

ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN



Propuesta de mejora de la gestión de respaldos de información de la Bolsa de Valores de Quito, 2022

Trabajo de Investigación

para optar el Grado a Nombre de la Nación de:

Maestro en

Gestión de Tecnologías de la Información

Autores:

Bach. Acosta Castillo, Henry Ramiro

Director:

Dr. Luis Enrique Espinoza Villalobos

TACNA- PERÚ

2023

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

Contenido

RESUMEN	10
INTRODUCCIÓN	11
CAPITULO I: Antecedentes de Estudio	14
1.1. Título del Tema	15
1.2. Planteamiento del Problema	15
1.3. Exposición del problema	15
1.4. Proyección del problema.....	16
1.5. Necesidad del estudio	16
1.6. Objetivos de la Investigación.....	17
1.7. Objetivo General	17
1.8. Objetivos Específicos	17
1.9. Metodología.....	17
1.10. Justificación.....	19
1.11. Principales definiciones.....	20
1.12. Alcances y limitaciones	23
CAPITULO II: Marco Teórico	25
2.1. Conceptualización de gestión de respaldos de información.....	25
2.1.1. Gestión de TI	25
2.1.2. Respaldos de información	38
2.2. Importancia de la variable gestión de respaldos de información	58
2.3. Análisis comparativo	93

2.4.	Análisis crítico	145
CAPITULO III: Marco Referencial		149
3.1.	Reseña histórica.....	149
3.1.1.	Obligaciones.....	149
3.2.	Filosofía organizacional.....	151
3.2.1.	Visión.....	151
3.2.2.	Misión	151
3.3.	Política de calidad	151
3.3.1.	Objetivos.....	151
3.4.	Diseño organizacional	152
3.4.1.	Estructura organizacional	152
3.4.2.	Funciones de las gerencias (áreas).....	153
3.5.	Productos y/o servicios.....	157
3.6.	Diagnóstico organizacional.....	157
CAPITULO IV: Resultados		171
4.1.	Propuesta de mejora	171
4.1.1.	Diagnóstico	171
4.1.2.	Diseño de la mejora	172
4.1.3.	Mecanismos de control.....	189
Conclusiones		198
Recomendaciones		199
BIBLIOGRAFÍA		201
ANEXOS		206

Índice de Tablas

Tabla 1 <i>Comparativa de tipos de respaldo</i>	58
Tabla 2 <i>Relevancia - gestión de TI</i>	59
Tabla 3 <i>Relevancia - políticas y estrategias de gestión de información</i>	60
Tabla 4 <i>Relevancia - infraestructura de TI</i>	62
Tabla 5 <i>Relevancia - seguridad de la información</i>	63
Tabla 6 <i>Relevancia - continuidad del negocio</i>	64
Tabla 7 <i>Relevancia – plan de continuidad</i>	66
Tabla 8 <i>Relevancia – objetivos de un plan de continuidad</i>	69
Tabla 9 <i>Relevancia – etapas de un plan de continuidad</i>	70
Tabla 10 <i>Comparativo – tipos de plan de continuidad</i>	72
Tabla 11 <i>Relevancia – información</i>	74
Tabla 12 <i>Relevancia – ciclo de vida de la información</i>	76
Tabla 13 <i>Comparativo – metodologías para gestionar el ciclo de vida de la información</i>	78
Tabla 14 <i>Relevancia – tipos de información</i>	80
Tabla 15 <i>Relevancia – valor de la información</i>	84
Tabla 16 <i>Relevancia – gestión de respaldos</i>	88
Tabla 17 <i>Relevancia – tipos de respaldos</i>	90
Tabla 18 <i>Comparativo - gestión de TI</i>	93
Tabla 19 <i>Comparativo - políticas y estrategias de gestión de información</i>	96
Tabla 20 <i>Comparativo - infraestructura de TI</i>	99
Tabla 21 <i>Comparativo - seguridad de la información</i>	101
Tabla 22 <i>Comparativo - continuidad del negocio</i>	103

Tabla 23 <i>Comparativo – plan de continuidad</i>	106
Tabla 24 <i>Comparativo – objetivos de un plan de continuidad</i>	109
Tabla 25 <i>Comparativo – etapas de un plan de continuidad</i>	112
Tabla 26 <i>Comparativo – tipos de plan de continuidad</i>	114
Tabla 27 <i>Comparativo – información</i>	117
Tabla 28 <i>Comparativo – ciclo de vida de la información</i>	120
Tabla 29 <i>Comparativo – metodologías para gestionar el ciclo de vida de la información</i>	124
Tabla 30 <i>Comparativo – tipos de información</i>	127
Tabla 31 <i>Comparativo – valor de la información</i>	133
Tabla 32 <i>Comparativo – gestión de respaldos</i>	138
Tabla 33 <i>Comparativo – tipos de respaldos</i>	141
Tabla 34 <i>Lugares actuales de almacenamiento</i>	159
Tabla 35 <i>Crecimiento de Información</i>	160
Tabla 36 <i>Crecimiento porcentual (constante)</i>	161
Tabla 37 <i>Crecimiento porcentual (variación)</i>	162
Tabla 38 <i>Propuesta de mejora</i>	173
Tabla 40 <i>Tipo, periodicidad y permanencia de backup</i>	178
Tabla 41 <i>Propuesta de política de clasificación de los activos de información en la BVQ</i>	179
Tabla 42 <i>Propuesta de inventario de activos en la BVQ</i>	181
Tabla 43 <i>Propuesta de coordinación entre las gerencias y colaboradores</i> ..	183
Tabla 44 <i>Evaluación de las tecnologías existentes para la realización de los respaldos de información</i>	185
Tabla 45 <i>Propuesta de actualización de tecnología</i>	187

