figura 53. Configuración de la política de retención a largo plazo

Luego seleccionaremos las opciones avanzadas, en la primera opción, la que indica Backup podemos elegir el tipo de Backup a realizar, pudiendo elegir Reverse incremental e Incremental, la opción reverse incremental que es más lenta, es la mejor opción si debemos mantener siempre una última copia full, la manera de realizar esta copia es inyectar los bloques cambiados entre copias, manteniendo la estructura full, y los bloques reemplazados se conservarán en una incremental inversa. De no verse restringidos por la necesidad de mantener una última copia full, la ventana de Backup es menor si escogemos una incremental, nótese, que hemos seleccionado generar una copia sintética full periódicamente los sábados

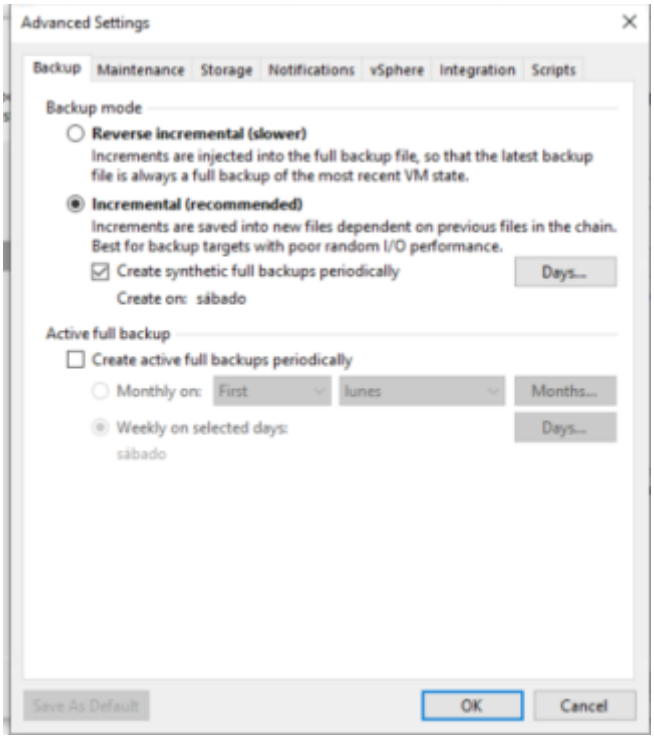

Figura 54. Configuración del tipo de Backup

Si pasamos a la pestaña de mantenimiento, nos permite seleccionar una comprobación periódica del estado de los archivos de copia, así como desfragmentar y compactar las copias full. De estas opciones la más importante obviamente es establecer una periodicidad de la verificación de archivos de Backup.

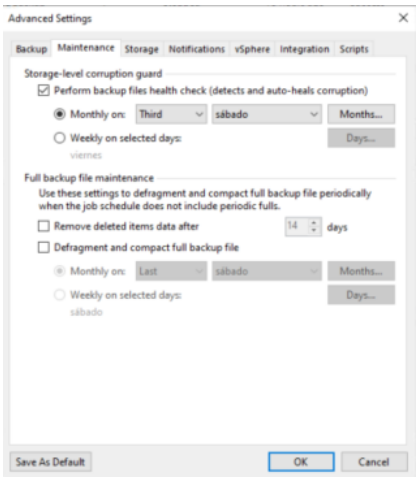

Figura 55. Configuración de la política de retención

La siguiente opción sería la que hace mención al almacenamiento, en ella explica si vamos a aplicar la inline data deduplicacion, el nivel de compresión y un ajuste en función de si los

archivos de Backup, van a estar alojados en el propio servidor, viajaran a través de una Lan o a través de una lan… por último, de esta configuración, señalar la configuración de la encriptación, que cifrará los archivos de Backup, para que no sean accesibles, cumpliendo así con la LOPD y RGPD

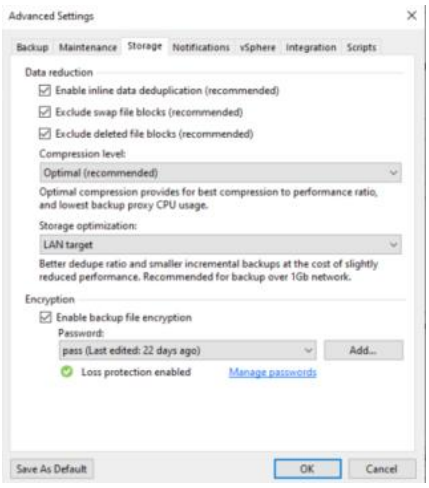

Figura 56.Configuracion optimización del repositorio encriptación

El resto de las opciones quedarían fuera del marco y no aportan valor a este con lo cual las dejaremos por defecto, si se necesita más información de estas se puede acceder a la información que Veeam https://www.veeam.com/documentation-guides-datasheets.html

Ya habríamos configurado toda la parte de almacenamiento y pasaremos a configurar la parte de procesamiento de aplicaciones de la maquina

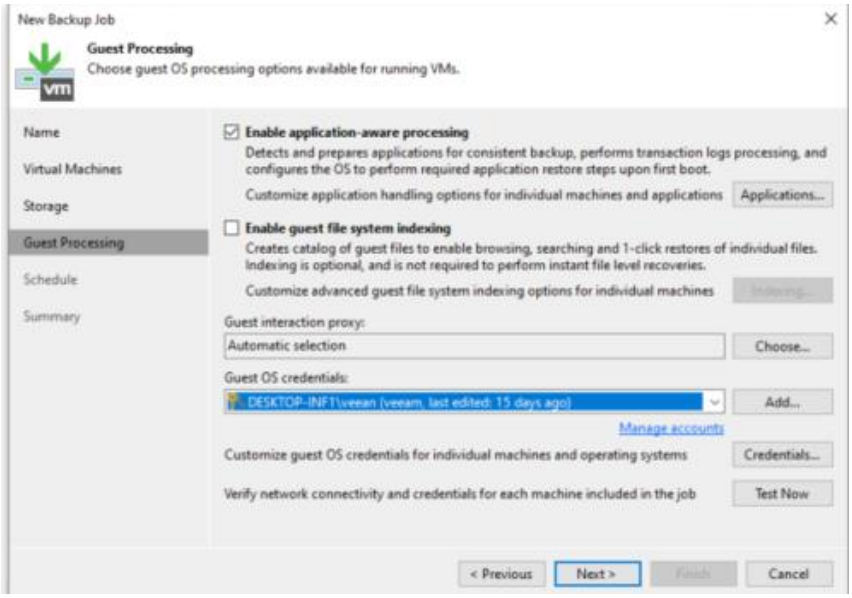

Figura 57. Configuración de procesamiento de aplicaciones

En esta pantalla tenemos os opciones principalmente, vamos a proceder a explicar cada una de estas opciones, siendo la más importante la primera opción Enable application-aware processing, esta opción detecta y prepara la máquina que vamos a respaldar según las aplicaciones que se están ejecutando, es decir al marcar este check veeam server, es capaz de detectar por ejemplo que se está ejecutando en el sistema anfitrión un servicio de SQL y preparar un proceso de log de transacciones veamos que opciones podemos configurar

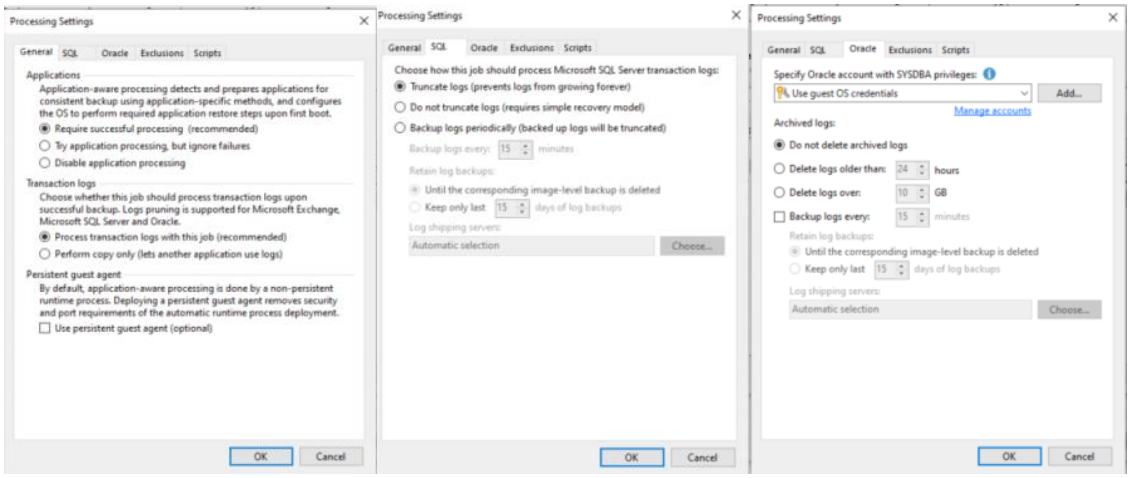

Figura 58. Opciones del procesamiento de aplicaciones

Según el tipo de maquina y de las necesidades realizaremos una configuración u otra, por ejemplo, si queremos evitar que el log de transacciones crezca sin control debemos truncar el log en la opción de SQL, si queremos realizar simplemente una copia de las transacciones lo seleccionaremos en la pestaña general.

Por último, ya, realizaremos una programación del trabajo recurrente.

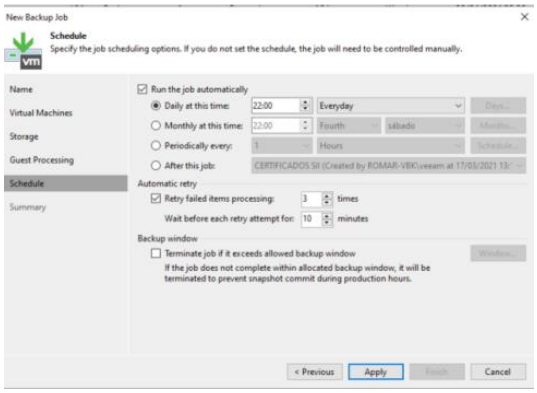

Figura 59. Opciones de programación del trabajo recurrente.

Al programar este trabajo diariamente, lo que en definitiva después de toda la parametrización anterior es que vamos a realizar una copia incremental diaria, que esta copia incremental diaria que se conservaran 14 días, además se realizara además una copia semanal full y que esta se conservará un mes.

Tras realizar el job para una máquina virtual, procederemos a generar el mismo, pero este para una equipo físico con Windows

Lo primero que nos pregunta el asistente es el tipo de equipo, en función de esta selección podremos seleccionar un modo u otro, si escogemos equipo de trabajo o Workstation, solo podremos escoger controlado por el agente en el modelo de copia y si escogemos failover cluster, solo podremos escoger controlado por el Backup server y por último si seleccionamos server podremos escoger ambos modos.

