CLASIFICACIÓN DE LA INFORMACIÓN DIGITAL INSTITUCIONAL Y REDISEÑO DEL SISTEMA DE COPIAS DE RESPALDO DE LA INFORMACIÓN QUE SE CONSERVA EN EL CENTRO DE DATOS DE LA UNIVERSIDAD PONTIFICIA BOLIVARIANA, SECCIONAL BUCARAMANGA

DANITZA STEFFANY AISLANT PORRAS

000334091

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2021

CLASIFICACIÓN DE LA INFORMACIÓN DIGITAL INSTITUCIONAL Y REDISEÑO DEL SISTEMA DE COPIAS DE RESPALDO DE LA INFORMACIÓN QUE SE CONSERVA EN EL CENTRO DE DATOS DE LA UNIVERSIDAD PONTIFICIA BOLIVARIANA, SECCIONAL BUCARAMANGA

DANITZA STEFFANY AISLANT PORRAS

000334091

Documento presentado como plan de trabajo de la práctica empresarial

DOCENTE SUPERVISOR

JOHANNA MARCELA SUÁREZ PEDRAZA

SUPERVISOR EMPRESARIAL

ARELIS GÓMEZ NOVA

ZAIRA YINETH HERNÁNDEZ RAMÍREZ

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2021

CONTENIDO

1 RESUMEN GENERAL DE TRABAJO DE GRADO

TÍTULO: Clasificación de la información digital institucional y rediseño del sistema de copias de respaldo de la información que se conserva en el centro de datos de la Universidad Pontificia Bolivariana, Seccional Bucaramanga

AUTOR(ES): Danitza Steffany Aislant Porras

PROGRAMA: Facultad de Ingeniería de Sistemas e Informática

DIRECTOR(A): Johanna Marcela Suárez Pedraza

RESUMEN

El presente documento evidencia el resultado de un plan de prácticas que tenía como objetivo el desarrollo del proyecto planteado por el Centro de Tecnología de Información y comunicaciones (CTIC) de la Universidad Pontificia Bolivariana, Seccional Bucaramanga, el cual se basó en una nueva propuesta de rediseño del sistema de copias de respaldo para la información digital que se maneja en la Universidad. Para el desarrollo de este proyecto se tuvieron en cuenta diversas actividades enfocadas a la automatización y optimización de las copias de respaldo, las cuales fueron tomadas como fases de una metodología para ir siguiendo durante este desarrollo. Por otro lado, la información necesaria para el desarrollo del proyecto fue dada y gestionada por el área del CTIC, es decir, se contó con una supervisión durante todo el proceso del proyecto. El resultado obtenido en el desarrollo de las prácticas como se había planteado fue la entrega de una nueva propuesta de rediseño del sistema de copias de respaldo para la información digital teniendo en cuenta los parámetros necesarios para automatizar y optimizar la información utilizada por la universidad.

PALABRAS CLAVE:

Copia de respaldo - TRD - Política de retención - Veeam Backup & Replication

2 GENERAL SUMMARY OF WORK OF GRADE

TITLE: CLASSIFICATION OF THE INSTITUTIONAL DIGITAL INFORMATION AND REDESIGN OF THE SYSTEM OF BACKUPS OF THE INFORMATION KEPT IN THE DATA CENTER OF THE UNIVERSITY PONTIFICAL BOLIVARIANA, BRANCH BUCARAMANGA

AUTHOR(S): Danitza Steffany Aislant Porras

FACULTY: Facultad de Ingeniería de Sistemas e Informática

DIRECTOR: Johanna Marcela Suárez Pedraza

ABSTRACT

This document evidences the result of an internship plan that aimed to develop the project proposed by the Center for Information and Communications Technology (CTIC) of the University Pontifical Bolivariana, Branch Bucaramanga, which was based on a new proposal for redesign of the backup system for digital information that is handled at the University. For the development of this Project, various activities focused on the automation and optimization of backups were taken into account, which were taken as phases of a methodology to be followed during this development. On the other hand, the information necessary for the development of the project was given and managed by the CTIC area, that is, there was supervision throughout the project process. The result obtained in the development of the practices as had been proposed was the delivery of a new proposal for the redesign of the backup system for digital information, taking into account the parameters necessary to automate and optimize the information used by the university.

KEYWORDS:

Backup - TRD - Retention Policy - Veeam Backup & Replication

3 INTRODUCCIÓN

En la actualidad, las copias de respaldo son un instrumento fundamental para el aseguramiento de la información de forma física o digital. En el caso de las entidades (empresas o instituciones) las cuales gracias a los avances tecnológicos manejan en este momento en su mayoría información digital, se observa que las copias de respaldo son un requisito para ellas, pues contar con un sistema de copias de respaldo permite a la entidad recuperar su información en caso de pérdida.

En el caso específico de la institución “Universidad Pontificia Bolivariana, Seccional Bucaramanga” se observa que, si se cuenta con un sistema de copias de respaldo, no obstante, este sistema no se está empleando de la mejor manera, pues se están haciendo copias de respaldo a información que podría prescindir de ella o, por otro lado, no se cuenta con parámetros específicos para realizar de manera ordenada y completa las copias de respaldo. Por esta razón se propone el rediseño del sistema de copias de respaldo de la información que se maneja en el centro de datos de la Universidad Pontificia Bolivariana, Seccional Bucaramanga.

4 GLOSARIO

4.1 Copia de respaldo: También conocida como copia de seguridad o Backup, es una copia que se realiza a información en forma física o digital con el fin de contar con un medio de recuperación en caso de pérdida.

4.2 Tabla de retención documental (TRD): Es un documento donde se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos.

4.3 Política de retención: Es un documento en el cual se describe la administración de los datos desde su creación hasta su eliminación.

4.4 Veeam Backup & Replication: Es el software que utiliza la Universidad Pontificia Bolivariana, Seccional Bucaramanga para la automatización de las copias de respaldo.

5 GENERALIDADES DE LA EMPRESA

La Universidad Pontificia Bolivariana es una institución creada por la iglesia católica, perteneciente a la Arquidiócesis de Medellín. Fundada el 15 de septiembre de 1936 bajo el nombre de Universidad Católica Bolivariana, siguiente a esto, en 1945 recibió el Sello Pontificio y cambió su denominación por la actual. La institución cuenta con 4 campus ubicados en Medellín como sede central, Bucaramanga, Montería y Palmira. [1]

Tiene como misión la formación integral de las personas que la constituyen, mediante la evangelización de la cultura, la búsqueda constante de la verdad en los procesos de docencia, investigación, proyección social y la reafirmación de los valores desde el humanismo cristiano, para el bien de la sociedad. Por otro lado, la Universidad Pontificia Bolivariana tiene como visión ser una institución de excelencia educativa en la formación de las personas sin dejar a un lado su ideología católica, para así ayudar al servicio del país con liderazgo ético, científico, empresarial y social. [1]

En este caso, las prácticas empresariales se desarrollarán en la sede de Bucaramanga con dirección en el campus Universitario Km 7 vía Piedecuesta. Teléfono (+57 7 6796220) y correo electrónico (info@upb.edu.co). [1]

5.1 Organización de la empresa

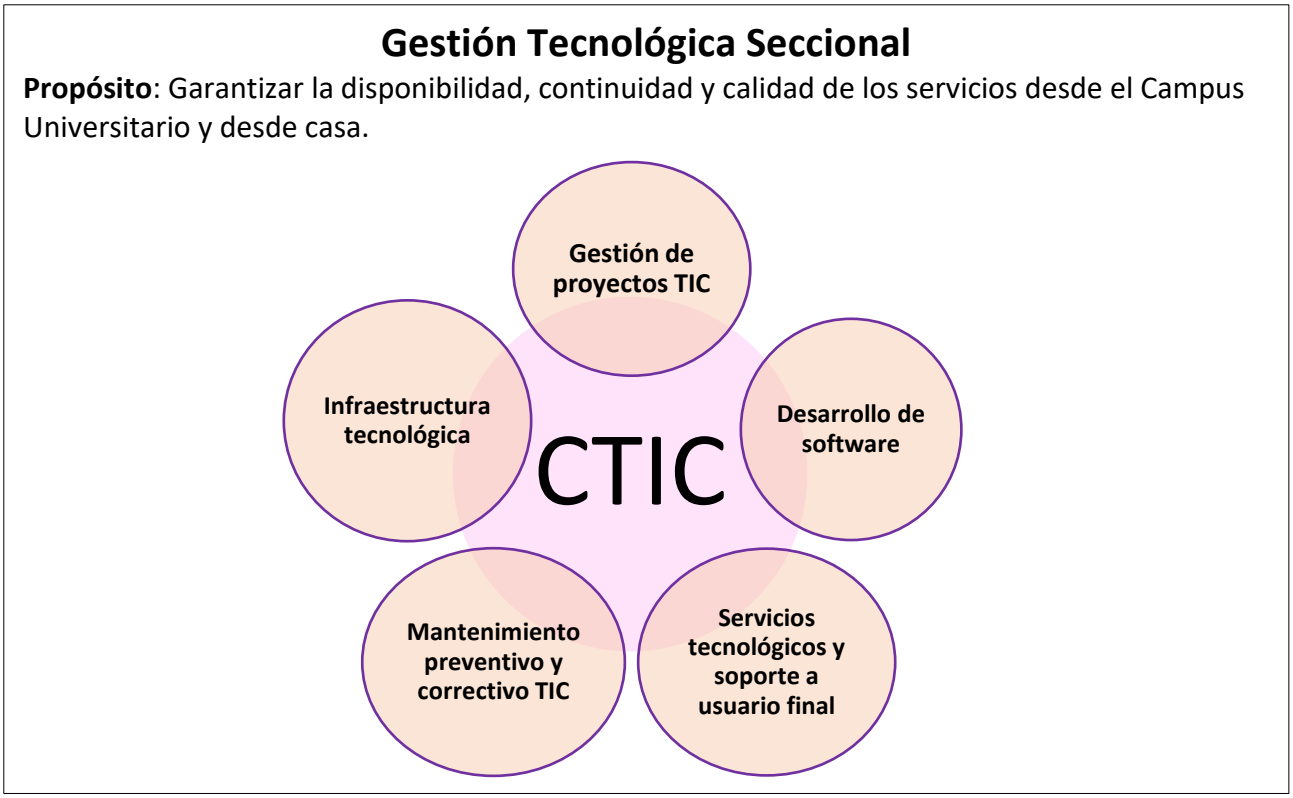


Figura 1. Organización del CTIC

5.2 Datos específicos del cargo en el cual se ubica la práctica empresarial

Cargo: Pasante en el Centro de Tecnología de Información y comunicaciones - CTIC de la Universidad Pontificia Bolivariana seccional Bucaramanga.

Supervisor empresarial: Zaira Yineth Hernández Ramírez | Profesional de infraestructura tecnológica - Red Física. Arelis Gómez Nova | Jefe Centro de Tecnologías de Información y Comunicación.

Proyecto: Replicar el modelo del archivo físico a un modelo digital y redefinir el modelo de copias de respaldo de la información.

Rol: Documentar y proponer un rediseño del proceso de copias de respaldo de la información, basado en las actividades que se proponen (Anexo cronograma de actividades).

Alcance: Obtener una documentación completa respecto al manejo de la información física y digital y de sus respectivas copias de respaldo, teniendo en cuenta la normatividad vigente y la clasificación de dicha información.

6 DEFINICIÓN DEL PROBLEMA

El proyecto que plantea el centro de tecnología de información y comunicaciones – CTIC seccional Bucaramanga, está enfocado al rediseño del modelo de copias de respaldo de la información utilizada. Por esta razón, se requiere clasificar la información digital institucional para optimizar el sistema de copias de respaldo que se conserva en el centro de datos de la Universidad Pontificia Bolivariana, Seccional Bucaramanga.

Por el momento, se cuenta con copias de respaldo de diversa información tanto digital como física que se ha ido obteniendo a partir de las diversas actividades y procesos que se realizan en la universidad, no obstante, se observa que varios de los datos que cuentan con copia de respaldo podrían prescindir de esta o que podría existir una mejor manera de realizar el proceso de copias de respaldo.

Con lo anteriormente nombrado se observan las actividades y el objetivo final que como pasante deberé realizar en el periodo de tiempo asignado.

7 OBJETIVOS

7.1 Objetivo general

Clasificar la información digital institucional mediante una documentación concisa para optimizar el sistema de copias de respaldo que se conserva en el centro de datos de la Universidad Pontificia Bolivariana Seccional Bucaramanga.

7.2 Objetivos específicos

- Buscar y revisar la información relevante para el proyecto.
- Realizar un diagnóstico de los activos de información institucional de la universidad seccional Bucaramanga.
- Planificar las soluciones tecnológicas para la conservación de la información digital clasificada.
- Realizar un diagnóstico de la configuración actual del sistema de copias de respaldo de la seccional.
- Proponer un nuevo rediseño del proceso de copias de respaldo.

8 METODOLOGÍA

La metodología utilizada, fue una metodología en fases. Es decir, se tomaron los objetivos anteriormente planteados y se construyó un diagrama con base en ellos, para así ir desarrollando cada actividad según corresponda. A continuación, se muestra el diagrama utilizado.

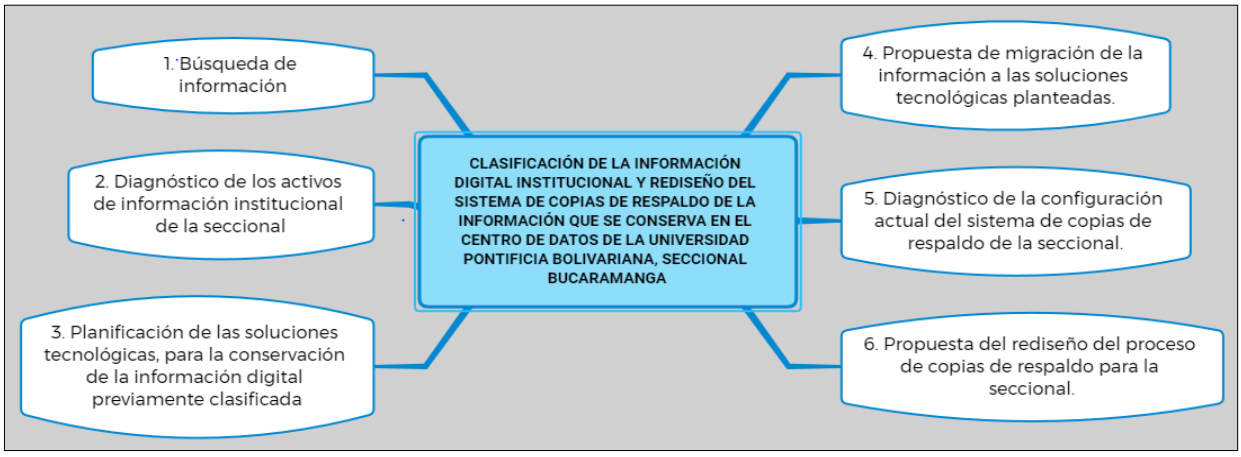


Figura 2. Metodología

9 ACTIVIDADES DESARROLLADAS

9.1 Marco histórico de la clasificación de la información

El siguiente apartado tiene la finalidad de exponer fuentes de información pertinentes respecto a las normativas vigentes que rigen la clasificación de la información digital. A continuación, se presentan referentes bibliográficos relevantes para el desarrollo del proyecto:

- **El archivo general de la nación** muestra una estructura conceptual de la preservación digital para lograr comprender los fundamentos de la preservación digital a largo plazo, teniendo como requisito la implementación de un sistema integrado de conservación. En este primer referente bibliográfico se observa que la información digital no cuenta con una clasificación específica, no obstante, se habla de documentos nativos digitales, documentos digitalizados con originales de naturaleza analógica y documentos digitalizados sin documentos originales analógicos, los cuales pueden contener información de cualquier índole ya sea de carácter cultural, educativo, científico, etc.[6]

- **La superintendencia de industria y comercio**, en este referente bibliográfico se habla acerca de los tipos de activos y su respectiva clasificación ya sea documental, software, persona, servicios, etc. Más específicamente, uno de los activos más importantes como lo es la información digital o física se rige por el decreto 103 de 2015, capítulo 1, artículo 38, donde se indica que una categoría de información es *"toda información de contenido o estructura homogénea, sea física o electrónica, emanada de un mismo sujeto obligado como resultado del ejercicio de sus funciones y que pueda agruparse a partir de categorías, tipos o clases según sus características internas (contenido) o externas (formatos o estructura)".* Por otro lado, la superintendencia de industria y comercio según la preservación digital maneja metadatos regidos por el decreto 1080 de 2015, artículo 2.8.2.7.9 Metadatos mínimos de los documentos electrónicos, el cual establece los siguientes metadatos: De contenido, De estructura y De contexto. Por ende, se puede deducir que la clasificación de la información digital está basada en este tipo de clasificación. [7]

- **El Ministerio de Tecnologías de la información y las Comunicaciones (Min TIC)** el cual establece que la clasificación de la información ya sea de manera física o digital se debe basar en el principio de confidencialidad primordialmente, contando este con tres niveles estipulados por la entidad y encontrados en la ley 1712 del 2014 los cuales son: información pública, información pública clasificada e información pública reservada. En este tipo

de información se pueden encontrar bases y archivos de datos, contratos, manuales de usuario, investigaciones, entre otros. [8]

- **Normas internacionales**, en este caso enfocadas al gobierno estadounidense y del Reino Unido. Estos dos gobiernos utilizan un esquema de clasificación de tres niveles, similar al que es utilizado nacionalmente y el cual se basa en el impacto que tendría la información si es divulgada. Los tres niveles mencionados son confidencialidad/ oficial, secreto y alto secreto. [9]

- **La norma NTC-ISO/IEC 27001** es "*un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI)*"[10]. Se debe tener en cuenta que la clasificación general de la información en las entidades nacionales que adoptaron un SGSI está regida por el anexo A.7.2 de esta norma internacional, la cual tiene como objetivo garantizar que se proteja la información en un nivel adecuado [10]. A su vez, este anexo cuenta con los apartados que se muestran a continuación.

A.7.2 Clasificación de la información Objetivo: asegurar que la información recibe el nivel de protección adecuado.		
A.7.2.1	Directrices de clasificación	Control La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.
A.7.2.2	Etiquetado y manejo de información	Control Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización

Figura 3. Clasificación de la información - Tomada de [10]

Según el Anexo 1 de la norma NTC-ISO/IEC 27001, las empresas que adopten un SGSI deben crear una política con los siguientes pasos para clasificar la información: [11]

- **Ingreso del activo de información en el Inventario de activos:** Llevar a cabo un inventario de datos o una auditoria de datos.

- **Clasificación de la información:** Toda la información debe ser clasificada en niveles de confidencialidad, pública, uso interno, restringida, confidencial.

- **Etiquetado de la información:** Indica en qué lugar, según el tipo de documentos que sea (documentos de papel, electrónicos, sistemas de

información, correo, almacenamientos electrónicos, etc.) debe llevar etiquetado el nivel de confidencialidad (pública, uso interno, restringida, confidencial).

- ❖ **Manejo de la información:** Todas las personas que tienen acceso a información clasificada deben seguir las reglas que se establecen en la política de clasificación de la información, son reglas de uso interno, uso restringido y uso confidencial, y esas reglas se aplican a cada tipo de documento (documentos de papel, electrónicos, sistemas de información, correo, almacenamientos electrónicos, etc.)

Como resultado de la investigación de estos referentes bibliográficos, se observa que la clasificación de la información ya sea física o digital en la mayoría de las organizaciones se enfoca en la gestión de riesgos [9], en donde se pueden encontrar los tres principios fundamentales de la seguridad de la información que son: confidencialidad, integridad y disponibilidad. Respecto a estos principios, cada dato manejado por la organización debe ser evaluado mediante el criterio de prioridad (alta, media, baja). [8]

Se deja claridad que la creación de una política de clasificación de la información, dentro del contexto de una futura adopción de un SGSI de parte de la Universidad, se encuentra fuera del alcance de este proyecto.

- **La procuraduría general de la nación** tiene público un documento disponible en el web llamado: Proceso de gestión documental, sub-proceso administración de documentos y registros “instructivo para la aplicación de las tablas de retención y valoración documental, las transferencias documentales y la eliminación”. Este instructivo, define las etapas del ciclo vital de los documentos, en cuanto a permanencia en cada uno de los tipos de archivos que tiene cada institución en sus distintas dependencias, esta permanencia se define en las tablas de retención documental (TRD). Respecto a la permanencia a continuación, se observa el ciclo vital de los documentos [12]:

  - ❖ **Archivo de Gestión**: Contiene la documentación que se produce y recibe en cada dependencia y es de consulta frecuente.

  - ❖ **Archivo Central:** Contiene la documentación que ha sido trasladada desde las diferentes dependencias para que se conserve durante un tiempo determinado, según las TRD.

- **Archivo Histórico**: Todos los documentos que no se eliminen en disposición final descritas en las TRD, son el archivo histórico.

Según lo anteriormente planteado y para dar más claridad del tema, se definen las **Tablas de retención documental (TRD)** como un documento donde se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos, que se generan en las distintas dependencias de una institución. Estos documentos contienen el registro de la serie documental, sub-serie, tipo de documento, tipo de acceso (ejemplo: general, restringido, retenido), la retención en años del archivo de gestión, archivo central y su disposición final, etc.[12] Por consecuencia, se encuentra una tabla y el gráfico de esta en resumen, donde se observa la aplicación de la definición de las etapas del ciclo vital de los documentos, según la procuraduría general de la nación, aplicadas en las TRD institucionales de la Seccional Bucaramanga

N°	Definición de las etapas del ciclo vital de los documentos, según la procuraduría general de la nación.		Aplicación de las etapas del ciclo vital de los documentos en las TRD institucionales de la Seccional Bucaramanga
1	**Archivo de Gestión:** Contiene la documentación que se produce y recibe en cada dependencia y es de consulta frecuente. La TRD debe indicar cuánto tiempo (en años) debe permanecer en esta etapa, para luego trasladarlo al archivo central.	⇨	**Retención 1 - Archivo de gestión:** La Seccional estableció para este tipo de archivo los siguientes opciones de tiempo en años: 1, 2,3,4,5,15.
2	**Archivo Central:** Contiene la documentación que ha sido trasladada desde las diferentes dependencias para que se conserve durante un tiempo determinado, según las TRD. La TRD también debe señalar el tiempo de retención (en años) en esta etapa, luego se procede a trasladarlo al Archivo Histórico o destruirlo.		**Retención 2 - Archivo central:** La Seccional estableció para este tipo de archivo los siguientes opciones de tiempo en años: 2,3,5,7,9,10,15,20,80.
3	**Archivo Histórico:** Contiene los documentos que deben conservarse de manera permanente, por sus valores secundarios y/o para dar cumplimiento a disposiciones de índole legal.		**Disposición final:** La Seccional estableció las siguientes opciones para disposiciones finales: Conservación total, conservación permanente, digitalización y eliminación. Es decir, todo lo que no se elimine en la disposición final, es archivo histórico.

Figura 4. Comparativa entre las etapas del ciclo vital de los documentos

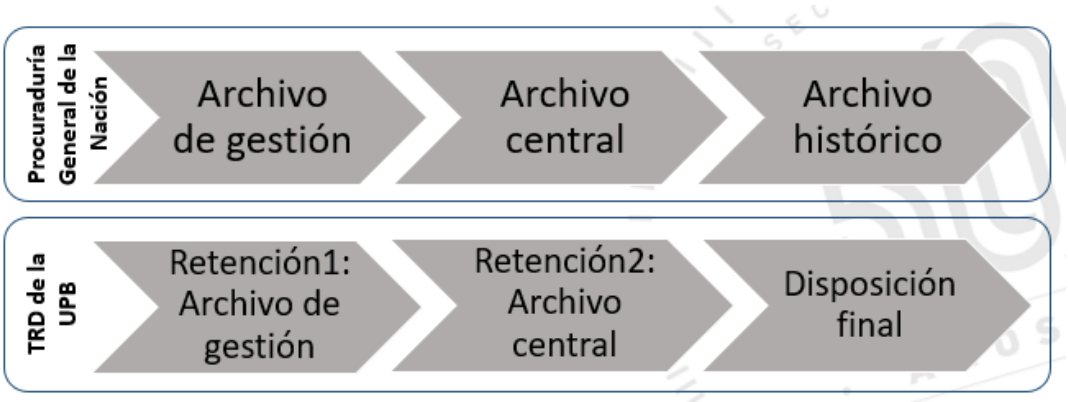


Figura 5. Resumen comparativo entre las etapas del ciclo vital de los documentos

De la anterior actividad se concluyó que la respuesta a la forma en la cual se debe clasificar la información digital Institucional de la Seccional se encuentra definida en las mismas TRD Institucionales. Por ende, se clasificó la información digital institucional para este proyecto basado en las etapas del ciclo vital de los documentos: archivo de gestión, archivo central y archivo histórico.

9.2 Diagnóstico de los activos de información institucional de la seccional

Para esta actividad se tomaron todas las TRD Institucionales de la Seccional y se consolidó toda esta información en un solo archivo de Excel llamado “Inventario de activos de información” anexo al documento, los objetivos que se cumplieron fueron:

- Identificar y conocer el inventario de activos de información institucional de la seccional
- Consolidar toda la información en un único archivo que permita filtrar para analizar
- Identificar el responsable o dueño de la producción del activo de información
- Identificar el tiempo de retención en años para el archivo de gestión, archivo central y disposición final
- Conocer el tipo de acceso para cada documento: general, restringido, retenido
- Identificar el medio de conservación y/o soporte: digital, físico, digital y físico
- Identificar qué dependencias manejan tipos de archivos especiales como: Informativos audiovisuales, videos institucionales, archivo fotográfico, etc.