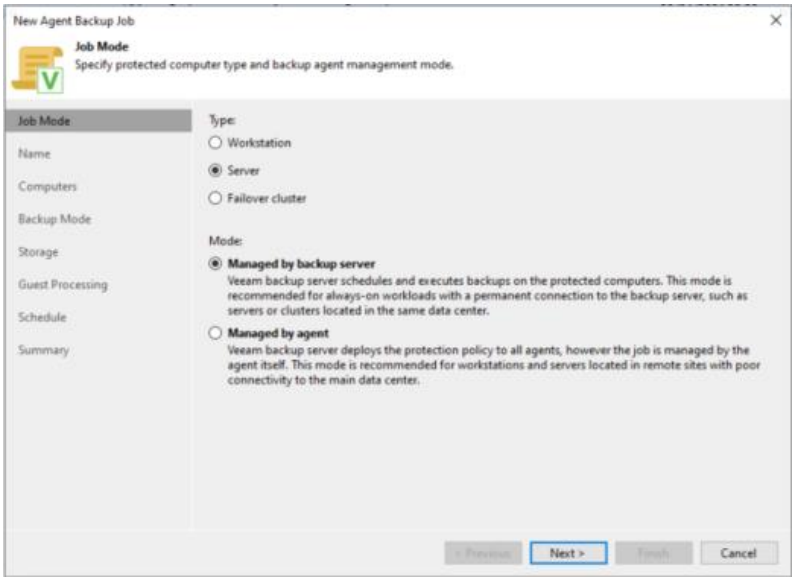

Figura 60. Ejemplo de nuevo Backup de equipo físico

La diferencia entre un modo u otro es seleccionar donde recae la tarea de realizar la copia, lo más recomendable en equipos que están permanente encendidos es seleccionar la opción administrador por el Backup server, ya que se obtienen mejores niveles de rendimiento además de mejor control del trabajo. Por este motivo seleccionaremos este modo para este entorno debido a que suponemos que los equipos a respaldar son servidores que están siempre encendidos.

A partir de este punto, vemos que la configuración es muy parecida al equipo virtual, definiremos nombre y descripción, después añadiremos equipo.

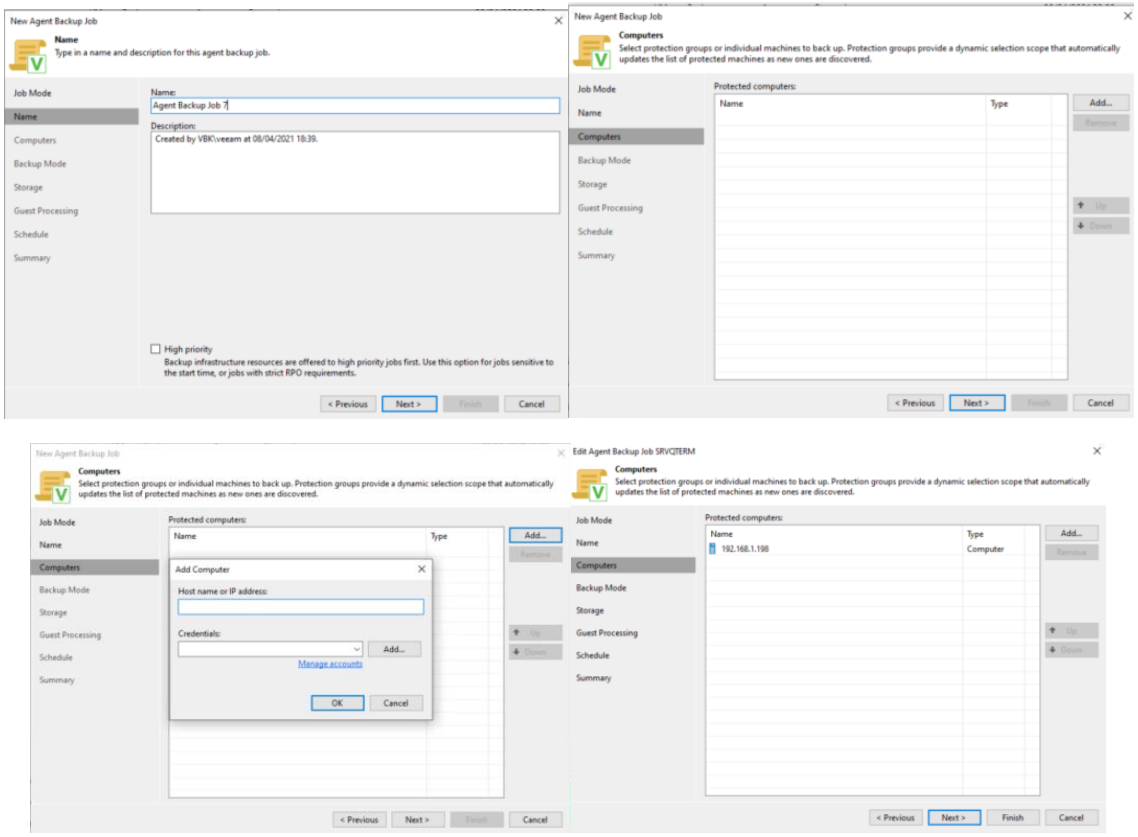

Figura 61. Opciones de adicción de equipo físico al trabajo de Backup

En la manera en la que se va a realizar el Backup, difiere de la opción virtual, al añadir la capacidad de seleccionar si deseamos respaldar la maquina entera (incluyendo o no USB), una unidad de disco o realizar un respaldo de ciertos ficheros.

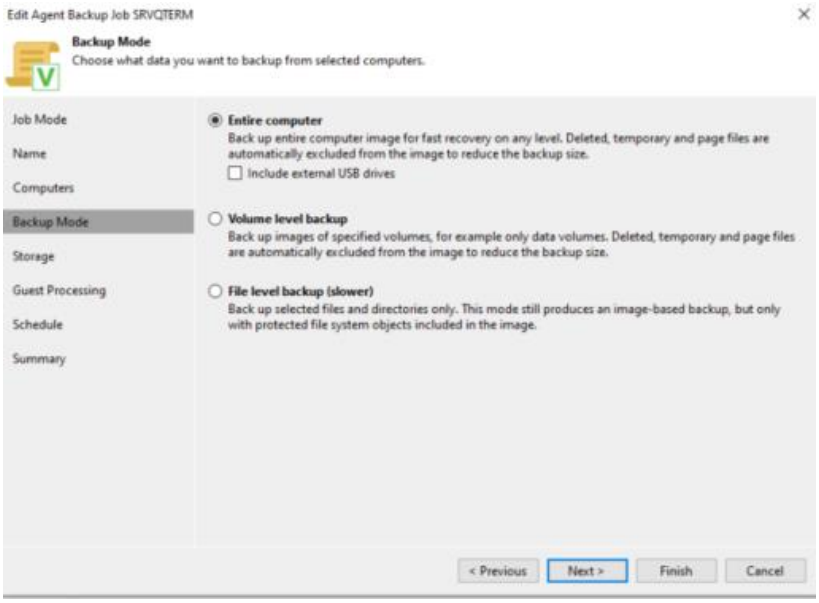

Figura 62. Configuración del tipo de copia

La opción más interesante es la opción de maquina entera, puesto que nos permite arrancar en caso necesario, una máquina virtual con la que poder restablecer el servicio en un RTO mínimo.

Después en las opciones de almacenamiento, son similares a lo que ofrece el job para máquinas virtuales, la gran diferencia es que aquí no existe un proxy ya que el propio agente que se instala en el equipo actúa de proxy es decir el propio equipo físico hace de proxy.