Como resultado de esta actividad, se obtuvo un archivo de Excel con el consolidado de la información de las TRD de la Seccional, a continuación, una captura de pantalla de la primera sección del archivo construido:

A	B	C	D	E	F	G	H	I	J	K
INVENTARIO DE ACTIVOS DE INFORMACIÓN										
Nombre del responsable de la producción de información	SERIE DOCUMENTAL (S)	Subserie documental (Sd)	Nombre o título de la categoría de información / Tipo documental	Descripción del contenido la categoría de la información	Idioma	Acceso (General, restringido)	Retención 1	Retención 2	Disposición fi	
									Disposición final =>	Conservac permanen
Auditoría interna	ACTAS	Actas de reuniones de grupo de trabajo	Acta		Español	Restringido	Archivo de gestión 2		Eliminación	
Auditoría interna	ACTAS	Actas de reuniones de grupo de trabajo	Anexos		Español	Restringido	Archivo de gestión 2		Eliminación	
Auditoría interna	ACTAS DE ELIMINACIÓN DE DOCUMENTOS		Acta de eliminación de documentos en papel de seguridad		Español	Restringido	Archivo de gestión 1	Archivo Central 10	Conservación permanente	X
Auditoría interna	ACTAS DE ELIMINACIÓN DE DOCUMENTOS		Anexos		Español	Restringido	Archivo de gestión 1	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Programa anual de auditoría		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Plan de auditoría		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Registro de asistencia a reunión de apertura		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Lista de verificación del proceso		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Memorando remisión de informe de auditoría		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Informe de auditoría		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Pruebas de cumplimiento y sustantivas		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Acta de reunión de cierre		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Registro de asistencia a reunión de cierre		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	AUDITORÍAS INTERNAS		Planes de acción		Español	Restringido	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X
Auditoría interna	INFORMES	Informes de arqueo de caja	Informe		Español	Restringido	Archivo de gestión 5		Conservación permanente	X
Auditoría interna	INFORMES	Informes de gestión	Informe		Español	Restringido	Archivo de gestión 5		Conservación permanente	X
Capellanía	CONFIRMACIONES		Listado de confirmados		Español	Restringido			Conservación permanente y Digitalización	X
Capellanía	INFORMES	Informes de gestión	Informe		Español	Restringido	Archivo de gestión 3	Archivo Central 10	Conservación permanente y Digitalización	X
Capellanía	PROGRAMA DE		Programa		Español	General	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X
Capellanía	PROGRAMA DE		Presupuesto		Español	General	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X
Capellanía	PROGRAMA DE		Correspondencia		Español	General	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X
Capellanía	PROGRAMA DE		Listado de asistencia		Español	General	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X
Capellanía	PROGRAMA DE		Reportes de horas libres		Español	General	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X
Capellanía	PROGRAMA DE		Informes de actividades		Español	General	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X
Capellanía	PROGRAMA DE		Evaluación de actividades		Español	General	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X
Centro de conciliación del consultorio jurídico	ACREDITACIÓN	Acreditación centro de servicios	Solicitud de acreditción		Español	Restringido	Archivo de gestión 2	Archivo Central 3	Eliminación	
Centro de conciliación del consultorio jurídico	ACREDITACIÓN	Acreditación centro de servicios	Contrato de prestación de servicios		Español	Restringido	Archivo de gestión 2	Archivo Central 3	Eliminación	
Centro de conciliación del consultorio jurídico	ACREDITACIÓN	Acreditación centro de servicios	Plan de auditoría		Español	Restringido	Archivo de gestión 2	Archivo Central 3	Eliminación	
Centro de conciliación del consultorio jurídico	ACREDITACIÓN	Acreditación centro de servicios	Informes de auditoría		Español	Restringido	Archivo de gestión 2	Archivo Central 3	Eliminación	
Centro de conciliación del consultorio jurídico	ACREDITACIÓN	Acreditación centro de servicios	Acciones preventivas o correctivas		Español	Restringido	Archivo de gestión 2	Archivo Central 3	Eliminación	

Figura 6. Inventario de los activos de información - Tomada del Excel “Inventario de activos de información”

Teniendo en cuenta los resultados de esta actividad, a continuación, se describe la información relevante que se tuvo en cuenta para la construcción de la propuesta metodológica de la clasificación de la información digital Institucional:

- En las TRD se encontraron dos tipos de retención para todos los documentos, retención 1 – archivo de gestión y retención 2 – archivo central, dado esto, se proponen dos soluciones tecnológicas diferentes para almacenar la información digital, una solución tecnológica para almacenar la información del archivo de gestión y una segunda solución tecnológica para almacenar la información del archivo central e histórico.

- Cada solución tecnológica propuesta para el archivo de gestión y archivo central e histórico tiene tiempos de periodicidad de copias de respaldo específicos, ejemplo: a la solución tecnológica asignada como archivo gestión se le realizarán copias de respaldo diariamente al tratarse de información que su consulta y cambios son frecuentes, y a la solución tecnológica asignada para el archivo central e histórico se le realizaran copias de respaldo mensuales al tratarse de información que presenta pocos cambios. Esta es una idea de optimización de los recursos tecnológicos de almacenamiento del Datacenter.

- Las dependencias que manejan Informativos audiovisuales, videos institucionales, y archivo fotográfico, se les brinda una solución tecnológica específica para almacenar este tipo de archivos que digitalmente representan gran ocupación de almacenamiento, también se le aplica una periodicidad especial de copias de respaldo de la información.

- Todos los documentos marcados con disposición final como eliminación y cuyo medio de conservación y/o soporte este marcado como digital, el CTIC debe brindar soluciones de almacenamiento digital y respaldo de esa información por el tiempo en años definido en las TRD, pero una vez cumplido los años de retención en el archivo central, se deberá indicar al responsable y dueño de la información que esta ya cumplió su ciclo y la puede trasladar a una solución tecnológica a la cual no se le realice copia de respaldo, ejemplo: cuenta departamental de OneDrive, esto con el fin de liberar espacio en el servidor de almacenamiento del data center.

- Dependencias como Registro y control académico que manejan aproximadamente 70 tipos de documentos diferentes y en su TRD no definen los tiempos de retención, y su disposición final es conservación total y digitalización, su información se debe conservar casi por siempre.

9.3 Planificación de las soluciones tecnológicas para la conservación de la información digital clasificada

En esta sección se describen las tecnologías de almacenamiento y virtualización existentes en el centro de datos de la seccional y las soluciones tecnológicas propuestas para la conservación de la información digital.

9.3.1 Descripción de las tecnologías de almacenamiento y virtualización existentes: Actualmente, en el centro de datos de la seccional, se encuentran las siguientes soluciones tecnológicas de almacenamiento y virtualización:

- **SAN (Storage Area Network):** El sistema en red de área de almacenamiento ubicado en el centro de datos de la Seccional se encuentra interconectado por medio de fibra óptica con el clúster de servidores de virtualización, esto con el fin de brindar un mayor rendimiento en las transacciones que allí se realizan. Este sistema se encuentra configurado con dos propósitos: almacenamiento para virtualización con VMWare para el clúster de servidores y almacenamiento para las copias primarias de seguridad con el software Veeam Backup. A continuación, se describe el sistema SAN:

  - **DELL COMPELENT SC200 SAN y expansión**
    Propietario del Activo: Arelis Gómez Nova
    Capacidad:114TB entre la controladora y la expansión.
    Conexión: Se encuentra interconectada con los Switch Brocade y los servidores del clúster de virtualización por Fiber Channel.
    Descripción: Se presentan 18 Lums al clúster de virtualización para una capacidad total presentada a cada Host del sistema de virtualización de 60 TB, el resto está presentado a un servidor (Polilla) como repositorio de Backups.
    Imagen 5 versión Firmware de SAN.

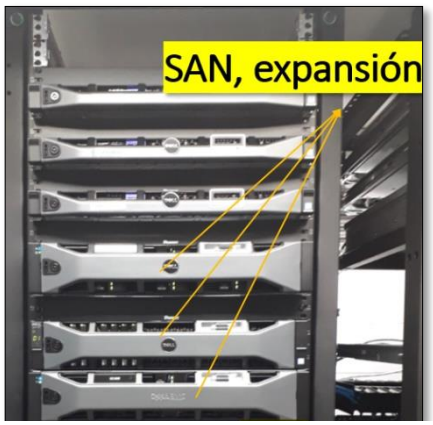


Figura 7. Fotografía del sistema SAN, ubicado en el centro de datos de la Seccional

Se realizó el diagnóstico del almacenamiento en la SAN y se obtuvo la siguiente información:

Descripción	Tamaño
Almacenamiento total reservado para máquinas virtuales en la SAN aproximadamente	61 TB
Almacenamiento total reservado para copias primarias de Veeam Backup aproximadamente	44 TB
Total almacenamiento reservado SAN	**105 TB**

Tabla 1. Total, almacenamiento reservado en la SAN

Descripción	Tamaño
Capacidad total almacenamiento SAN	114 TB
Capacidad total almacenamiento reservado SAN	105 TB
Total almacenamiento disponible SAN	**9 TB**

Tabla 2. Total, almacenamiento disponible en SAN

- **NAS (Network Attached Storage):** La seccional cuenta con 3 servidores de almacenamiento conectados en red NAS, dos ubicados en el centro de datos y uno ubicado en el edificio L. A continuación, se describen los 3 servidores:

NAS	Propietario	Función	Capacidad de almacenamiento	Ubicación	Descripción
Dell DR4300E	Arelis Gómez Nova	Repositorio de Veeam Backup	10 TB	Centro de datos	Sistema para guardar copias de seguridad
QNAP TVS-1271U-RP			36 TB Memoria: 32 GB	Sótano edificio L	
DELLEMC NX3240			44 TB Memoria: 16 GB	Aún sin configurar	

Tabla 3. Características de los almacenamiento NAS

A continuación, se presenta la tabla con el resumen del almacenamiento ocupado y el almacenamiento disponible, de la SAN, la NAS 1 y NAS 2:

Descripción	Total capacidad almacenamiento	Total almacenamiento utilizado	Porcentaje de almacenamiento ocupado	Porcentaje de almacenamiento disponible
SAN	114 TB	105 TB	92%	8%
NAS1	10 TB	8.09 TB	81 %	19%
NAS2	36 TB	21 TB	58 TB	42 %

Tabla 4. Resumen de almacenamiento de servidores

- **Clúster de virtualización:** Este sistema se compone de tres servidores con las siguientes características en común:

    - **Servidor Dell Power Edge R630 Clúster Virtualización Oruga**
    - **Servidor Dell Power Edge R630 Clúster Virtualización Avispa**
    - **Servidor Dell Power Edge R630 Clúster Virtualización Zancudo**

    Propietario del Activo: Arelis Gómez Nova
    Sistema operativo: VMware ESXi, 6.7.0
    No poseen disco duros
    Memoria RAM: 256 GB
    Procesadores: 2 procesadores Intel(R) y Xeon(R) CPU E5-2690 v4 @ 2.60GHz
    Descripción: En este clúster de servidores están todas las máquinas críticas para el funcionamiento de la empresa, hay File servers, servidores Web, servidores de bases de datos, un servidor de Veeam backup, un controlador de dominio, entre otros. También se encuentran un Windows server 2012 R2 estándar y 2016 estándar, servidores con Red hat 7, Ubuntu 14.04 LTS, Ubuntu 10.0.4 y Ubuntu 12.0.4.

9.3.2 Descripción de las soluciones tecnológicas propuestas para la conservación de la información digital

La Universidad Pontificia Bolivariana, asume desde el año 2001 el modelo de organización orientada por procesos, lo que se traduce al medio universitario como UOP. Los macroprocesos están clasificados según la concepción tradicional, en procesos estratégicos, de valor y de apoyo. Se presenta en la figura N°7 el mapa de los 5 macroprocesos: Administrativo y financiero, investigación, docencia y aprendizaje, proyección social y extensión y estrategia.

Según experiencia técnica del equipo de Infraestructura tecnológica (IT) del CTIC, se observa que la administración de recursos tecnológicos de almacenamiento y la recuperación de la información con el software de gestión de copias de respaldo se hace más sencilla si se crean varios servidores de almacenamiento y no uno solo. Por esta razón, el equipo de IT decide crear una solución tecnológica de almacenamiento para cada macroproceso, teniendo en cuenta que cada servidor de macroproceso contiene las dependencias que pertenecen a este.

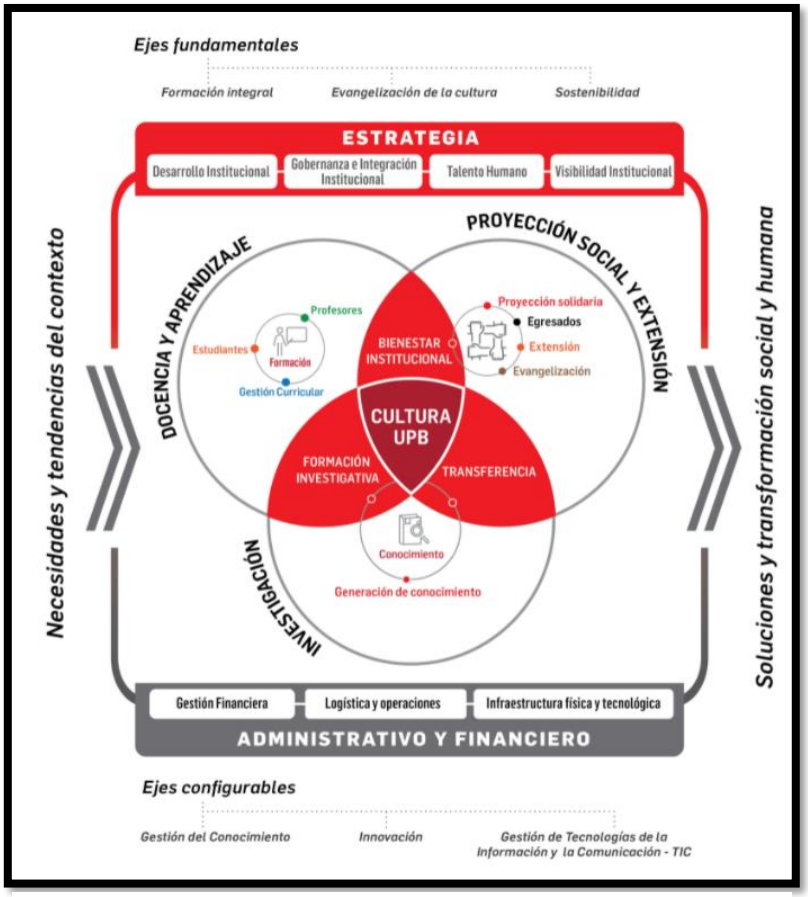


Figura 8. Mapa de macroprocesos de la Universidad Pontificia Bolivariana

A continuación, en la figura N° 8 se presenta el diagrama de la propuesta metodológica, para la clasificación de la información digital institucional y rediseño del sistema de copias de respaldo de la información que se conserva en el centro de datos de la Universidad Pontificia Bolivariana, Seccional Bucaramanga.

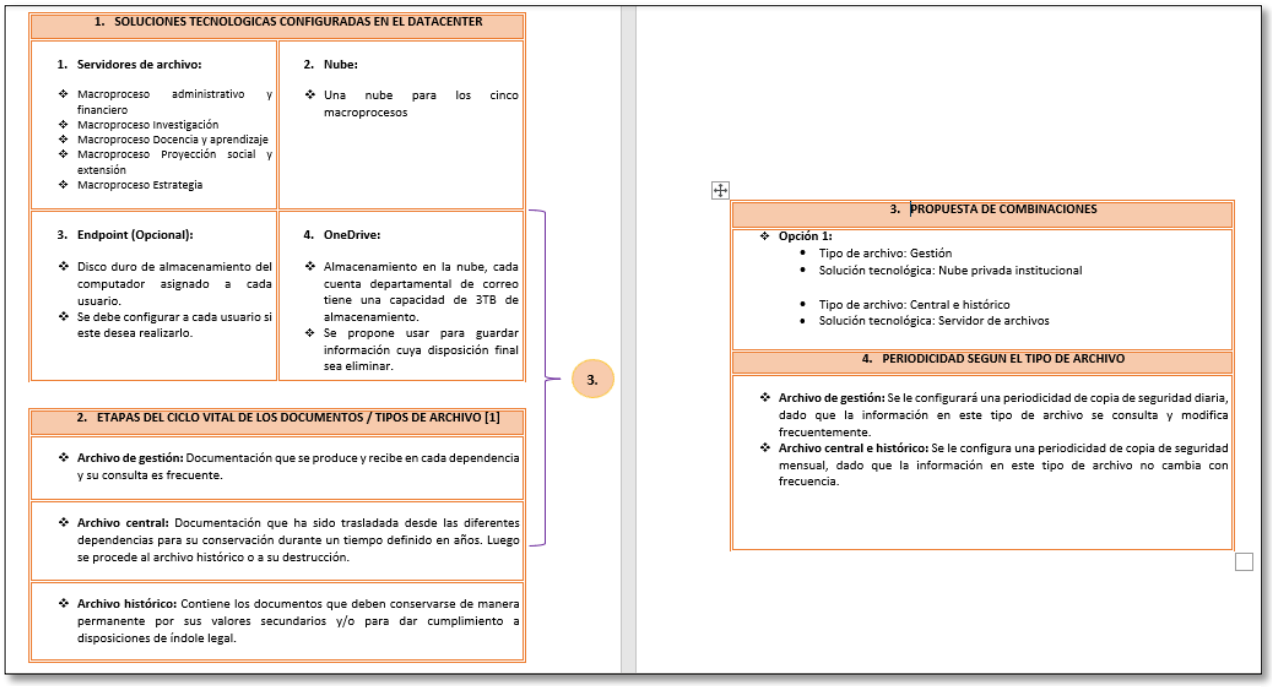


Figura 9. Diagrama de las soluciones tecnológicas propuestas

Para continuar, se describen las soluciones tecnológicas propuestas para el almacenamiento de la información digital Institucional de la Seccional que se clasificará. Algunas de estas soluciones tecnológicas ya se encuentran funcionando en el centro de datos, debido a que se fueron creando y configurando a medida que se realizaba este proyecto.

- **Servidor de archivos (file server)**
  Durante varios años en el centro de datos de la Seccional, se encontraba configurada una solución de almacenamiento de la información Institucional brindada a los usuarios (personal administrativo), llamada carpetas compartidas. No obstante, era una solución con mal funcionamiento a la hora de compartir y mapear las carpetas en los equipos de los usuarios. A continuación, se presentan algunos datos que se tenían en cuenta para el almacenamiento de las carpetas compartidas.

Nombre de la Máquina Virtual	Tamaño de almacenamiento VM utilizado en SAN	Tamaño de almacenamiento Copia de seguridad
CarpetasCompartidas	2.5 TB	3.86TB
CarpetasCompartidas1	482,8 GB	810GB
CarpetasCompartidas2	443,7 GB	886GB
CarpetasCompartidas3	395,2 GB	769GB
CarpetasCompartidas4	310,1 GB	660GB
CarpetasCompartidas5	384,2 GB	398GB
CarpetasCompartidas6	454,1 GB	522GB
CarpetasCompartidas7	1,5 TB	548GB
CarpetasCompartidas8	586,1 GB	487GB

Tabla 5. Almacenamiento de las carpetas compartidas

Por esta razón, se planteó migrar las carpetas compartidas a una solución más completa y administrable llamada Servidor de archivos (file server). Siguiendo a esto, se propone crear un servidor de archivos para cada macroproceso. Estos servidores de archivos se crean cada uno en una máquina virtual (del clúster de virtualización y su recurso de almacenamiento se encuentra en la SAN), las características físicas y recursos asignados a cada servidor virtual, se muestran a continuación en las figuras N°9, N°10.

En la figura N°9, se encuentran los recursos de hardware asignados a la máquina virtual del servidor de archivos, creado para el macroproceso Administrativo y financiero.

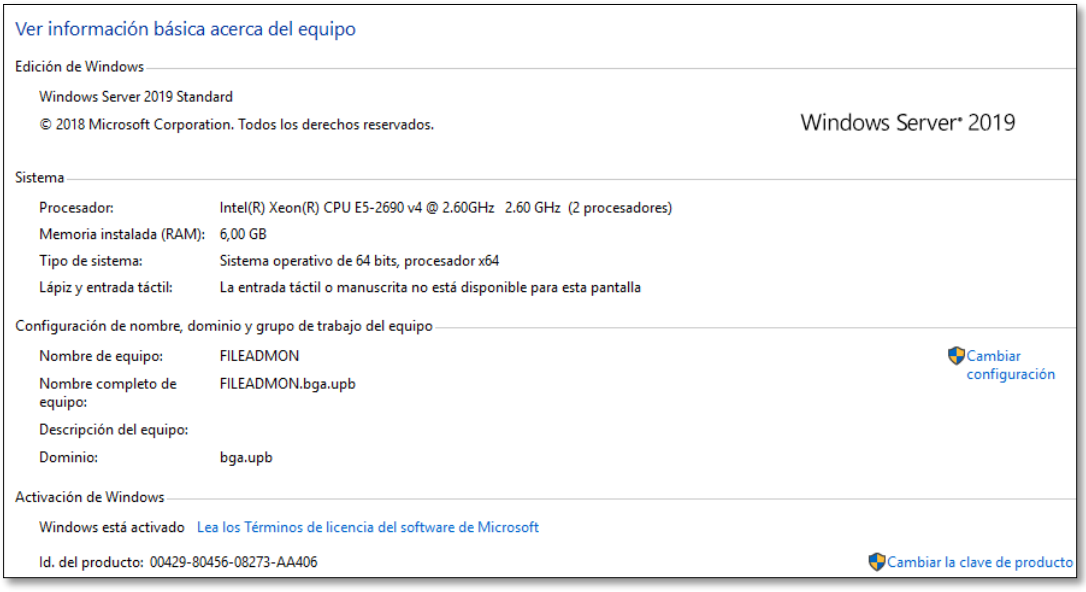


Figura 10. Recursos de hardware asignados a cada servidor de archivos

Según la figura N°10, el tamaño del almacenamiento asignado al servidor de archivos es 750GB, sin embargo, esta capacidad de almacenamiento se puede ampliar a medida que se requiera.

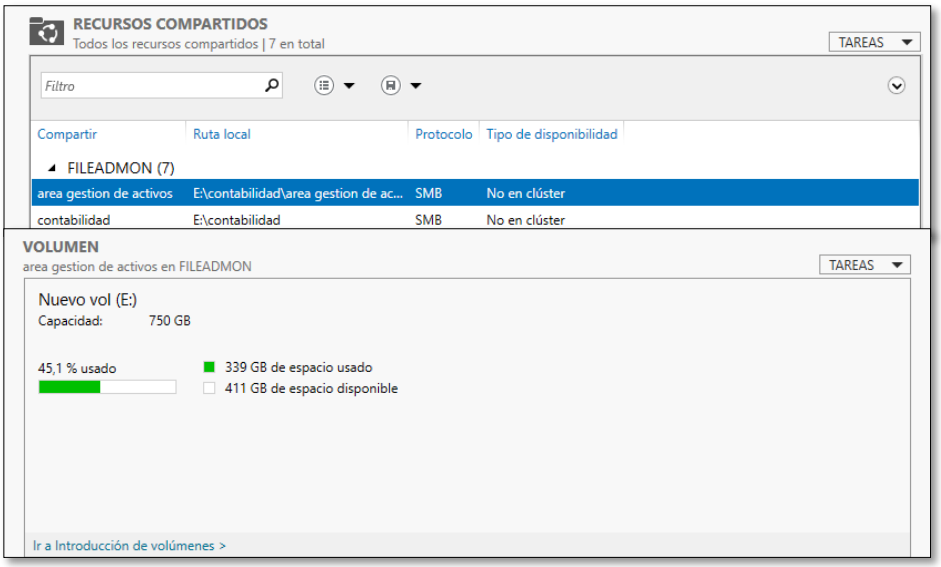


Figura 11. Pantalla de administración del servidor de archivos

Cómo ya se mencionó, se crearán servidores de archivos con las mismas características para los 4 macroprocesos restantes.

- **Nube privada Institucional**

  Es una solución tecnológica brindada al personal administrativo y docente de la universidad y hasta el momento se encuentran creados aproximadamente 240 usuarios. Actualmente no se ha parametrizado que tipo de información deben almacenar los usuarios en esta solución, con el fin de optimizar el tamaño de la máquina virtual y las copias de seguridad que se programan. Respecto a esta solución se encontró la siguiente información:

Nombre de la Máquina virtual	Tamaño de almacenamiento VM reservado en SAN	Tamaño de almacenamiento Copia de seguridad
RedHat_Servidor_Nextcloud_nube_2020	5.1 TB	2.56TB

Tabla 6. Almacenamiento de la nube privada institucional

Cabe mencionar, que anteriormente se tenía previsto la creación de cinco nubes; una para cada macroproceso, no obstante, se optó por dejar en funcionamiento una sola nube para todos los macroprocesos, puesto que es necesario compartir información de macroproceso a macroproceso, por otro lado, se observó que existen más de 60 docentes como usuarios a los cuales

se les debería migrar la información si se crean las cinco nubes, lo cual no es viable, y para finalizar se tuvo en cuenta para la toma de decisión que el almacenamiento de la nube se va a optimizar mediante la clasificación de la información anteriormente mencionada (archivo de gestión, archivo central e histórico).

- **EndPoint (Opcional)**

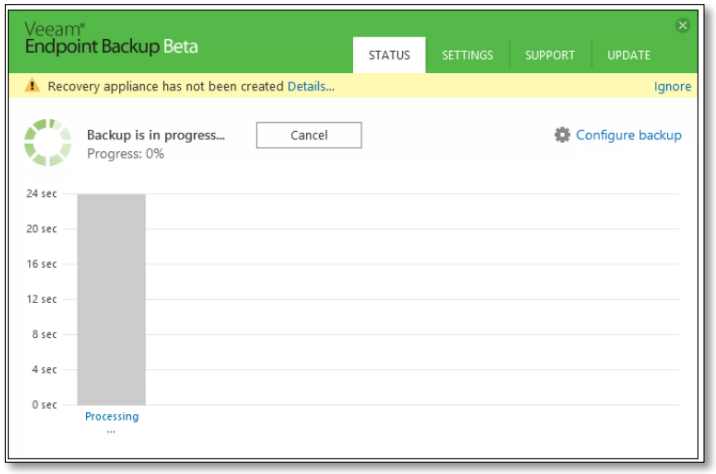


Figura 12. Captura de pantalla de la ventana de EndPoint

El software que la Seccional utiliza para la creación y gestión de las copias de seguridad en el centro de datos se llama Veeam Backup & Replication. Esta solución de software contiene un recurso sencillo llamado EndPoint para realizar copias de seguridad de equipos de escritorio y portátiles basados en Windows para usuarios finales. Estas copias de seguridad que se realizaban a nivel de cada computador de un usuario final, fue una estrategia que se utilizó hasta antes de que el personal administrativo pasara a trabajar en modalidad remota por la pandemia que se vive en la actualidad; Dado que la gran mayoría de usuarios tuvieron que llevar sus computadores de trabajo a su casa y con el lanzamiento de la nube privada Institucional, los EndPoint se suspendieron. Finalmente, para este proyecto se decidió que esta solución se dejará cómo una opción, solamente para casos particulares, no se configurará nuevamente a todos los computadores de los usuarios finales, debido a la propuesta que se está planteando en este proyecto.

- **OneDrive**

La plataforma tecnológica que la universidad utiliza y tiene contratada para la gestión de correo electrónico es la plataforma de Office 365 de Microsoft, en esta, cada cuenta de correo Institucional tiene una herramienta de almacenamiento en la nube llamada OneDrive. Cada cuenta de OneDrive tiene

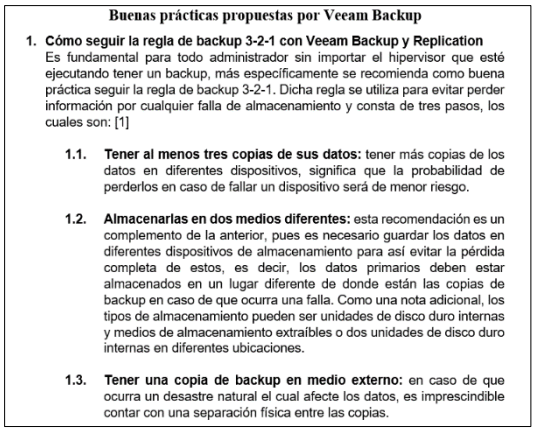
una capacidad de 3TB de almacenamiento, sin embargo, a esta solución la Universidad no le realiza copias de seguridad debido a que la solución de Veeam Backup no realiza copias a esta plataforma. Por otro lado, esta herramienta no se ha definido como repositorio oficial de la información Institucional, no obstante, se utiliza como una herramienta disponible para casos específicos.