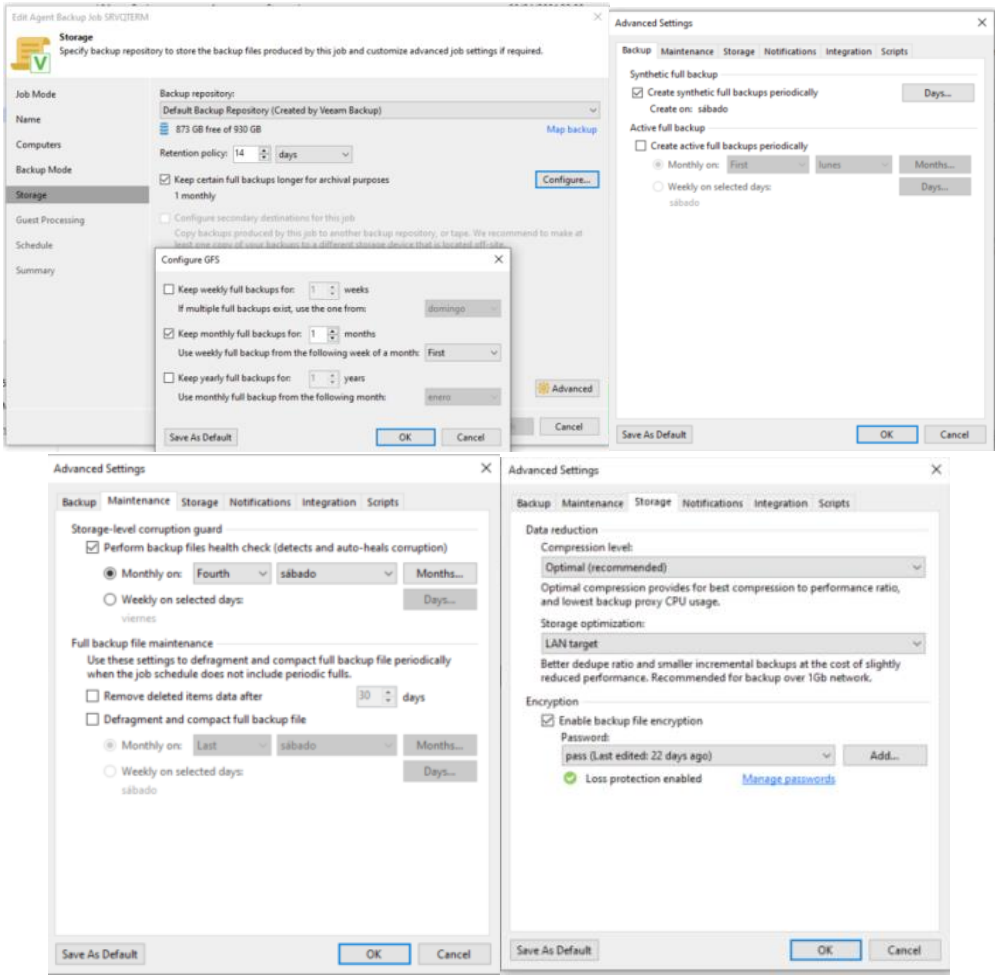

Figura 63. Opciones de configuración para el equipo físico

también son similares la opciones de Guest processing y tarea programada

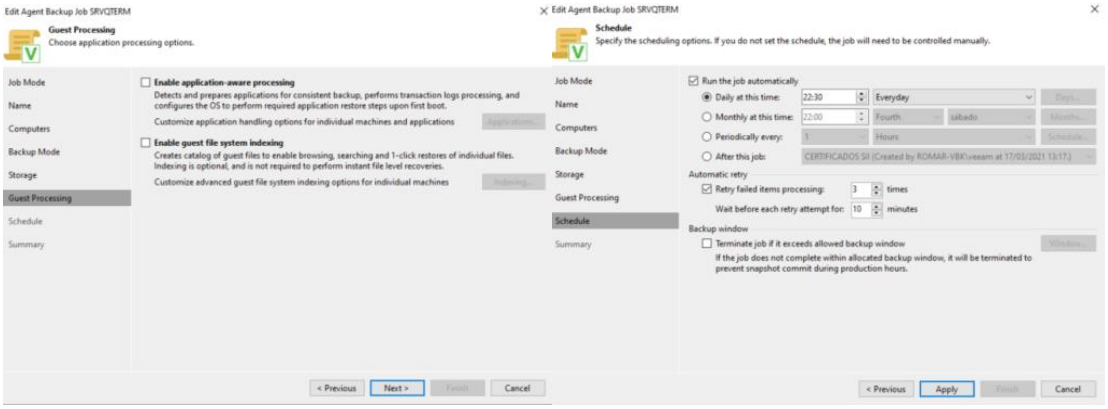

Figura 64. Opciones de guest processing y de tarea programada

Con lo que podemos comprobar que ambos sistemas de copias son similares, de echo hemos programado el mismo tipo de plan de copia para poder realizar una mejor comparativa.

El proceso de copia de archivos de un servidor de fichero es un poco diferente primero seleccionaremos el nombre del trabajo

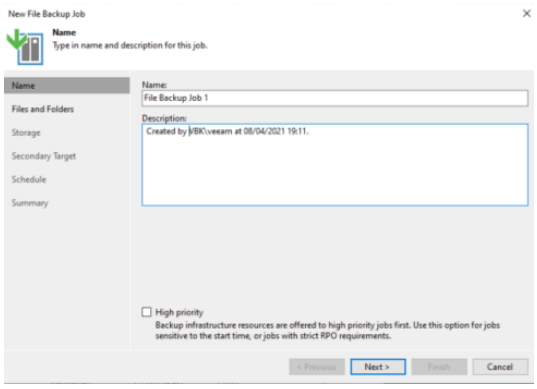

Figura 65. Ejemplo de nuevo trabajo de copia de fichero

Y después indicaremos en que carpeta se encuentran los archivos a respaldar.

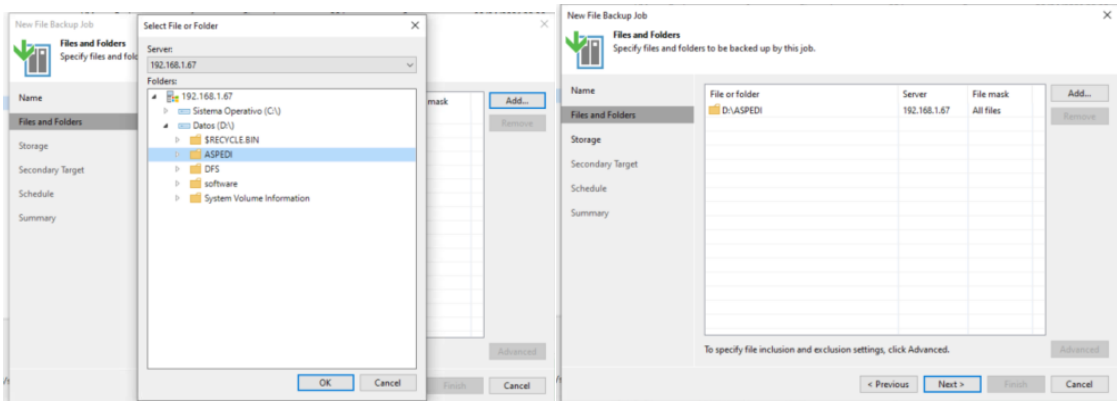

Figura 66. Selección de carpetas y ficheros a respaldar.

Después configuramos el storage de acuerdo con la política de copias

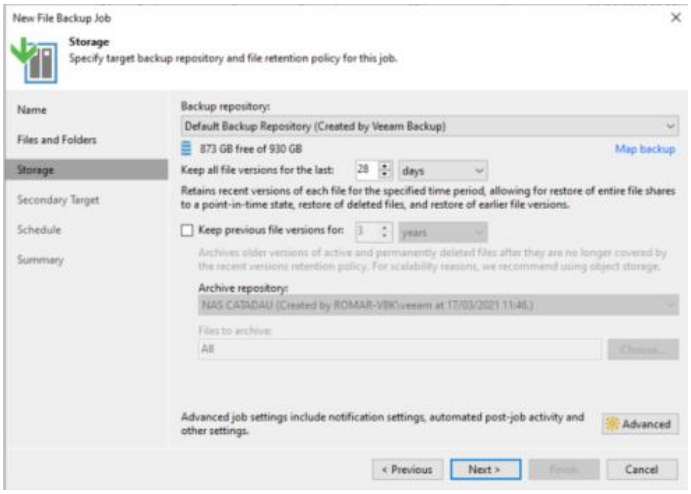

Figura 67. Configuración del almacenamiento y políticas de retención

Y podemos también seleccionar un segundo objetivo adicional.

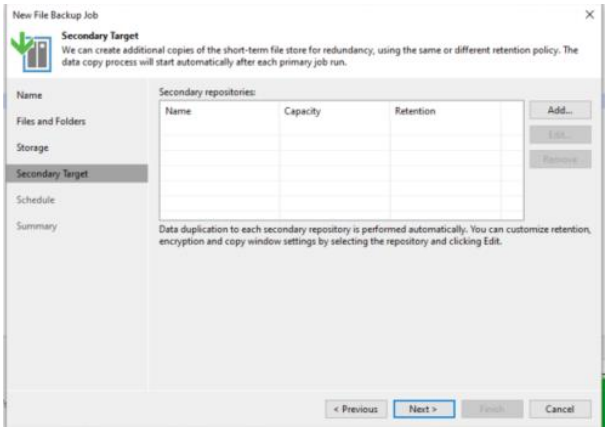

Figura 68. Selección de objetivo adicional.

Por último, escogemos la periodicidad y ya tendríamos configurado un job de copia de ficheros.

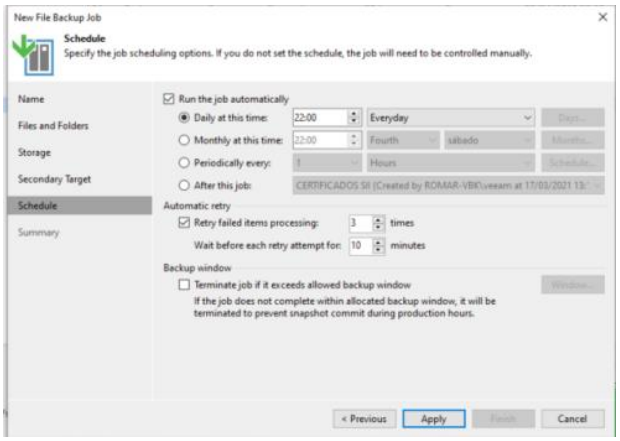

Figura 69. Configuración de la periodicidad del trabajo

Con esto tenemos una breve explicación de que parámetros más interesantes a la hora de realizar los trabajos en el servidor Veeam Backup con lo que ya podríamos realizar pruebas de respaldo y recuperación pero, primero vamos a realizar la parametrización de Cloud, que de acuerdo a costes según la infraestructura del marco, seleccionaremos una opción BaaS mas concretamente nos apoyaremos en la tecnología Scale-out Repository, la cual nos permite en el momento que se publican los ficheros de copia en el repositorio, se desencadena una tarea que permite escalarlo al cloud, es decir envía una copia de este respaldo al cloud, viendo todas la opciones, nos decantaremos por la opción más económica que es el S3 Glacier de Amazon.

Con lo que a nivel de parametrización simplemente conectaremos los repositorios que ya hemos creado con Amazon y de esta manera adquirimos esta funcionalidad.

Para configurar el almacenamiento off-site en el cloud de amazon, debemos registrarnos en amazon AWS y despues generar un vault en AWS S3 Glacier

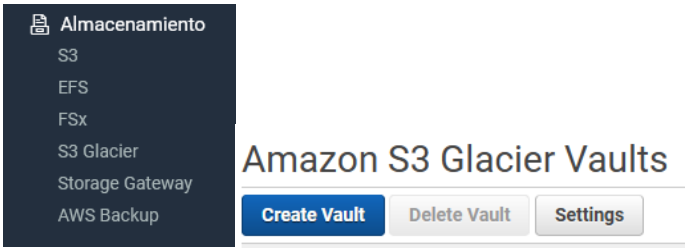

Figura 70. Creación de repositorio en S3 Glacier

Para ello definiremos un nombre y una localizacion, Lo mas cercano a nuestra localizacion posible y si nos encntramos en la EU, para no tener complicaciones con la GDPR, es lo mas recomendable, tambien deveremos indicar su queremos recibir notificaciones de los eventos

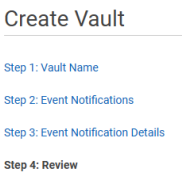

Figura 71.Crear espacio de almacenamiento Vault

Una vez creado el vault, tenemos que ir a nuestro nombre de usuario a la izquierda y al clickar sobre el aparecera el siguiente menu, donde clicaremos en mis credenciales de seguridad

Despues seleccionaremos claves de acceso y generaremos una nueva

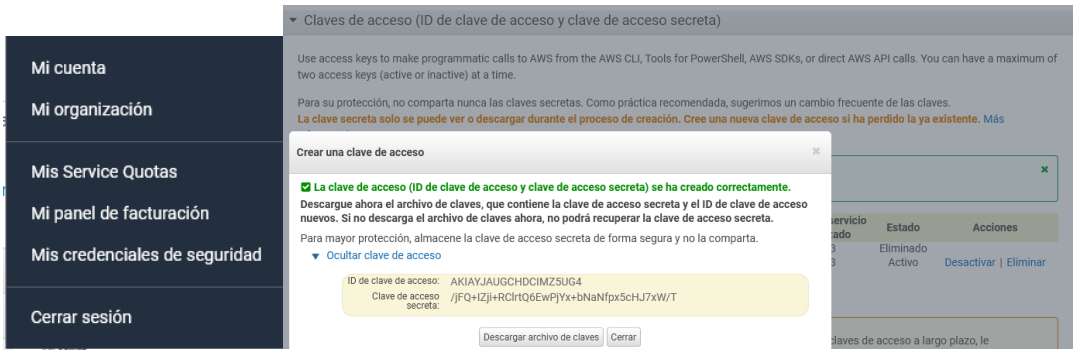

Figura 72. Creación de claves de acceso

Ya disponemos de todo lo necesario para realizar la conexión con S3 Glacier, ahora en la consola del servidor Veeam, vamos al backup infraestructure y en Scale -Out Repositories, añadimos uno nuevo

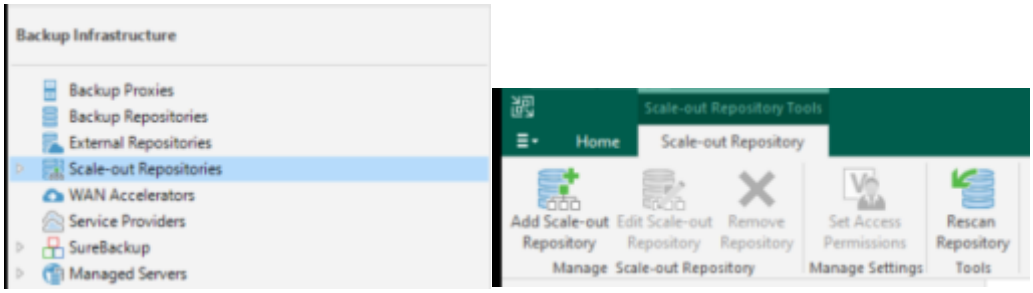

Figura 73.Preparacion del escalado hacia S3 Glacier

Al clicar en add Scale-out Repository aparece la siguiente ventana, donde definiremos el nombre del reposiorio asi como una descripcion.

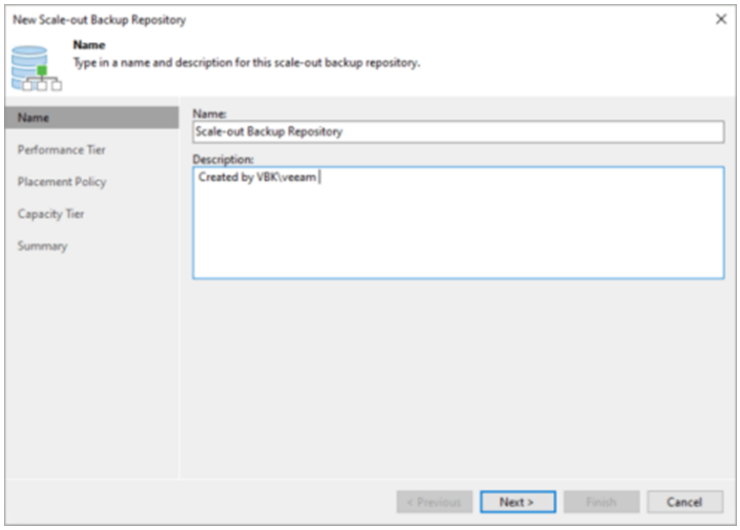

Figura 74. Creación de repositorio escalado.

Seleccionaremos de los repositorios existentes, aquel que cuando reciba los archivos de Backup producirá un duplicado en la nube

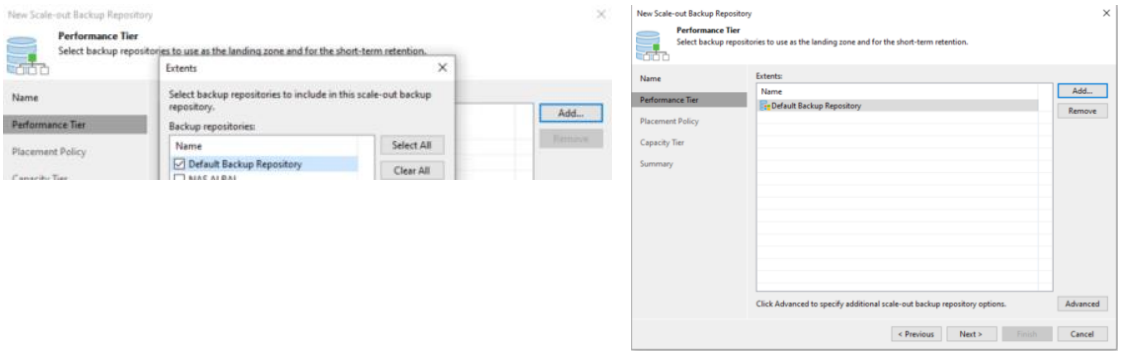

Figura 75. Configuración Performance Tier

En este punto debemos definir la política de ubicación de la copia de, en este caso al buscar realizar un Backup copy debemos indicar data locallity es decir que deseamos mantener la localidad de los datos almacenando los archivos de respaldo que pertenecen a la misma cadena de respaldo juntos

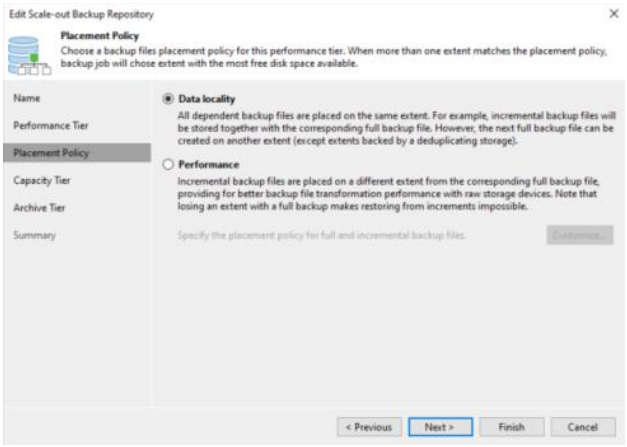

Figura 76. Configuración de la política de almacenamiento

Ahora es en el Capacity Tier donde configuraremos el AWS S3 Glacier y definiremos que se envíe a este Vault en cuanto se creado, lo que a nivel practico se traduce en enviar off-site las copias.

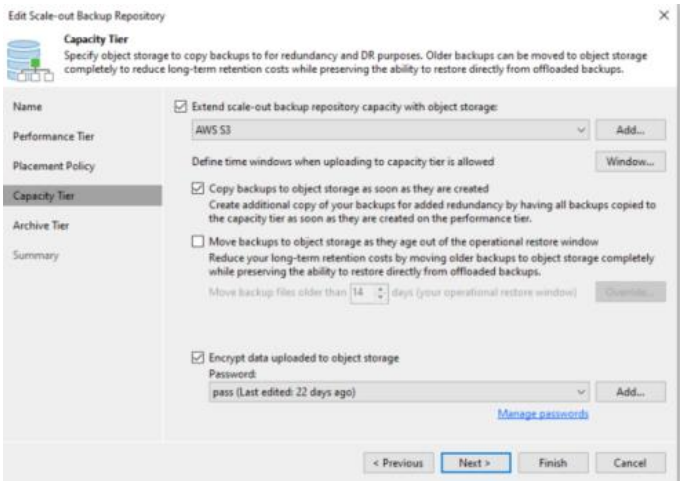

Figura 77.Parametrizacion de Capacity Tier hacia S3 Glacier

Por último configuraremos el Vault directamente de amazon para que todo lo que tenga antigüedad de dos meses, así que en la siguiente opción en el archive tier no marcamos nada puesto que no necesitamos un Archivado.

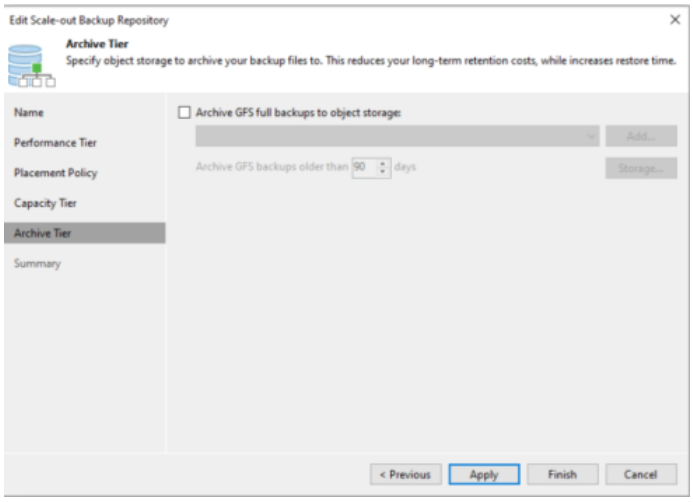

Figura 78. Configuración del Archivado(no es necesario)

Esta configuración, nos va a dotar de toda la capacidad de un sistema BaaS, en cuanto se cree la copia un Backup copy subirá como objeto a S3 Glacier, permitiendo la migración a EC2 o arrancar en caso de desastre en esta infraestructura, así como permitiendo el acceso desde el servidor de Veeam de esta manera, no hace falta afrontar los costes de licenciamiento de otras soluciones vistas con anterioridad pagando simplemente por el almacenamiento consumido y por la descarga cuando sea necesario.

El resultado de un Backup lo veremos a nivel estadístico de la siguiente manera:

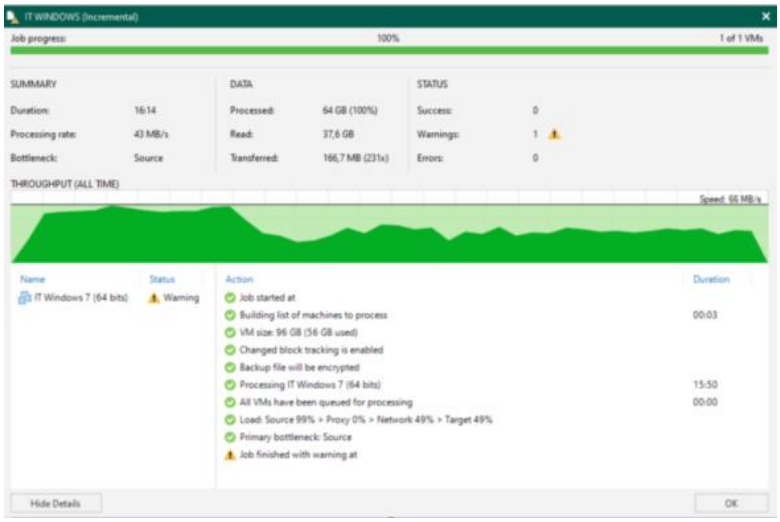

Figura 79.Report resultados de un respaldo

En el veremos los promedios, a nivel de procesed rate de bytes transmitidos, datos leídos etc., un dato importante es que nos indica el consumo sufrido:

Load: Source 99% > Proxy 0% > Network 49% > Target 49%

Esto indica que durante la copia el servidor de Veeam ha estado trabajando casi al 100% y que la carga de red y la carga del repository (Target) ha sido del 49%, con lo que detectamos un cuello de botella en el servidor y vemos la necesidad de definir un proxy que aligere la carga de trabajo del Server.