En este proyecto se propone que esta herramienta se utilice como almacenamiento para la información de los estudiantes, cuya pérdida ocasional de la información no ocasionaría un gran impacto en los procesos de la Universidad, también se plantea que se utilice cuando se requiera compartir alguna información específica entre docentes, empleados y estudiantes. Por último, se aconseja que se utilice OneDrive cuando un empleado requiera guardar información cuya disposición final según las TRD sea eliminar, para así evitar guardar información en discos duros portátiles y memorias USB que pueden ser extraviadas físicamente y/o que pueden presentar fallas técnicas.

9.4 Diagnóstico de la configuración actual del sistema de copias de respaldo de la Seccional

9.4.1 Buenas prácticas para la implementación de un sistema de copias de seguridad según Veeam Backup

En esta actividad se consultó la documentación que se encuentra en línea de Veeam Backup y se construyó un documento mostrado a continuación, donde se plasmaron las buenas prácticas que recomienda este fabricante y las cuales se deberían implementar en un sistema de copias de seguridad eficiente.



Buenas prácticas propuestas por Veeam Backup

1. **Cómo seguir la regla de backup 3-2-1 con Veeam Backup y Replication**
   Es fundamental para todo administrador sin importar el hipervisor que esté ejecutando tener un backup, más específicamente se recomienda como buena práctica seguir la regla de backup 3-2-1. Dicha regla se utiliza para evitar perder información por cualquier falla de almacenamiento y consta de tres pasos, los cuales son: [1]

   1.1. **Tener al menos tres copias de sus datos:** tener más copias de los datos en diferentes dispositivos, significa que la probabilidad de perderlos en caso de fallar un dispositivo será de menor riesgo.

   1.2. **Almacenarlas en dos medios diferentes:** esta recomendación es un complemento de la anterior, pues es necesario guardar los datos en diferentes dispositivos de almacenamiento para así evitar la pérdida completa de estos, es decir, los datos primarios deben estar almacenados en un lugar diferente de donde están las copias de backup en caso de que ocurra una falla. Como una nota adicional, los tipos de almacenamiento pueden ser unidades de disco duro internas y medios de almacenamiento extraíbles o dos unidades de disco duro internas en diferentes ubicaciones.

   1.3. **Tener una copia de backup en medio externo:** en caso de que ocurra un desastre natural el cual afecte los datos, es imprescindible contar con una separación física entre las copias.

Figura 13. Documento de buenas prácticas de Veeam Backup - Tomada de Archivo "Anexo2 - Buenas prácticas de Veeam Backup"

Por otro lado, teniendo en cuenta la información del documento de las buenas prácticas de Veeam Backup se construyó una lista de verificación, dentro de la cual se encuentran:

- Regla de backup 3-2-1
- Mejores prácticas para los Backups de VMware vSphere
- Mejores prácticas para la prevención del ramsonware
- Mejores prácticas para la continuidad del negocio

El objetivo de construir esta lista era evaluar y verificar si el estado actual del sistema de copias de seguridad cumplía o no con las buenas prácticas dadas por el fabricante de Veeam Backup y sus recomendaciones según corresponda. Así pues, se obtuvo la siguiente información:

- **Objetivo de control 1:** Evaluar el cumplimiento de todos los requisitos de la regla de backup 3-2-1 propuesta por Veeam Backup & Replication

Requerimiento de verificación	Cumple
Verifique que además de los datos primarios, se realicen dos copias de seguridad en lo posible almacenados físicamente en ubicaciones diferentes.	Si
Verifique si las copias de seguridad se almacenan al menos en dos medios diferentes. Ejemplo: discos, cintas, nube, otros.	No
Verifique si las copias de seguridad se almacenan en un sitio externo (fuera del sitio - offline)	No

Tabla 7. Requisitos de la regla 3-2-1 de Veeam Backup

- **Objetivo de control 2:** Evaluar si se cumple con las mejores prácticas para los Backups de Vmware vSphere, recomendados por Veeam Backup & Replication

Requerimiento de verificación	Cumple
Verificar si se encuentra instalada la última versión de Veeam backup & replication	No
Verificar si se cuenta con el licenciamiento de Veeam Continuos Data Protection (CDP) para recuperación ante desastres	No
Verificar si el licenciamiento actual que tiene contratado la Universidad permite la instalación de Veeam ONE	Si

Tabla 8. Mejores prácticas para Backups de VMware vSphere

- **Objetivo de control 3:** Evaluar si se cumplen con las estrategias definitivas para la prevención del ransomware según Veeam Backup & Replication

Requerimiento de verificación	Cumple
Verificar si se realizan jornadas de educación hacia los usuarios finales acerca de la definición del ransomware y cómo evitarlo.	No
Verificar si el licenciamiento actual que tiene contratado la Universidad permite la instalación de Veeam ONE	Si
Verifique si las copias de seguridad se almacenan en un sitio externo (fuera del sitio - offline)	No

Tabla 9. Estrategias para la prevención del ramsonware según Veeam Backup

- **Objetivo de control 4:** Evaluar si se cuenta con un plan de continuidad del negocio enfocado en las copias de seguridad que respalde el futuro digital de la Seccional

Requerimiento de verificación	Cumple
Verificar si se cuenta con un plan de continuidad del negocio enfocado en las copias de seguridad: Identificación de amenazas, análisis de impacto en la empresa, plan de respuesta y recuperación, para así probar el plan de recuperación.	No

Tabla 10. Plan de continuidad de negocio enfocado en las copias de seguridad

Como resumen, se observa la tabla con el porcentaje de cumplimiento de cada objetivo anteriormente mencionado.

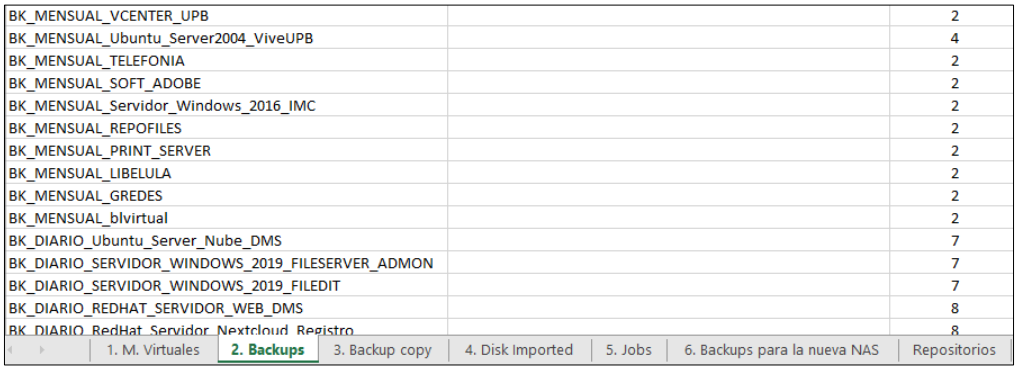
Objetivo de control	Descripción	% de cumplimiento
N° 1.	Requisitos de la regla de backup 3-2-1 propuesta por Veeam Backup & Replication	**33.33 %**
N° 2.	Las mejores prácticas para los Backups de VMware vSphere, recomendados por Veeam Backup & Replication	**33.33 %**
N° 3.	Estrategias definitivas para la prevención del ransomware según Veeam Backup & Replication	**33.33 %**
N° 4.	Plan de continuidad del negocio enfocado en las copias de seguridad que respalde el futuro digital de la Seccional	**0%**

Tabla 11. Porcentaje del cumplimiento de los objetivos

9.4.2 Análisis del almacenamiento actual utilizado

En esta actividad se realizó el inventario de lo siguiente para conocer a que información se debe hacer copia de seguridad:

- Máquinas virtuales del clúster de virtualización
- Backups actuales (diarios, semanales, mensuales)
- Jobs del EndPoint



BK_MENSUAL_VCENTER_UPB		2
BK_MENSUAL_Ubuntu_Server2004_ViveUPB		4
BK_MENSUAL_TELEFONIA		2
BK_MENSUAL_SOFT_ADOBE		2
BK_MENSUAL_Servidor_Windows_2016_IMC		2
BK_MENSUAL_REPOFILES		2
BK_MENSUAL_PRINT_SERVER		2
BK_MENSUAL_LIBELULA		2
BK_MENSUAL_GREDES		2
BK_MENSUAL_blvirtual		2
BK_DIARIO_Ubuntu_Server_Nube_DMS		7
BK_DIARIO_SERVIDOR_WINDOWS_2019_FILESERVER_ADMON		7
BK_DIARIO_SERVIDOR_WINDOWS_2019_FILEDIT		7
BK_DIARIO_REDHAT_SERVIDOR_WEB_DMS		8
BK_DIARIO_RedHat_Servidor_Nextcloud_Registro		8

1. M. Virtuales | 2. Backups | 3. Backup copy | 4. Disk Imported | 5. Jobs | 6. Backups para la nueva NAS | Repositorios

Figura 14. Inventario de la información a analizar – Tomada de Excel "Anexo4 - Listado máquinas virtuales y backups"

- Usuarios que actualmente tienen un usuario en la nube privada

NOMBRE	CARGO
Usuario 1	Auxiliares y técnicos
Usuario 2	Docentes
Usuario 3	Jefes de dependencias
Usuario 4	Auxiliares y técnicos
Usuario 5	Directivos
Usuario 6	Auxiliares y técnicos
Usuario 7	Auxiliares y técnicos
Usuario 8	Judicantes CPS
Usuario 9	Auxiliares y técnicos
Usuario 10	Docentes
Usuario 11	Docentes
Usuario 12	Temporales
Usuario 13	Temporales
Usuario 14	Docentes

Figura 15. Usuarios en la nube privada – Tomada de Excel "Anexo5 - Listado usuarios de nube

A continuación, se observa la cantidad de usuarios respecto a cada cargo consignado en la tabla anterior y el total de usuarios completos.

Cargo	Cantidad de usuarios
Administrador	4
Auxiliares y técnicos	73
BCEP	11
BCPS	1
CTIC	7
Directivos	5
Docentes	61
Jefes de dependencias	23
Judicantes CPS	7
Profesionales	35
Temporales	9
Test	1
Total	237

Tabla 12. Cargos y cantidad de usuarios de nube

- Documento del listado de carpetas compartidas por migrar, estas carpetas compartidas se deben migrar a un nuevo file Server, este trabajo fue desarrollado por el equipo de infraestructura, pero se anexo a la propuesta pues tiene relevancia en el rediseño de la clasificación de la información digital institucional.

					Mes 1		
					SEMANA 1	SEMANA 2	SEMANA 3
		Tamaño	Numero de Carpetas	Carpetas Compartidas			
		248 GB					
HECTOR	10.xx.xx.xx		1	Camaras	X		
			2	fotos Intranet	X		
			3	Contabilidad	X		
			4	FACTURAS PROVEEDRORES	X		
			5	JefeContabilidad	X		
			6	Biblioteca	X		
			7	Escuela de Inegnieria	X		
			8	Facultad Ciencias Politicas y Gobierno	X		
ZAIRA	10.xx.xx.xx	320 GB					
			9	CTIC	X		
			10	Planeacion	X		
			11	FTA 2020-2022	X		
			12	Análisis UPBVirtual	X		
			13	**PDI 2017-2019**Claudia SuarezNelson Moreno	X		
			14	**Estadisticas UPBControl TOTAL**paola.sierrav	X		
			15	Autoevaluacion de Programaspaola.sierrav	X		
			16	PlantaFisica_SeguridadEnElTrabajo	X		
JOHN	10.xx.xx.xx	202 GB					
			17	Lab_Est_Ambien	X		
			18	Post_Derecho	X		
			19	DOCUMENTOS 2	X		

Figura 16. Carpetas compartidas por migrar

9.4.3 Identificación de las herramientas de almacenamiento y respaldo (software y hardware) que se encuentran actualmente funcionando en el centro de datos de la seccional

En esta actividad se realizó el diagrama de la configuración actual de las copias de seguridad para observar que cambios se debían realizar después de la propuesta de este proyecto.

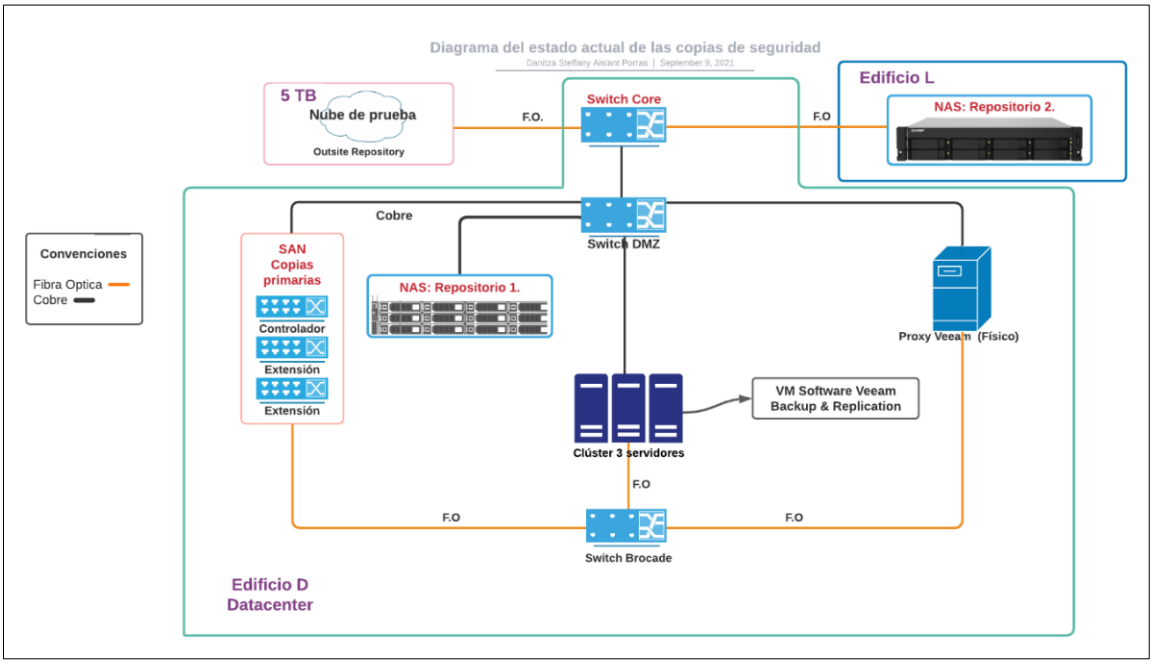


Figura 17. Diagrama del estado actual de las copias de seguridad

En esta figura se observan los equipos de telecomunicaciones y servidores que hacen posible el funcionamiento del sistema de copias de seguridad de la Universidad. El software de Veeam Backup & Replication se encuentra instalado en un clúster de servidores, este clúster administra el almacenamiento externo SAN. En este almacenamiento están las copias primarias. Por otro lado, existen dos servidores NAS presentados al sistema de copias de seguridad como repositorios, también se muestra un servidor físico que cumple la función de Proxy del software Veeam Backup el cual se encarga de procesar las tareas de Backups y de gestionar el tráfico de las copias de seguridad.