Con todo lo anteriormente explicado, definiremos todos los trabajos necesarios de acuerdo con el marco de trabajo, realizando un trabajo para cada máquina que según el análisis BIA habíamos detectado que poseía varios datos y sistemas críticos que debían ser salvaguardar en las sedes.

Los servidores de redundancia, no los incluimos en el plan de copias, porque al tener una copia del original es suficiente, recordemos que los equipos a respaldar serán los siguientes:

Sede A

- servidor MSSQL BBDD's Software de nóminas, control de presencia 1 principal y uno secundario con replicación para la redundancia de datos
- Servidor oracle SQL BBDD's ERP
- Servidor MSSQL software de control de producción, toma de datos en planta y cálculo de OEE
- Servidor Mysql para el GMAO que además es utilizado por el inventario y un sistema de Tickets del departamento de tecnologías de la información.
- Servidor ficheros DFS en conjunto a Active Directory

Sede B

- Servidor oracle SQL BBDD's ERP
- Servidor MSSQL software de control de producción, toma de datos en planta y cálculo de OEE
- Servidor ficheros DFS en conjunto a Active Directory

Sede C

- Servidor ficheros DFS en conjunto a Active Directory

Con lo que para cada servidor de los mencionados generaremos un Job, dependiendo de si se trata de un equipo físico o virtual, de acuerdo a la configuración anteriormente descrita, además utilizando la sincronización de carpetas Synology Shared Folder Sync (si dispusiéramos de otro tipo de NAS que no dispusieran de una tecnología similar generaríamos o scripts de copia, o scripts de upload ftp incluso si es necesario podemos generar trabajos duplicados), que nos permitirá crear una copia de los ficheros de una carpeta desde un Servidor NAS Synology de origen a un Servidor NAS Synology remoto, lo bueno de esta sincronización es que permite la sincronización al modificar la carpeta, además de permitir la sincronización a nivel de bloque (que reducirá el ancho de banda necesario) transfiriendo solo datos diferenciales y comprimidos, también tiene un sistema de verificación de errores, de esta manera tendremos una copia funcional en otro medio físico. Si a esto le sumamos que hemos escalado el repositorio al Cloud de Amazon S3 Glacier con Scale-out de acuerdo con lo anteriormente descrito, cumpliríamos con la regla 3-2-1 teniendo un sistema BaaS con posibilidad de convertirlo en DRaaS al menor coste posible. Cumpliendo con el propósito de este proyecto que es conseguir implantar un sistema de Backup de infraestructura hibrida eficiente al menor coste posible.

3.7. Recuperación utilizando de la solución

Existen varios escenarios de recuperación ante desastres, veamos entre las opciones de recuperación que tenemos que es lo que hace cada una:

- **Instant VM Recovery** permite restaurar inmediatamente una VM en un ambiente de producción ejecutando la VM directamente desde el archivo de respaldo. La VM en si misma no es restaurada directamente al Storage de producción, sino que Veeam enciende esta máquina utilizando un host ESXi utilizando los ficheros del repositorio, aunque estos estén de duplicados y comprimidos. con esta función de recuperación se consigue mejorar los objetivos de tiempo de recuperación (RTO), minimizando las interrupciones y a la vez el tiempo de inactividad de las cargas de trabajo de producción.
- **Instant VM Disk Recovery** permite restaurar instantáneamente un disco de VM y publicarlos en el entorno de produccion sin necesidad de recuperar el disco, utilizando los ficheros que se encuentran en el respaldo.
- **Entire VM Recovery** permite recuperar una máquina virtual de un archivo de copia de seguridad en su ubicación original u en otro Hyper-v, VSphere o ESXi.
- **VM files restore** permite recuperar archivos de VM separados (discos virtuales, archivos de configuración, etc.), en el caso VMware la recuperación será de los archivos *.vmx, *. vmxf, *. nvram y *. vmdk en una ubicación definida.
- **Virtual disks restore** permite recuperar un disco duro específico de una máquina virtual desde el archivo de respaldo y adjuntarlo a la máquina virtual original o a una nueva máquina virtual, es decir el device virtual del disco y añadirlo a otra maquina en produccion
- **Disk export** permite recuperar un disco especifico y prepararlo para incorporarlo a una instancia Amazon EC2, Microsoft Azure VM
- **Guest OS file Recovery** permite abrir un browser y recuperar archivos individuales independientemente de si el sistema operativo es Windows, Linux o Mac

Si en lugar de ser un Backup de equipo virtual es un Backup de un equipo fisco, la elección *Instant VM Disk Recovery* no existe, pero aparece la opción de exportar el disco como un disco virtual. vamos a ver las diferentes opciones como se ejecutarían.

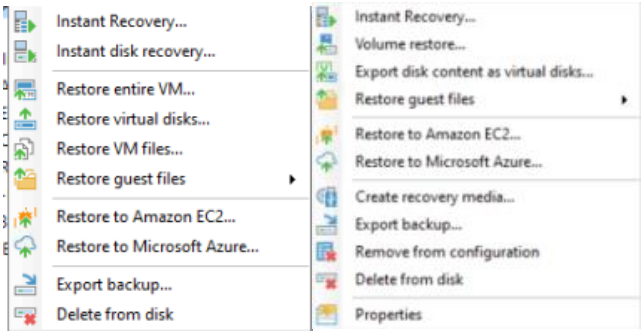

Figura 80. Opciones de recuperación

Probemos con el Instant Recovery, aparece una ventana con la máquina que deseamos restaurar, así como una descripción del punto a restaurar

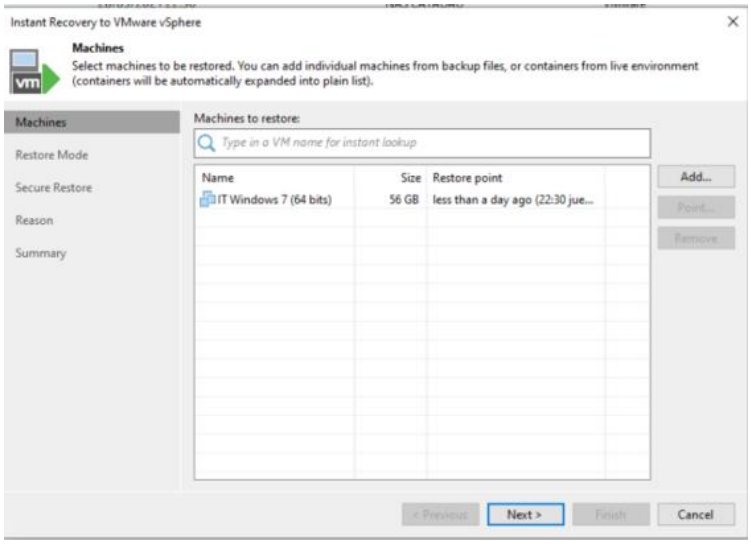

Figura 81. Selección punto de restauración.

Nos da la capacidad de restaurar en el mismo lugar o en otro punto (otro ESXi), si escogemos esta última opción podremos escoger tanto el nombre de la maquina como el equipo donde se va a restaurar.

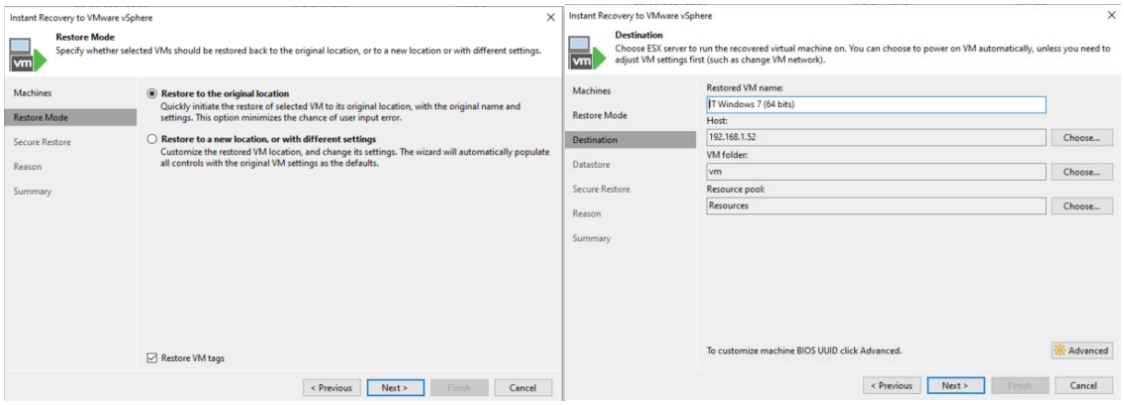

Figura 82. Modo de restauración y destino de restauración

El resto del proceso es idéntico, existe la capacidad de realizar un secure restore que no es mas que programar un escaneo del antivirus antes de montar la maquina y por último nos da la capacidad de anotar la razón de porque se ha realizado la restauración para que esta quede documentada.

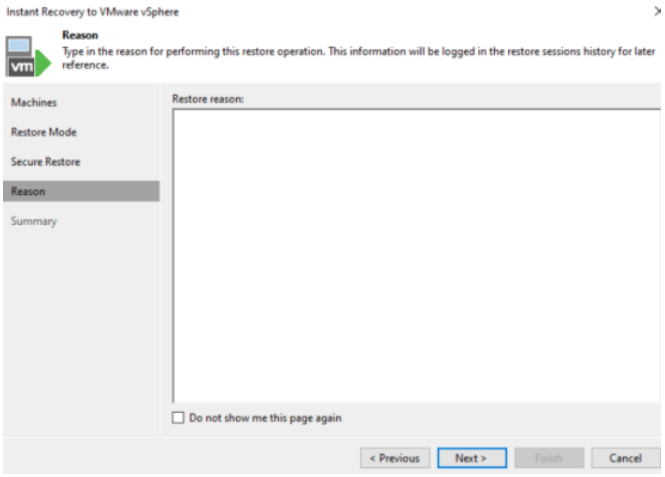

Figura 83. Observaciones y justificación de la restauración

Con Instant VM Disk Recovery, la primera ventana que se abre es la que nos permite seleccionar el punto de restauración entre todos los existentes.

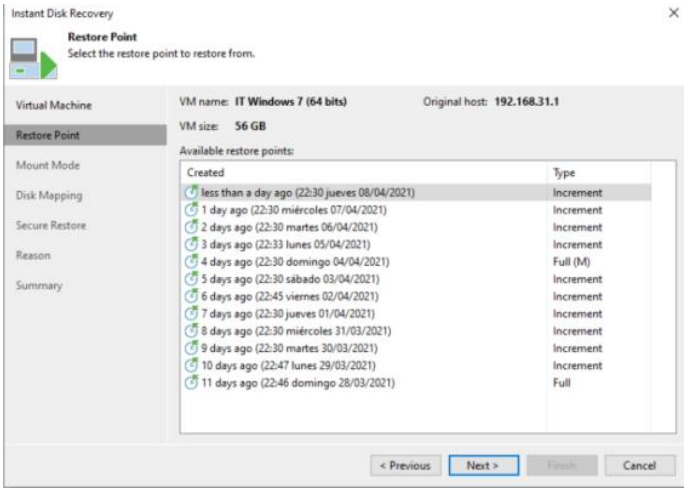

Figura 84. Selección del punto de restauración con VM Disk Recovery

Después seleccionaremos el tipo de montaje si se va a publicar discos recuperados en el entorno de producción o si se van a registrar los discos recuperados como FCD en el entorno de producción.

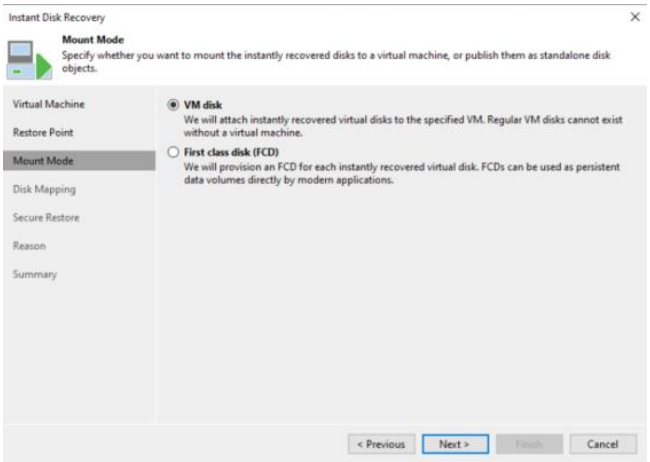

Figura 85. Modo de recuperación

ahora debemos indicar donde se va a restaurar el disco restaurado

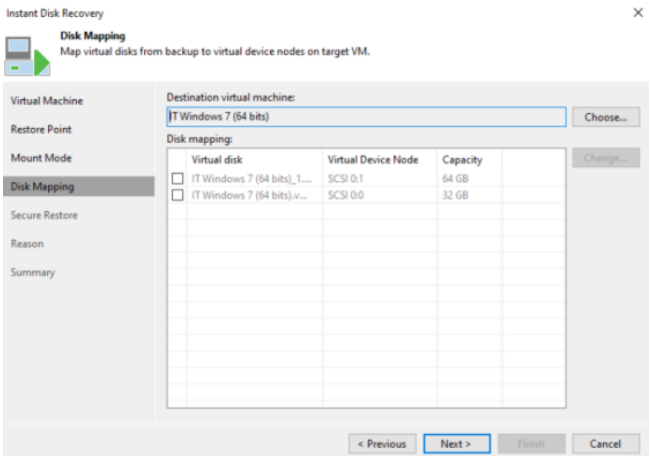

Figura 86. Mapeado de disco virtual

Y las opciones de secure restore y reason son iguales que para el Instant Recovery

Continuemos con el Entire VM Recovery, vemos que aparece la ventana en la que aparece el recurso a restaurar

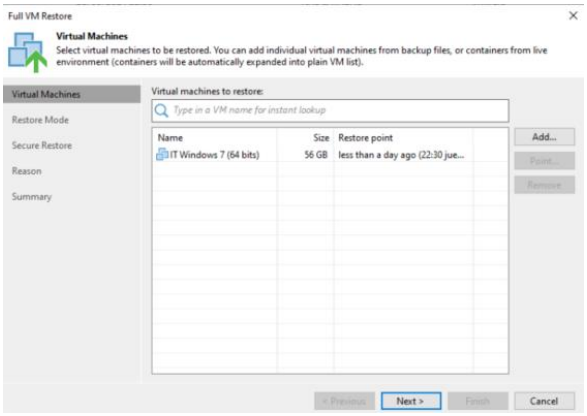

Figura 87. Seleccion de recurso a restaurar

Cuando le damos a siguiente, el programa, nos da la opción de elegir el modo de restauración. Dando nos tres opciones, restaurar en la ubicación original, restaurar en una nueva ubicación o con una configuración diferente y la restauración por etapas

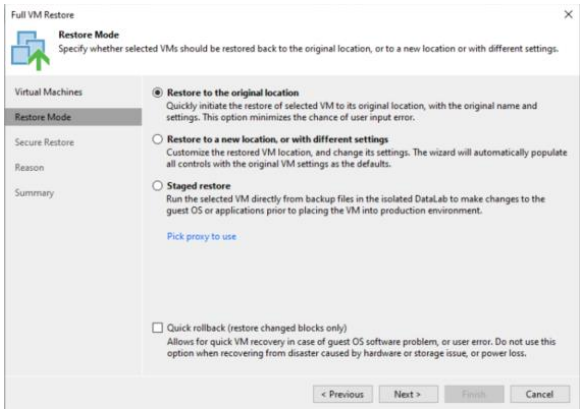

Figura 88. Selección del modo de restauración

Si seleccionamos el staged restore y el restore to a new location, debemos definir un host, un Resource pool, el datastore y el folder. El resto de los puntos son idénticos a los procesos anteriormente descritos en Instant Recovery.

El proceso VM files restore se realizaría de la siguiente manera; en primer lugar, seleccionaríamos el punto de restauración Y después donde vamos a dejar los archivos que componen la máquina virtual.

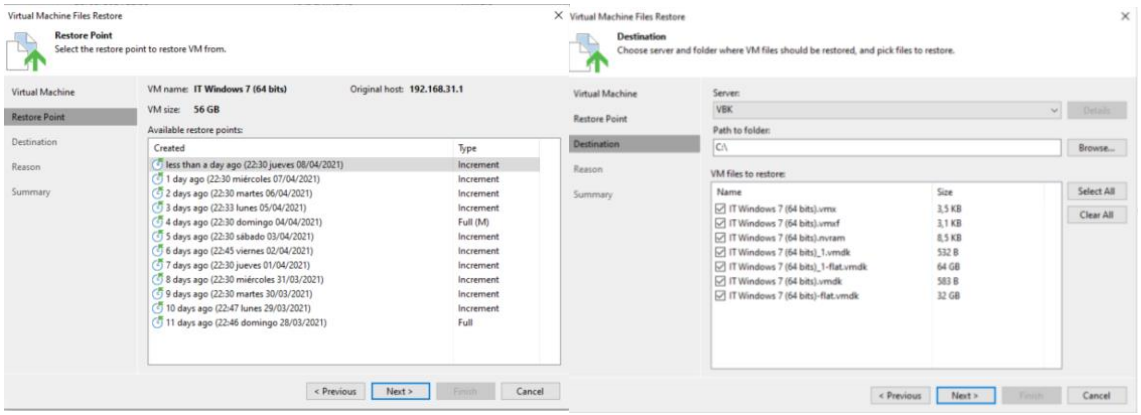

Figura 89.Seleccion punto de restauración y destino de los VM's files restore

En Virtual disks restore escogeremos el punto de restauración y el punto donde mapearemos en la máquina virtual

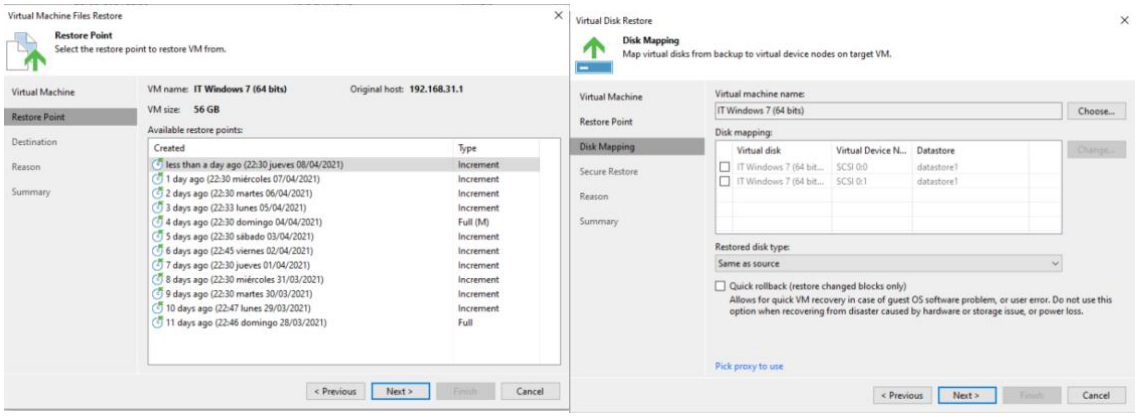

Figura 90. Selección punto de restauración y destino del mapeo de discos en el Virtual Disk restore

En Guest OS file Recovery primero escogemos el punto de restauración y después se nos abrirá un browser que nos permitirá explorar la unidad así como los ítems que se hayan detectado en la copia, si marcamos la opción Enable application-aware processing

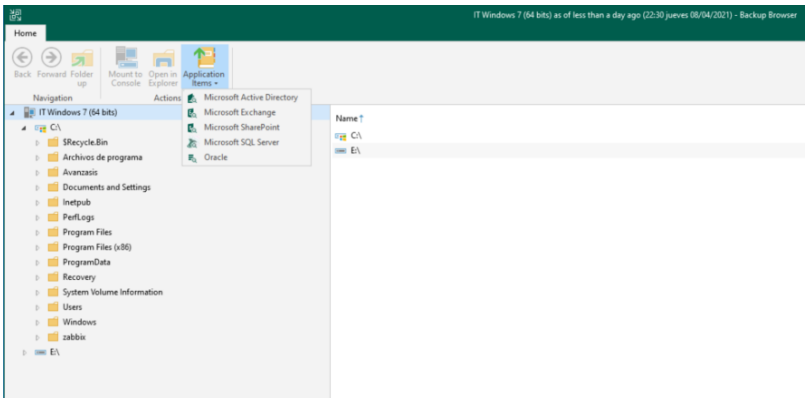

Figura 91. selección de ficheros e items a restaurar

Pudiendo de esta manera restaurar ficheros e ítems.