Para finalizar, se observa una nube de prueba como repositorio externo a la universidad donde se almacenan algunas copias de seguridad.

9.4.4 Situación actual del plan de respaldo de la información institucional

En esta actividad se identificó la información actual de las copias de seguridad que se realizan con Veeam Backup en el centro de datos de la seccional y se encontró lo siguiente: la frecuencia de respaldo, la retención actual y los puntos de restauración con los que cuenta cada Backup.

Nombre	Frecuencias de backup	Retención actual	Puntos de restauración
BK_DIARIO_Ubuntu_Server_Nube_DMS	Diario	7	7
BK_DIARIO_SERVIDOR_WINDOWS_2019_FILESERVER_ADMON	Diario	12	7
BK_DIARIO_SERVIDOR_WINDOWS_2019_FILEDIT	Diario	11	7
BK_DIARIO_REDHAT_SERVIDOR_WEB_DMS	Diario	12	8
BK_DIARIO_RedHat_Servidor_Nextcloud_Registro	Diario	13	8
BK_DIARIO_RedHat_Servidor_Nextcloud_nube2020	Diario	11	10
BK_DIARIO_RedHat_Servidor_Nextcloud_Dir_Docencia	Diario	13	8
BK_DIARIO_NEXTCLOUD	Diario	12	8
BK_DIARIO_CARPETASCOMPARTIDAS8	Diario	13	8
BK_DIARIO_CARPETASCOMPARTIDAS7	Diario	13	8

Figura 18. Situación actual del plan de respaldo de la información institucional - Tomada del Excel "Anexo4 - Listado máquinas virtuales y backups"

9.4.5 Resultados del diagnóstico de configuración actual de copias de seguridad

Luego de realizar las actividades anteriores y profundizando un poco más en cada detalle del inventario realizado, se encontró lo siguiente:

- El software que se utiliza actualmente para hacer copias de seguridad se llama Veeam Backup & Replication, este software solo realiza copias de seguridad a las máquinas virtuales creadas en la plataforma VMware.
- La versión de Veeam Backup & Replication instalada es la 9.5, no obstante, el software en este momento está en la versión 11.
- El software de copias de seguridad cuenta con la licencia Veeam availability suite enterprise de suscripción anual.
- Dentro del Software de gestión de servidores Vcenter Server – VMware se encontraron 120 máquinas virtuales de las cuales actualmente se le realizan copias de seguridad a las máquinas virtuales más importantes que en total son 59.
- El sistema de copias de seguridad tiene configurado 4 repositorios, en la siguiente imagen se describen las carpetas creadas en cada repositorio, el medio de almacenamiento (Discos duros, nube, etc.) y la capacidad.

N°	Repositorio	Carpetas creadas en el repositorio	Medio de almacenamiento	Ubicación	Capacidad total
1	SAN	DS_VEEAMSERVER_01	Discos duros	Datacenter	8,0 TB
		DS_VEEAMSERVER_02			8,0 TB
		DS_VEEAMSERVER_03			8,0 TB
		DS_VEEAMSERVER_04			8,0 TB
		TSMVEEAM3			4,0 TB
		TSMVEEAM4			4,0 TB
		TSMVEEAM5			4,0 TB
2	NAS DR4300	DR4300	Discos duros	Datacenter	7,8 TB
3	NAS QNAP	QNAP	Discos duros	Cuarto técnico, Edificio L semisótano	35,6 TB
4	C&W	CWC Backup Repository	Nube	Proveedor externo	4,7 TB

Figura 19. Repositorios del sistema de copias de seguridad

- Dentro del servidor principal de Veeam Backup existen dos tipos de copias de seguridad:

  - **Backups:** Son las copias primarias que realiza el software de Veeam Backup y se encuentran en la SAN, se encontraron las siguientes cantidades.

Frecuencia	Retención	Cantidad
Diaria	5,7,11,12,13 días	18
Semanal	4,5,6,11,12,17,30,48 días	28
Mensual	1,11,12,13,26 días	13
	Total	59

Tabla 13. Frecuencia y cantidad de copias de seguridad

La descripción de frecuencia es la siguiente:

Frecuencia diaria: este tipo de copia se asigna a las máquinas en donde la información es de uso recurrente.
Frecuencia semanal: este tipo de frecuencia se asigna a las máquinas en donde la información presenta cambios con menos frecuencia que la diaria.
Frecuencia mensual: este tipo de copia se asigna a las máquinas en donde la información no presenta cambios significativos.

  - **Backups copy:** Son las copias que se realizan a las copias primarias en repositorios externos. Los backups copy están configurados para crear dos copias mensuales a cada copia primaria, una copia almacenada en el repositorio NAS DR4300 (Ubicada en el Datacenter)

y la segunda copia almacenada en la NAS QNAP (Ubicada en el Edificio L).

Repositorio	Cantidad de Backup Copy
Nube (CWC)	4
NAS DR4300	55
NAS QNAP	54
Total	113

Tabla 14. Repositorio y cantidad de Backup Copy

- El EndPoint, como se mencionó anteriormente, es una solución tecnológica que se dejará como opcional, no obstante, al realizar el diagnóstico se encontraron las siguientes cantidades:

	Estado	Cantidad
Job Windows agent Backup	Success	324
	Failed	472
	Warning	26
	Total	822

Tabla 15. Estado y cantidad de los Jobs

Por otro lado, se observó que este proceso de copias de seguridad en los equipos de los usuarios finales, actualmente se encuentra suspendido.

9.5 Propuesta de rediseño de las copias de respaldo

De acuerdo con la previa clasificación de la información digital institucional, la definición de las soluciones tecnológicas para la conservación de la información digital, las mejores prácticas para las copias de respaldo y el diagnóstico del actual funcionamiento de las copias de seguridad, a continuación, se presenta la propuesta del rediseño del proceso de copias de respaldo para la seccional:

9.5.1 Definición de la Información digital que se debe respaldar

La forma en la cual se clasifica la información digital Institucional de la Seccional Bucaramanga como se mencionó anteriormente, se encuentra definida en las tablas de retención documental (TRD). Por esta razón, los tipos de archivos propuestos son los siguientes:

- **Archivo de gestión:** contiene la documentación que se produce y recibe en cada dependencia y es de consulta frecuente.

- **Archivo central**: contiene la documentación que ha sido trasladada desde el archivo de gestión para que los documentos se conserven durante un tiempo determinado, según las TRD.
- **Archivo Histórico:** todos los documentos que no se eliminen en disposición final descritas en las TRD, son el archivo histórico.

Tomando como base estas definiciones, en el archivo “Inventario de activos de información” se encuentra la descripción de los activos que se deben respaldar.

INVENTARIO DE ACTIVOS DE INFORMACIÓN								
Nombre del responsable de la producción de información	Retención 1	Retención 2	Disposición final					Medio de conservac... y/o soporte
			Disposición final =>	Conservación permanente	Conservación total	Digitalización	Eliminación	
Auditoría interna	Archivo de gestión 2		Eliminación				X	Digital
Auditoría interna	Archivo de gestión 2		Eliminación				X	Digital
Auditoría interna	Archivo de gestión 1	Archivo Central 10	Conservación permanente	X				Físico
Auditoría interna	Archivo de gestión 1	Archivo Central 10	Conservación permanente	X				Físico
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 4	Archivo Central 10	Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 5		Conservación permanente	X				Digital
Auditoría interna	Archivo de gestión 5		Conservación permanente	X				Digital
Capellanía			Conservación permanente y Digitalización	X		X		Digital
Capellanía	Archivo de gestión 3	Archivo Central 10	Conservación permanente y Digitalización	X		X		Digital
Capellanía	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X		X		Digital
Capellanía	Archivo de gestión 2	Archivo Central 10	Conservación permanente y Digitalización	X		X		Digital

Figura 20. Inventario de activos de información

Por consiguiente, se realizarán copias de seguridad con el software Veeam Backup & Replication a la información que en las TRD indiquen que el medio de conservación y/o soporte es digital.

9.5.2 Soluciones tecnológicas para el almacenamiento de la información digital

Este apartado respecto al ítem 9.3.2 “Descripción de las soluciones tecnológicas propuestas para la conservación de la información digital”, no realizó ningún cambio, pues se consideró oportuno las soluciones allí planteadas, las cuales fueron:

- **Nube privada institucional** como almacenamiento para la información de archivo de gestión.
- **Servidor de archivos** como almacenamiento para la información de archivo central e histórico. En esta solución deberán migrarse las carpetas compartidas.
- **EndPoint** como una solución opcional. No obstante, se propone descontinuar su uso, pues la nube privada institucional pasó a ser un reemplazo de esta.

- **OneDrive** como una solución de almacenamiento a la cual no se le realiza copia de seguridad.

9.5.3 Política de retención de copias de seguridad

La política de retención escogida para las copias de seguridad se basa en el siguiente esquema: mensual, semanal, diario**.**

- **Política de retención de los backup en Veeam Backup:**

  - **Programación mensual:** se ejecuta el trabajo un día elegido de la última semana del mes.
    Política de retención: se deben mantener las últimas doce (12) copias de seguridad.
    Puntos de restauración en Veeam Backup: 12

  - **Programación semanal:** se ejecuta el trabajo un día elegido a la semana.
    Política de retención: se deben mantener las últimas cuatro (4) copias de seguridad.
    Puntos de restauración en Veeam Backup: 4

  - **Programación diaria:** se ejecuta el trabajo todos los días.
    Política de retención: se deben mantener las últimas siete (7) copias de seguridad.
    Puntos de restauración en Veeam Backup: 7

- **Política de retención de los backups copy en Veeam Backup**

  La política de retención para los backups copy, se basa en un esquema mensual, en el cual se le realiza una copia de seguridad cada 30 días a cada uno de los backups anteriores. Con este esquema se garantiza un año de retención de la información (365 días) para cada uno de los backups diarios, semanales o mensuales.

9.5.4 Diseño del proceso de copias de respaldo o seguridad de la información

- **Servidores virtuales para respaldar:**
  La información digital para respaldar se encuentra almacenada en las distintas soluciones tecnológicas (servidores ubicados en el centro de datos) brindadas por el CTIC. Por tal razón la información que debe contar con copia de

seguridad son aquellos servidores virtuales con información y servicios críticos para la Universidad, como los siguientes:

- Los servidores virtuales que manejan bases de datos.
- Los servidores virtuales que manejan servicios importantes para la red de la Universidad cómo Directorio activo, DNS, DHCP.
- Los servidores virtuales donde se encuentra configurada la nube privada.
- Los servidores virtuales que manejan aplicaciones web.
- Los servidores virtuales de carpetas compartidas y servidores de archivos.

En el archivo “Anexo4 - Listado máquinas virtuales y backups” hoja N°1 “M. Virtuales”, se encuentra el listado de los servidores virtuales a los cuales se les continuará realizando copias de seguridad de la información con el software Veeam Backup, a continuación, una pequeña captura de este anexo.