En caso de restaurar en Amazon EC2 o en Azure veamos que ocurre con Amazon EC2, en primer lugar seleccionamos la cuenta de AWS así como la localización del Data center

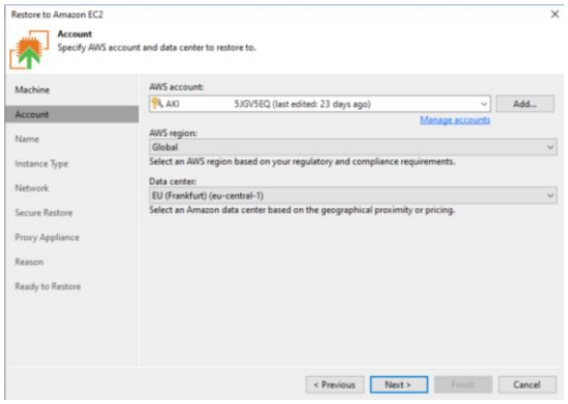

Figura 92.Restaurar a infraestructura hacia Amazon EC2

Después el nombre que va a tener y el tipo de instancia donde definiremos los componentes como CPU y RAM que son necesarios para el correcto funcionamiento de la maquina y que en función de estos el coste será uno u otro, pero nos va proveer de un plan de DRaaS

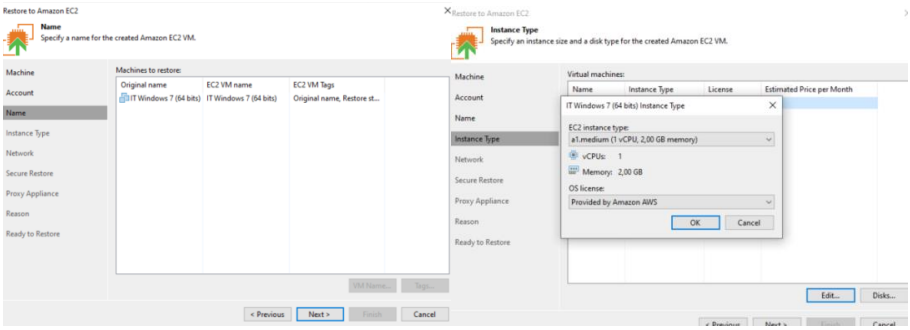

Figura 93. Seleccionar recurso y tipo de instancia donde se va a restaurar

Tras la realización de cualquier restauración obtendremos un pequeño reporte en el cual podremos ver ciertos datos, como son el tiempo de inicialización tiempo de finalización y un log con los problemas si hubiere.

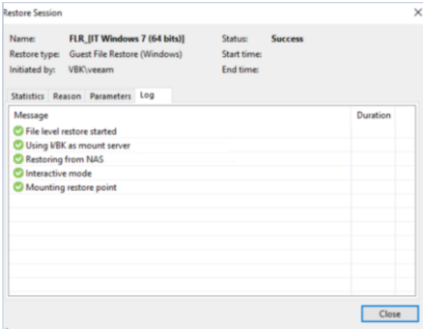

Figura 94.Report resultante restauración.

Ahora disponemos de toda la información necesaria para realizar cada uno de los tipos de restauración en función de la necesidad que se imponga en cada momento escogiendo la mejor solución, puesto que no tiene sentido que necesitemos restaurar un fichero y montemos infraestructura virtual, siendo la ocupación del operador de Backup, realizar la tarea según de la necesidad subyacente.

4. Conclusión

Durante este proyecto, hemos visto la importancia de tener un sistema de copias de seguridad robusto, que ofrezca un reducido RTO, la importancia de una reducida ventana de Backup, gracias al análisis que proporciona el Business Impact Analysis hemos visto cómo podemos detectar aquellas aplicaciones y datos que son críticos para la continuidad de negocio y en definitiva minimizar el impacto de un desastre en la organización.

Por otro lado, se han intentado minimizar los riesgos que nos podemos encontrar durante la implantación de este tipo de proyecto teniendo en cuenta el principio de Pareto aplicado a la gestión de proyectos, es decir que el 20% de los problemas consumen el 80% del tiempo, sin olvidar la normativa vigente que afecta a los sistemas de copias que son la LOPD y la RGPD, sobra decir que ambas son de obligado cumplimiento y cuyo quebranto pueden alcanzar duras sanciones económicas. Al analizar las tecnologías existentes hemos recorrido las ventajas y desventajas de las infraestructuras On-Premises y de las on-cloud, para poder tener claro las necesidades que nos debe satisfacer el software y de esta manera realizar un filtro entre la enorme cantidad de aplicaciones existentes en el mercado, focalizando nuestra atención en aquellas soluciones que poseían una plusvalía y es que para realizar una elección correcta de la solución de software, más allá a de la infraestructura, hemos tenido que profundizar en las tecnologías que se ven involucradas en las copias de seguridad, analizando los tipos de almacenamientos existentes, así como las diferentes tecnologías existentes para la optimización de capacidad de los repositorios en la realización de las copias de seguridad.

Tras lo cual hemos adquirido el conocimiento necesario para poder analizar el mercado existente de soluciones de Backup detectado que a algunas soluciones les faltan madurez claro ejemplo de esto son Urbackup o Duplicati, quedando casi desde el inicio orientadas a ser soluciones para entorno no profesionales o a microempresas. quedándose fuera allí donde la robustez y solidez de la solución debe estar más que contrastada, quizás con el tiempo Urbackup, consiga madurar y crecer de tal manera que termine siendo una solución más profesional, a otras soluciones son demasiado complejas como es el caso de Bacula, de tal manera que se hace necesario contactar el servicio Enterprise para obtener la calidad y el respaldo necesario para una arquitectura empresarial , el problema de la utilización de este software, es que la falta de profesionales con experiencia utilizando la herramienta, hace que contratar un equipo para implantar la solución, pueda irse de presupuesto, no obstante los resultados que se pueden obtener con este software no tiene nada que envidiar a las soluciones de software privativo. Cuando comparábamos los diferentes entornos privativos, nos encontramos con un modo de licenciamiento bastante complejo por parte Commvault, que tiene el peligro de no saber el alcance de la licencia que estas comprado y aunque si bien es cierto que tras contactar con un parner algunas dudas se resolvieron, muchas de ellas no quedaron aclaradas, finalmente estuvimos dudando entre la solución que ofrece Acronis y la que ofrece Veeam, siendo esta última mucho más económica, razón por la que se seleccionó para la parte empírica del proyecto. De la misma manera que analizamos las diferentes soluciones de copias de seguridad, con todo lo aprendido, nos pusimos a analizar las soluciones en Cloud los enfoque existentes BaaS y DRaaS, así como los costes y servicios que ofrecían los diferentes proveedores de esto servicios como AWS, Azure e IBM.

Para alcanzar finalmente el verdadero conocimiento, más allá de lo meramente teórico, establecimos un marco practico y utilizando los conocimientos adquiridos durante la parte teórica del proyecto, así como los obtenidos en las asignaturas que he cursado en la UOC, que me han permitido la implantación empírica de una solución Backup hibrida, aplicando todas las construcciones teóricas. Asimismo, quiero reiterar mi agradecimiento a Mario Prieto Vega por su guía en la elaboración de todo el proyecto

5. Glosario

- **3-2-1 Backup,** regla que surge de la idea de que una solución de copia de seguridad mínima debería incluir tres copias de los datos, incluidas dos copias locales y una copia remota.
- **BaaS,** Backup as a Service o Respaldo como Servicio Se trata de una tecnología que te permite resguardar tus respaldos en la Nube pública o Privada
- **Backup,** consiste en un término en ingles que significa copia de seguridad, respaldo, copia de respaldo o copia de reserva
- **Backup Copy**, de la misma manera que una copia de seguridad es una instancia duplicada, un Backup Copy es una copia de la copia de seguridad.
- **Backup policy,** los procedimientos y reglas de una organización para garantizar que se realicen un número y tipo adecuados de copias de seguridad, incluidas las pruebas frecuentes y adecuadas del proceso para restaurar el sistema de producción original a partir de las copias de seguridad.
- **BIA**, Business Impact Analysis consiste en el análisis de impacto empresarial ante la interrupción de sus operaciones y como puede afectar a la organización.
- **Deduplicacion**, La deduplicacion de datos es un método de compresión que funciona eliminando copias duplicadas de bloques de datos. Permitiendo un uso más eficaz del espacio de almacenamiento y transferencias de archivos más rápidas
- **Disaster Recovery,** consiste en el proceso de recuperación después de un desastre, es decir, restaurar o recrear datos. Uno de los objetivos principales de la creación de copias de seguridad es facilitar una recuperación ante desastres exitosa. Para lograr la máxima eficacia, este proceso debe planificarse con anticipación y auditarse
- **DRaaS,** Disaster Recovery as a Service ofrece servicios de recuperación instantáneo al ejecutar sistemas en un centro de datos externo.
- **Full Backup,** consiste en una copia de seguridad de todos los archivos (seleccionados) del sistema. A diferencia de la imagen de una unidad, esto no incluye las tablas de asignación de archivos, la estructura de las particiones ni los sectores de arranque.
- **Incremental Backup,** consiste en una copia de seguridad que solo contiene los archivos que han cambiado desde la copia de seguridad más reciente (completa o incremental). La ventaja de esto son los tiempos de copia de seguridad más rápidos, ya que solo es necesario guardar los archivos modificados. La desventaja son los tiempos de recuperación más prolongados, ya que es necesario restaurar la última copia de seguridad completa y todas las copias de seguridad incrementales hasta la fecha de la pérdida de datos.
- **LOPD (LOPD-GDD),** Ley Orgánica de Protección de Datos es una ley orgánica española que tenía por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales
- **MAO**, Maximum Acceptable Outage Interrupción máxima aceptable es el período de tiempo durante el cual una recuperación debe hacerse efectiva antes de que una interrupción comprometa la capacidad de una organización.
- **MTD,** Maximum tolerable downtime o el tiempo de inactividad máximo tolerable, especifica el período máximo de tiempo que un proceso determinado puede estar inoperativo antes de que la supervivencia de la organización esté en riesgo.
- **MTPD**, Maximum Tolerable Period of Disruption o período máximo tolerable de interrupción es el tiempo máximo permitido durante el cual los productos o servicios clave de la organización no están disponibles o no pueden entregarse antes de que su impacto se considere inaceptable.