N	Nombre	Tamaño utiliza	Tamaño reserva	Tamaño Reservado para sumar		Carpeta
1	antivirus	84,6 GB	133,6 GB	133,6	GB	Discovered virtual machine
2	DNSExterno	11,1 GB	11,1 GB	11,1	GB	Discovered virtual machine
3	Gredes	62,1 GB	62,1 GB	62,1	GB	Discovered virtual machine
4	Libelula	51,1 GB	51,1 GB	51,1	GB	Discovered virtual machine
5	mail	95,8 GB	95,8 GB	95,8	GB	Discovered virtual machine
6	MySql14	134,5 GB	304,1 GB	304,1	GB	Discovered virtual machine
7	Mysql14_Borrar_30Abril_2017	119,6 GB	304,1 GB	304,1	GB	Discovered virtual machine
8	Print Server	130,3 GB	130,3 GB	130,3	GB	Discovered virtual machine
9	Centos_Servidor_Mail_IredMail	102,1 GB	102,1 GB	102,1	GB	Discovered virtual machine
10	PRTG-DMZ	293,0 GB	316,1 GB	316,1	GB	Discovered virtual machine
11	Servidor_Windows_2019_Fileserver_Admon	876,1 GB	876,1 GB	876,1	GB	vm
12	sqlsis	139,9 GB	211,2 GB	211,2	GB	Discovered virtual machine
13	Ubuntu_Web_Prueba	92,4 GB	168,2 GB	168,2	GB	Discovered virtual machine
14	vCenter Server 6.7	568,1 GB	770,5 GB	770,5	GB	Discovered virtual machine
15	Web 14 2016	66,3 GB	101,1 GB	101,1	GB	Discovered virtual machine
16	Web_Administrativa	60,1 GB	60,1 GB	60,1	GB	Discovered virtual machine
17	weta	2,9 TB	2,9 TB	2969.6	GB	Discovered virtual machine
18	Servidor_Windows_2019_Fileserver	628,1 GB	628,1 GB	628,1	GB	vm
19	CentOS_Servidor_DNS02	54,1 GB	54,1 GB	54,1	GB	Discovered virtual machine
20	Windows10_1909_Remoto1	408,1 GB	408,1 GB	408,1	GB	vm
21	CarpetasCompartidas4	310,1 GB	384,1 GB	384,1	GB	Discovered virtual machine
22	CARLOS_BANNER_BORRAR_SEPTIEMBRE_2017	88,1 GB	88,1 GB	88,1	GB	Discovered virtual machine
23	CarpetasCompartidas5	384,2 GB	384,2 GB	384,2	GB	Discovered virtual machine
24	CarpetasCompartidas6	454,1 GB	454,1 GB	454,1	GB	Discovered virtual machine
25	CarpetasCompartidas3	395,2 GB	729,1 GB	729,1	GB	Discovered virtual machine
26	CarpetasCompartidas7	1,5 TB	1,5 TB	1536	GB	Discovered virtual machine

Figura 21. Máquinas virtuales para respaldar

- **Servidores virtuales que se proponen eliminar**
  En el archivo mencionado en el ítem anterior, se encuentra el listado de las máquinas virtuales que se deben eliminar, debido a que se encuentran apagadas por no ser usadas. No obstante, se muestra captura de pantalla de las 10 máquina que se proponen eliminar.

A	B	C	D	E	F	G
N	Nombre	Tamaño utiliza	Tamaño reserva	Tamaño Reservado para sumar		Carpeta
34	RedHat_Servidor_web_Plantilla	70,0 GB	72,2 GB	72,2	GB	Discovered virtual machine
63	RedHat_Seginfo	100,0 GB	102,2 GB	102,2	GB	Discovered virtual machine
80	vCenter-UPB	114,4 GB	122,6 GB	122,6	GB	Discovered virtual machine
82	Windows_Servidor_WSUS	1,1 TB	1,1 TB	1126.4	GB	Discovered virtual machine
83	Dnsbga	50,0 GB	51,2 GB	51,2	GB	Discovered virtual machine
87	Web_14_clon_bit	50,0 GB	51,2 GB	51,2	GB	Discovered virtual machine
88	crmupb	4,7 GB	5,4 GB	5,4	GB	Discovered virtual machine
113	moodlext	62,0 GB	124,1 GB	124,1	GB	Discovered virtual machine
114	mantisv	183,8 GB	187,0 GB	187	GB	Discovered virtual machine
116	Fastback	36,4 GB	63,2 GB	63,2	GB	Discovered virtual machine

Figura 22. Máquinas virtuales para eliminar

- **Backup de los servidores virtuales**
  En el archivo “Anexo4 - Listado máquinas virtuales y backups” hoja N°2 “Backups” y hoja N°3 “Backup copy”, se encuentra el listado de las copias de seguridad que se continúan realizando (backup y backup copy), sin embargo, se propone la reconfiguración de los puntos de restauración para así poder cumplir con la política de retención propuesta para cada backup y backup copy, de la siguiente manera.

  - **Backup mensual:** Cada copia de seguridad definida con frecuencia mensual se propone configurar de la siguiente manera:
    Puntos de restauración en Veeam Backup: 12

  - **Backup semanal:** Cada copia de seguridad definida con frecuencia semanal se propone configurar de la siguiente manera:
    Puntos de restauración en Veeam Backup: 4

  - **Backup diaria:** Cada copia de seguridad definida con frecuencia diaria se propone configurar de la siguiente manera:
    Puntos de restauración en Veeam Backup: 7

  - **Backup copy:** Cada backup copy que se le realiza a cada uno de los backup se propone configurar de la siguiente manera:
    Puntos de restauración en Veeam Backup: 12

- **Backups copy que hacen falta por programar**
  Durante las actividades desarrolladas en el diagnóstico, se verificó que cada backup tuviera su respectivo backup copy configurado para ser almacenado en los dos servidores NAS1 y NAS2, no obstante, se encontró que algunos backup

no contaban con su backup copy, por esta razón se muestran los siguientes backup copy se deben configurar.

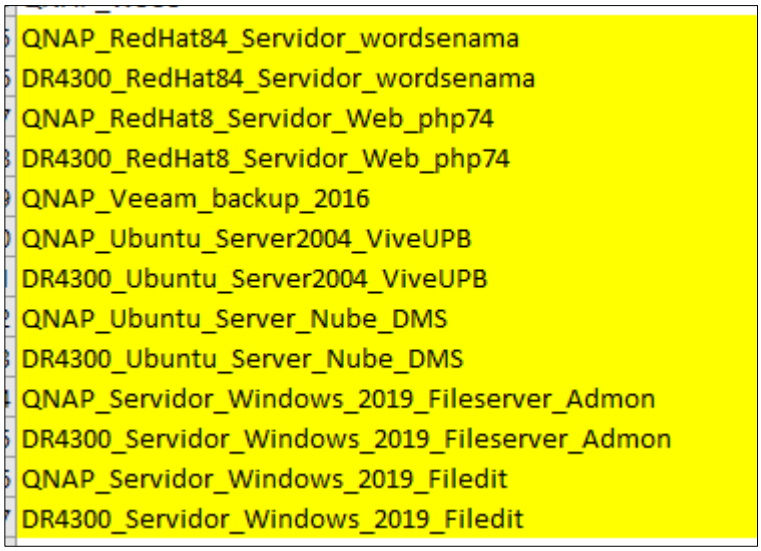


Figura 23. Backups copy para configurar

- **Backups que se proponen eliminar**

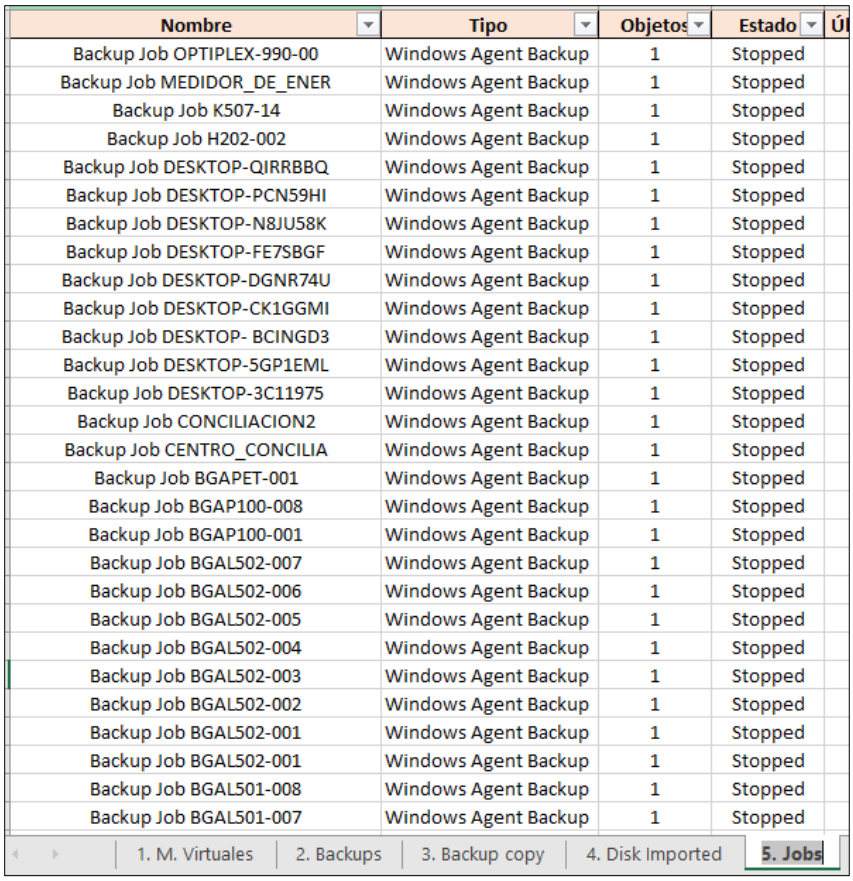
En el archivo mencionado anteriormente, hoja N°4 “Disk imported”, se encuentra el listado de 92 backups y backup copy que alguna vez estuvieron configurados y actualmente ya no se encuentran en funcionamiento, por esta razón se propone eliminarlos del sistema de copias de seguridad, pues se revisó con el personal de Infraestructura tecnológica y se encontró que la información que allí se encuentra ya no es relevante de retener. Por otro lado, se propone eliminar el backup copy llamado CLOUDCWC_RedHat_Servidor_NextCloud_nube2020, el cual se almacena en el repositorio de nube de prueba llamado CWC Backup Repository. Pues este backup copy es muy grande en tamaño y llenó la capacidad total de la nube de prueba.

N°	Nombre del job	Fecha de craciόn	Puntos de restauración	Repositorio	Plataforma
1	QNAP_WSUS	30/03/2017 7:20 p.m.	No existe	QNAP2	Vmware
2	QNAP_Web_Terceros	30/03/2017 12:30 p.m.		QNAP2	Vmware
3	QNAP_Web_SYS	30/03/2017 12:30 p.m.		QNAP2	Vmware
4	QNAP_Web_CMS	30/03/2017 11:30 p.m.		QNAP2	Vmware
5	QNAP_Web_Administrativa	30/03/2017 11:30 p.m.		QNAP2	Vmware
6	QNAP_Web_Academica	30/03/2017 10:30 p.m.		QNAP2	Vmware
7	QNAP_Web_14_2016	30/03/2017 10:30 p.m.		QNAP2	Vmware
8	QNAP_Vcenter UPB	31/03/2017 5:30 a.m.		QNAP2	Vmware
9	QNAP_simger_produccion	31/03/2017 9:30 a.m.		QNAP2	Vmware
10	QNAP_servidor NPS Radius	30/03/2017 4:30 p.m.		QNAP2	Vmware
11	QNAP_Repofiles	30/03/2017 7:30 p.m.		QNAP2	Vmware

Figura 24. Backups y Backup copy para eliminar

- **Nuevos backup copy propuestos a configurar en el repositorio de nube de pruebas CWC Backup Repository**
  Se propone que el repositorio “CWC Backup Repository” se configure para almacenar los backup de los nuevos servidores de archivos (file server) que se crearan en reemplazo de las carpetas compartidas.

- **Jobs de End Point que se proponen eliminar**
  Dado que desde el año 2020 a causa del trabajo remoto en casa se dejó de configurar estos Jobs, sin embargo, se siguen ejecutando en gran cantidad de computadores de usuarios finales, se propone que el listado del “Anexo4 - Listado máquinas virtuales y backups” hoja N°5 “Jobs” se le envíe al área de Hardware y software para que de forma gradual se desinstale el agente de EndPoint.



Nombre	Tipo	Objetos	Estado	Úl
Backup Job OPTIPLEX-990-00	Windows Agent Backup	1	Stopped	
Backup Job MEDIDOR_DE_ENER	Windows Agent Backup	1	Stopped	
Backup Job K507-14	Windows Agent Backup	1	Stopped	
Backup Job H202-002	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-QIRRBBQ	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-PCN59HI	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-N8JU58K	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-FE7SBGF	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-DGNR74U	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-CK1GGMI	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP- BCINGD3	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-5GP1EML	Windows Agent Backup	1	Stopped	
Backup Job DESKTOP-3C11975	Windows Agent Backup	1	Stopped	
Backup Job CONCILIACION2	Windows Agent Backup	1	Stopped	
Backup Job CENTRO_CONCILIA	Windows Agent Backup	1	Stopped	
Backup Job BGAPET-001	Windows Agent Backup	1	Stopped	
Backup Job BGAP100-008	Windows Agent Backup	1	Stopped	
Backup Job BGAP100-001	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-007	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-006	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-005	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-004	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-003	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-002	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-001	Windows Agent Backup	1	Stopped	
Backup Job BGAL502-001	Windows Agent Backup	1	Stopped	
Backup Job BGAL501-008	Windows Agent Backup	1	Stopped	
Backup Job BGAL501-007	Windows Agent Backup	1	Stopped	

1. M. Virtuales | 2. Backups | 3. Backup copy | 4. Disk Imported | 5. Jobs

Figura 25. Jobs para eliminar

- **Configuración de un nuevo repositorio de almacenamiento de las copias de seguridad**
  Dado que el servidor NAS DR4300 donde se almacena una de las dos copias de backup copy se encuentra casi lleno con un porcentaje de ocupación de

93% se propone configurar nuevamente estos backup en un nuevo servidor NAS que fue adquirido con capacidad de almacenamiento de 43,7 TB. Se propone que la información que actualmente se encuentra en el repositorio DR4300 se deje aproximadamente un año antes de ser borrada y que el listado que se encuentra en el “Anexo4 - Listado máquinas virtuales y backups” hoja N°6 “Backups para la nueva NAS”, se configure en el nuevo servidor NAS NX3240

Nombre	Tipo	Siguiente backup	Objetivo
NX3240_AGENTS	Windows Agent Backup Copy	<Continuous>	DR4300
NX3240_antivirus	VMware Backup Copy	<Continuous>	DR4300
NX3240_Apps	VMware Backup Copy	<Continuous>	DR4300
NX3240_Autoevaluacion	VMware Backup Copy	<Continuous>	DR4300
NX3240_BANCAPAGOS	VMware Backup Copy	<Continuous>	DR4300
NX3240_BANCAUPBW10	VMware Backup Copy	<Continuous>	DR4300
NX3240_blbdvirtual	VMware Backup Copy	<Continuous>	DR4300
NX3240_blvirtual	VMware Backup Copy	<Continuous>	DR4300
NX3240_CALLEXPRESS	VMware Backup Copy	<Continuous>	DR4300
NX3240_CarpetasCompartidas	VMware Backup Copy	<Continuous>	DR4300
NX3240_CarpetasCompartidas1	VMware Backup Copy	<Continuous>	DR4300
NX3240_CarpetasCompartidas2	VMware Backup Copy	<Continuous>	DR4300
NX3240_CarpetasCompartidas3	VMware Backup Copy	<Continuous>	DR4300

Figura 26. Backups para la nueva NAS

A continuación, se presenta el resumen general de las acciones de mejora a realizar y los servidores y copias de respaldo a eliminar.

Acciones de mejora	Eliminar
110 Servidores virtuales para respaldar	10 Servidores virtuales
13 Backups copy para programar	92 Backups y Backups copy
Configurar nuevos backups en el repositorio de nube de pruebas CWC	Todos los Jobs de EndPoint
Configurar un nuevo repositorio de almacenamiento de las copias de seguridad	

Tabla 16. Acciones para realizar

9.5.5 Recomendaciones de acuerdo con la lista de verificación de cumplimiento de las reglas o buenas prácticas

Luego de evaluar la actual configuración del sistema de copias de seguridad de la Seccional utilizando el instrumento “Anexo3 - Lista de verificación de cumplimiento de las reglas o buenas prácticas”, se emiten las siguientes recomendaciones como propuesta de mejora al actual sistema:

- Se recomienda adicionar un medio de almacenamiento de copias de seguridad diferente a los discos.
- Se recomienda contratar una nube externa como almacenamiento adicional de las copias de seguridad.
- Se recomienda contratar el soporte de Veeam backup. Para esto los cambios de versiones deben ser acompañados por expertos de Veeam Backup.
- Se recomienda contratar el soporte de Veeam backup y solicitar la instalación y configuración de una máquina con la herramienta Veeam ONE que ayuda a detectar el ransomware
- Preparar, programar y realizar jornadas educativas contra ransomware, al menos una vez al año.
- Se recomienda contratar el licenciamiento de Veeam Continuos Data Protection (CDP) para recuperación ante desastres y así armar un plan de continuidad del negocio.

9.5.6 Nuevo esquema propuesto para el sistema de copias de seguridad

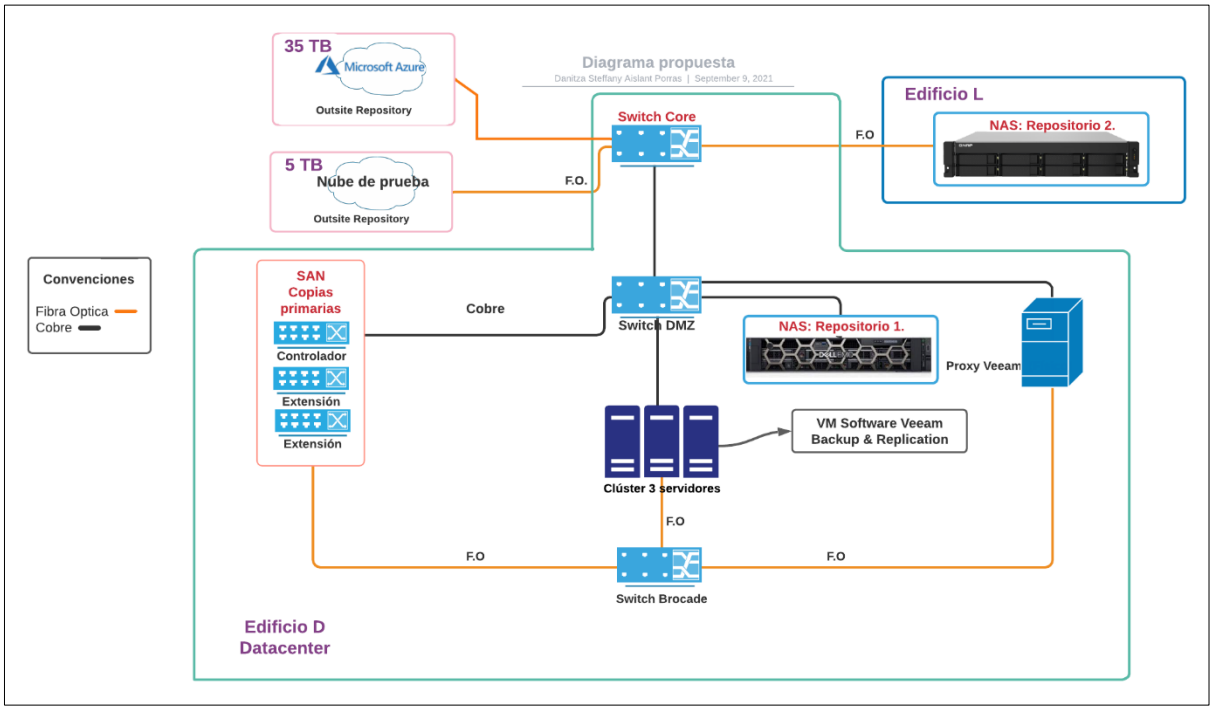


Figura 27. Diagrama de la propuesta de copias de seguridad

Dentro de los cambios significativos del diagrama propuesto y basados en las recomendaciones anteriores, se encuentran el cambio de uno de los repositorios para backup copy por ocupación de su almacenamiento total y la agregación de un repositorio externo de nube con una capacidad de 35 TB. De esta forma se garantiza tener una infraestructura de Veeam Backup en un sitio externo sin acceso a internet (fuera del sitio - offline) para así inhibir la introducción a ransomware y recuperar las copias ante otro tipo de desastres.

9.5.7 Propuesta económica de un nuevo repositorio como infraestructura de nube (Repositorio Outsite)

Se identifica que el licenciamiento de Veeam actualmente usado por la universidad no requiere modificaciones o adición de algún otro tipo de licencia para implementar un modelo de Outsite Repository para el archivado de backup en la nube. De acuerdo con lo anterior se genera la siguiente propuesta comercial, en la cual se pueden encontrar los siguientes apartados que cuales son necesarios para la implementación del servicio descrito:

- Infraestructura y recursos requeridos en la nube para la implementación de la solución.
- Servicios profesionales para la configuración y despliegue de los componentes requeridos, así como de su parametrización.

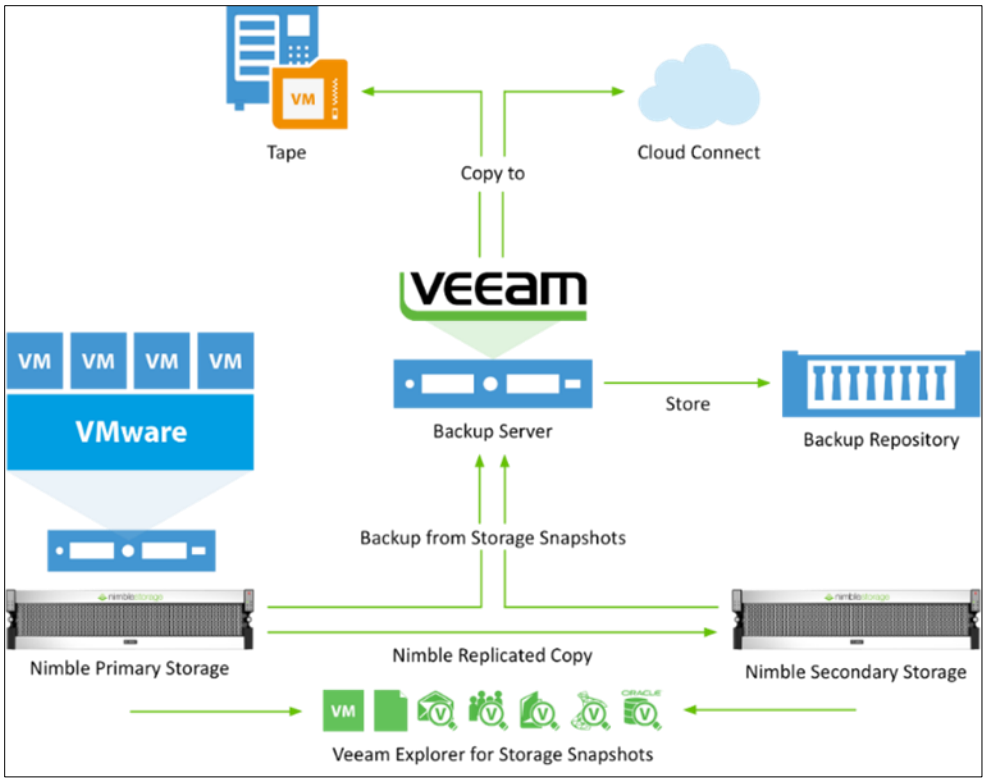


Figura 28. Modelo de Outsite Repository

Resumen del alcance de servicios

- Configuración del Cloud Connect en un servidor Veeam Backup ya instalado.
- Configuración de Repositorio Outsite, para la réplica de los respaldos (Blob Storage de 35 TB).
- Configurar los parámetros de replicación del Cloud Connect (Frecuencia de réplica de datos respaldados a repositorio Outsite)
- Definir límites de almacenamiento en Veeam para la información replicada.
- Definición de políticas de retención para la réplica Outsite.

Propuesta económica de infraestructura de repositorio en la nube

Propuesta económica Infraestructura en la nube			
ITEM	Cantidad	Valor Estimado Mensual	
(ALMACENAMIENTO) Block Blob Storage, General Purpose V2, LRS Redundancy, Hot Access Tier, 35 TB Capacity - Pay as you go, 100,000 Write operations, 100,000 List and Create Container Operations, 100,000 Read operations, 100,000 Archive High Priority Read, 1 Other operations. 1,000 GB Data Retrieval, 1,000 GB Archive High Priority Retrieval, 1,000 GB Data Write	1	USD	684.66
(DATA TRANSFER) Internet egress, 1024 GB outbound data transfer from East US 2 routed via Public Internet	1	USD	84.50
(SOPORTE o GARANTÍA MICROSOFT) Microsoft Support Standard level	1	USD	100.00
Total Mensual Estimado		**USD**	**869.16**
Total Estimado para 12 meses		**USD**	**10,429.96**

Figura 29. Propuesta económica de infraestructura N°1

Servicios			
ITEM	Periodos a pagar	Varlor total antes de IVA	
Servicio de instalación y configuración de Veeam cloud Connect con política de replicación Outsite	1	**USD**	**840.26**

Figura 30. Propuesta económica de infraestructura N°2

Respecto a esto cabe mencionar que:

- Actualmente los servicios de infraestructura en nube se encuentran por ley exentos de IVA, en Colombia.
- Se recomienda presupuestar USD $12.000 aproximadamente para la contratación anual del servicio de infraestructura en nube con el fin de incluirlo como repositorio para mantener una copia de respaldo fuera del sitio.

10 CONCLUSIONES

- La búsqueda de los referentes bibliográficos sirvió para tomar como punto de partida una manera de clasificar la información digital Institucional.
- El diagnóstico de los activos de información fue de gran utilidad para consolidar, filtrar y conocer la información que necesita de una copia de seguridad o, por el contrario, se debería eliminar.
- El desarrollo del diagnóstico de las copias de respaldo contribuyó al proyecto en gran medida, pues con este se logró verificar el cumplimiento de los requisitos que establece Veeam Backup.

- Con ayuda de la lista de verificación se lograron establecer recomendaciones de buenas prácticas según Veeam Backup para el manejo de las copias de seguridad

11 REFERENCIAS BIBLIOGRÁFICAS

[1] "Universidad Pontificia Bolivariana." https://www.upb.edu.co/es/home (accessed Mar. 02, 2021).

[2] B. D0UOC UC, "Definición y propósito de la Investigación Aplicada," 2018. http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada (accessed Feb. 03, 2021).

[3] D. Rodríguez, "Investigación aplicada: características, definición, ejemplos," *17 de Septiembre*, 2020. https://www.lifeder.com/investigacion-aplicada/ (accessed Feb. 03, 2021).

[4] Maravillosa es la mente, "Diseños de investigación: enfoque cualitativo y cuantitativo," *10 de Septiembre*, 2018. https://lamenteesmaravillosa.com/disenos-de-investigacion-enfoque-cualitativo-y-cuantitativo/ (accessed Feb. 03, 2021).

[5] J. M. Parra, "La investigación o enfoque cualitativo," *29 de Junio*, 2013. http://yamilesmith.blogspot.com/2012/06/la-investigacion-o-enfoque-cualitativo.html (accessed Feb. 03, 2021).

[6] C. C. Castillo, *Fundamentos de preservación digital a largo plazo*, Comité Edi. Bogotá D.C., 2018.

[7] "Instrumentos de gestión de información pública | Superintendencia de Industria y Comercio," 2020. https://www.sic.gov.co/node/18546 (accessed Apr. 27, 2021).

[8] Mintic, "Seguridad y privacidad de la información," vol. 1.0.0, p. 6,7, 2016, [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf.

[9] Organización de los Estados Americanos, *Clasificación de datos*, Edición 6. 2019.

[10] Icontec, *Norma técnica NTC-ISO/IEC Colombiana 27001*. Colombia, 2006, p. 25.

[11] Icontec, *Norma técnica NTC-ISO/IEC Colombiana 17799*. Colombia, 2005, p. 39.

[12] Procuraduría general de la nación, "Instructivo para la aplicación de las tablas de retención y valoración documental, las transferencias documentales y la eliminación," 2009. https://www.procuraduria.gov.co/portal/media/file/modulo_calidad/mapa_proceso/282_INS-GD-AS-008_Instructivo_aplicación_de_TRD_y_TVD_transferencias_y_eLI (MA).pdf.