- **RGPD,** Reglamento General de Protección de Datos consiste en el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos
- **RPO,** El Recovery Point Objective, es la cantidad máxima de tiempo desde su última copia de seguridad,
- **RTO,** El Recovery Time Objective es el tiempo que se tarda en restaurar los datos más restablecer los sistemas como si el desastre no se hubiera producido.
- **Synthetic Backup,** o Backup sintético consiste en una copia restaurable que se sintetiza en el servidor de copia de seguridad a partir de una copia de seguridad completa anterior y todas las copias incrementales
- **Ventana de Backup,** o Backup Window es el tiempo necesario para realizar la copia de seguridad
- **Virtual Tape Library (VTL)**, consiste en un dispositivo de almacenamiento que simula ser una biblioteca de cintas para respaldar software, pero que en realidad almacena datos por otros medios.

6. Bibliografia

- RTO and RPO: Understanding Disaster Recovery Times, Eric Siron, 2020, Disponible en: https://www.altaro.com/hyper-v/rto-rpo-disaster-recovery/
- Understanding RPO and RTO, Pierre-Francois Guglielmi, 2019, Disponible en: https://www.rubrik.com/en/blog/technology/19/5/rpo-rto-disaster-recovery
- Backup Retention Policy: Best Practices for IT Admins and Business Owners, Anna, Cybersecurity Expert at Spin Technology, 2021, Disponible en: https://spinbackup.com/blog/backup-retention-policy-best-practices/
- Backup: primera línea de defensa, INCIBE, 2018, Disponible en: https://www.incibe.es/protege-tu-empresa/blog/backup-primera-linea-defensa
- How a Risk Assessment Can Protect Your Data and Your Business, 2019, Disponible en: https://veristor.com/blog/how-a-risk-assessment-can-protect-your-data-and-your-business/
- Risk Impact Assessment in Disaster Recovery: Where to Start, Alex Mayer, 2020, Disponible en: https://www.nakivo.com/blog/risk-impact-assessment-in-disaster-recovery-where-to-start/
- España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, 06 de diciembre de 2018, núm. 294. BOE-A-2018-16673 Disponible online en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
- UE. Reglamento (UE) 2016/679 del parlamento europeo y del consejo, 27 de abril de 2016, Disponible online en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 y https://www.boe.es/doue/2016/119/L00001-00088.pdf
- GDPR implications on data backup and disaster recovery, disponible online https://www.backup-systems.co.uk/blog/6-gdpr-implications-on-data-backup-and-disaster-recovery
- ¿Va a causar GDPR un apocalipsis para el Backup?, Iván Abad, Technical Services Manager de Commvault, 2018, Disponible en: https://www.computing.es/seguridad/opinion/1106103002501/causar-gdpr-apocalipsis-backup.1.html
- GDPR: Does the Right to Erasure Include Backups?, David Froud, Disponible en: https://www.davidfroud.com/does-right-to-erasure-include-backups/
- What is On-Premises or On-Prem Everything You Should Know, Shivang, Disponible en: https://www.8bitmen.com/what-is-on-premises-or-on-prem-everything-you-should-know/
- On-Prem vs. Colocation vs. Cloud: Making the Best Decision, Blair Felter,2019, Disponible en: https://www.vxchnge.com/blog/on-premise-vs.-colocation
- Which is better - Cloud or On-Premise Backup, Disponible en: https://mybusiness.singtel.com/techblog/which-better-cloud-or-premise-backup
- ON-PREMISES BACKUP FOR CLOUD DATA AND CLOUD INFRASTRUCTURE PROTECTION, On-Premises Backup for cloud data and cloud infrastructure protection, Mitch Tulloch, 2019, Disponible en: https://techgenix.com/on-premises-backup/
- Types of Backup: SaaS Backup vs On-Premises Backup, Michael Schneider, 2020, Disponible en: https://www.cloudally.com/blog/types-of-backup-saas-cloud-backup-vs-on-premises-backup/
- Cloud vs. on-Premises backup: Why a cloud-based solution has significant advantages, Mark Pendergrast,2019, Disponible en: https://www.skykick.com/blog/on-premises-vs-cloud-backup-why-a-cloud-based-solution-has-significant-advantages/

- What type of Storage Media should I be using?, Macrium Software, 2019, Disponible en: https://blog.macrium.com/what-type-of-storage-media-should-i-be-using-e3ef2eb75152
- How to Backup Your Data - Best Practices, Disponible en: http://www.data-master.com/BackupMediaTypes.html
- Data Backup Devices, Swapna Naraharisetty,2021, Disponible en: https://www.2brightsparks.com/resources/articles/data-backup-devices.html
- What is data deduplication?, Disponible en: https://www.netapp.com/data-management/what-is-data-deduplication/
- Introducción a la deduplicacion de datos, 2017, Disponible en: https://docs.microsoft.com/es-es/windows-server/storage/data-deduplication/overview
- 4 Reasons why quality deduplication matters for backup, TechGenix Editorial Team, 2018, Disponible en: https://techgenix.com/deduplication-backups/
- The importance of data backup policies and what to include, Paul Kirvan; Colm Keegan, 2020, Disponible en: https://searchdatabackup.techtarget.com/tip/The-importance-of-backup-policies
- The National Cybersecurity Societ, 2019, Disponible en: https://nationalcybersecuritysociety.org/wp-content/uploads/2019/10/Backup-Policy-Template.pdf
- Data Backup Policy, wofford.edu, 2007, Disponible en: https://dept.wofford.edu/it/Data%20Backup%20Policy.pdf
- Bacula Documentation, Disponible en: https://www.bacula.org/documentation/
- Bacula lat, Site en castellano, Disponible en: https://www.bacula.lat
- Enterprise Edition Comparison with Community Version, Disponible en: https://www.baculasystems.com/corporate-data-backup-software-solutions/professional-backup-software/enterprise-community-comparison/
- Tarifs Bacula,2021, Disponible en: https://www.commeo.eu/tarifs-bacula/
- Urbackup Administration Manual, 2019, Disponible en: https://www.urbackup.org/administration_manual.html
- Usando UrBackup Para Copias de Seguridad,202, Disponible en: https://todoservidores.web.ve/usando-urbackup-para-copias-de-seguridad/
- Duplicati Site, Disponible en: https://www.duplicati.com/
- Duplicati: Conoce esta herramienta para realizar copias de seguridad fácilmente, Javier Ceballos Fernández, 2017, Disponible en: https://www.redeszone.net/2017/04/22/duplicati-conoce-esta-herramienta-realizar-copias-seguridad-facilmente/
- Block-level Deduplication, Compression, and Encrypted Backup With Duplicati, Skip Levens, 2020, Disponible en: https://www.backblaze.com/blog/duplicati-backups-cloud-storage/
- Acronis Site, Disponible en: https://www.acronis.com/es-es/products/backup/
- Acronis Cyber Backup 12.5 user guide, Disponible en: https://dl.acronis.com/u/pdf/AcronisCyberBackup_12.5_userguide_es-ES.pdf
- Acronis Cyber Backup Review, Daniel Brame,2019, Disponible en: https://www.pcmag.com/reviews/acronis-backup
- Acronis Cyber Backup Ratings Overview, Disponible en: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions/vendor/acronis/product/acronis-backup

- Commvault Site, Disponible en: https://www.commvault.com/es-es/complete-data-protection/backup-recovery/
- Commvault Backup and Recovery Ratings Overview, Disponible en: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions/vendor/commvault/product/commvault-complete-backup-and-recovery
- ¿Está ya cansado de la complejidad de Commvault? Ventajas de Veeam sobre Commvault, 2021,Disponible en: https://go.veeam.com/rs/870-LBG-312/images/wp_the_benefits_of_Veeam_over_Commvault_es.pdf?v20210408
- CommVault, Licensinng Sales Guide, Disponible en: https://www.adn.de/fileadmin/user_upload/Hersteller/CommVault/Datenblaetter/Commvault_Booklet_-_Printable_PDF_Final__2_.pdf
- CommVault Price list, Disponible en: https://www.freeitdata.com/wp-content/uploads/2018/09/3407-List-with-Disc.pdf
- Veeam: Veeam se consolida como líder en el último cuadrante de Gartner en la sección de soluciones de Data Center Backup y Recovery, 2019, Disponible en: https://www.jorgedelacruz.es/2019/10/14/veeam-veeam-se-consolida-como-lider-en-el-ultimo-cuadrante-de-gartner-en-la-seccion-de-soluciones-de-data-center-backup-y-recovery/
- Veeam: Como funciona Instant VM Recovery (vSphere), Patricio cerda, Disponible en: https://patriciocerda.com/veeam-como-funciona-instant-vm-recovery-vsphere/
- Veeam Backup and Replication – Métodos de Backup y políticas de retención, Patricio cerda, Disponible en: https://patriciocerda.com/veeam-backup-and-replication-metodos-de-backup-y-politicas-de-retencion/
- What Is Backup as a Service?, Disponible en: https://info.cloudcarib.com/blog/what-is-backup-as-a-service
- Backup as a Service (BaaS), 2020, Disponible en: https://documentation.commvault.com/commvault/v11/article?p=117329.htm
- Guía de DRaaS, Disaster Recovery as a Service, Ángel Eulises Ortiz,2020, Disponible en: https://www.hostdime.com.pe/blog/guia-de-draas-disaster-recovery-as-a-service-recuperacion-de-desastres-como-servicio/
- Disaster Recovery as a Service (DRaaS), Juan Cristóbal Sanchez,2021, Disponible en: https://blog.aitana.es/2021/02/02/disaster-recovery-as-a-service-draas/
- BaaS vs DRaaS: What are the differences?, Martin Tang,2020, Disponible en: https://www.exabytes.cloud/blog/baas-vs-draas-differences/
- Backup vs. Disaster Recovery as a Service: Which Is Better for You and Why?,2020, Disponible en: https://www.volico.com/backup-vs-draas-which-is-better-for-you-and-why/
- Precios de Amazon S3, 2021 Disponible en: https://aws.amazon.com/es/s3/pricing/
- Precios de Amazon S3 Glacier, 2021 Disponible en: https://aws.amazon.com/es/glacier/pricing/
- Precios de los blobs en bloques, 2021, Disponible en: https://azure.microsoft.com/es-es/pricing/details/storage/blobs/
- Precios de IBM Cloud Object Storage, 2021, Disponible en: https://cloud.ibm.com/objectstorage/create#pricing
- UE. Anexo I, Definición de una PYME, Reglamento (UE) N.º 651/2014, Pag 70, 2014, Disponible Online en: https://www.boe.es/doue/2014/187/L00001-00078.pdf
- Helpcenter Veeam, Disponible en: https://helpcenter.veeam.com/docs/backup/vsphere/overview.html?ver=110