Tabla 46 <i>Propuestas de definición de roles y responsabilidades</i>	189
Tabla 47 <i>Propuestas de controles</i>	191
Tabla 48 <i>Indicadores de crecimiento y gestión de espacio de almacenamiento de los respaldos de información de la BVQ</i>	193
Tabla 49 <i>Propuesta de estrategias de análisis de costo beneficios.</i>	196

Índice de Figuras

Figura 1 <i>Usos de la palabra información</i>	42
Figura 2 <i>Obligaciones de BVQ</i>	150
Figura 3 <i>Objetivos de la BVQ</i>	151
Figura 4 <i>Estructura organizacional de BVQ</i>	152
Figura 5 <i>Funciones gerenciales de BVQ</i>	153
Figura 6 <i>Gerencia legal de BVQ</i>	154
Figura 7 <i>Gerencia comercial de BVQ</i>	154
Figura 8 <i>Gerencia de tecnología de BVQ</i>	155
Figura 9 <i>Lineamientos de la Gerencia administrativa, Financiera y Recursos Humanos</i>	156
Figura 10 <i>Crecimiento de Información</i>	161
Figura 11 <i>Matriz de información por cada funcionario/departamento</i>	163
Figura 12 <i>Tipo de información por funcionario</i>	164
Figura 13 <i>Diagnóstico organizacional (FODA)</i>	165
Figura 14 <i>Diagrama de Ishikawa</i>	167
Figura 15 <i>Gestión de respaldos de información</i>	176

DEDICATORIA

Dedico mi trabajo de investigación a Dios, por darme la fuerza y sabiduría necesaria para culminar esta meta.

A mi esposa y mi hija, por todo su amor y por motivarme a seguir hacia adelante.

Y, finalmente dedico a ustedes este logro amado padres, como una meta más conquistada.

RESUMEN

La presente investigación se enfocó en mejorar la gestión de los respaldos de información crítica en la Bolsa de Valores de Quito (BVQ), debido a la falta de coordinación efectiva entre actores y la identificación de riesgos y vulnerabilidades en la gestión actual de la información. La BVQ es una organización dedicada al mercado bursátil en el Ecuador y, por tanto, es crucial que su información crítica esté segura y disponible en todo momento. Por ello, para realizar esta investigación, se empleó una metodología basada en la identificación de problemas en la gestión actual de la información, seguido de la propuesta de una mejora basada en las mejores prácticas y mecanismos de control. Se recomendó la continuidad del negocio, la evaluación periódica de riesgos y vulnerabilidades, la implementación de sistemas de gestión de la calidad y seguridad de la información, la capacitación y conciencia en seguridad de la información en los colaboradores, y la colaboración con otras instituciones del sector financiero y bursátil. Por lo tanto, la implementación de la propuesta de mejora permitirá reducir significativamente los riesgos y vulnerabilidades identificados, garantizando la seguridad y disponibilidad de la información crítica de la BVQ. La investigación concluye que la BVQ debe adoptar medidas preventivas para la gestión de su información crítica y fomentar una cultura de seguridad de la información en todos los niveles de la organización. La propuesta de mejora también contribuirá a consolidar a la BVQ como una organización segura y confiable en el manejo de la información crítica.

Palabras claves: Gestión de información, riesgos y vulnerabilidades, mejores prácticas, seguridad de la información, sector financiero.

INTRODUCCIÓN

A continuación, se realiza una breve explicación del contenido del trabajo de investigación:

CAPÍTULO I: Antecedentes de Estudio

En este capítulo se presenta el título del tema de investigación, se plantea el problema que se aborda en el estudio, se explica en detalle el problema y se proyecta hacia el futuro para resaltar la importancia de su solución. Además, se establece la necesidad del estudio, se definen los objetivos de la investigación y se explica la metodología utilizada en la investigación. También se justifica la relevancia del estudio y se establecen las principales definiciones, alcances y limitaciones.

CAPÍTULO II: Marco Teórico

En este capítulo se conceptualizan los tópicos claves que se abordan en la investigación, tales como la gestión de TI, los respaldos de información, entre otros. También se explica la importancia de estas variables, se realiza un análisis comparativo y crítico, así como se establecen las implicaciones que tienen para la solución del problema planteado en el capítulo anterior.

CAPÍTULO III: Marco Referencial

En este capítulo se presenta una reseña histórica de la organización objeto de estudio, se explica su filosofía organizacional, política de calidad, diseño organizacional, funciones de las gerencias, productos y servicios que ofrece, y se realiza un diagnóstico organizacional (FODA), como un diagrama de Ishikawa.

CAPÍTULO IV: Resultados

En este capítulo se presenta la propuesta de mejora diseñada para la gestión de respaldos de información en la BVQ. La propuesta de mejora se compone de tres partes: el diagnóstico, el diseño de la mejora y los mecanismos de control.

Inicialmente, se presenta un breve resumen del diagnóstico que se realizó previamente. Luego, se describirá en detalle la propuesta de mejora, que tiene como objetivo mejorar la eficiencia y eficacia en la gestión de respaldos de información en la BVQ. Para ello, se establecerán los mecanismos de control que permitirán medir la efectividad de la propuesta y se establecerá un plan de acción para la evaluación de su implementación.

CONCLUSIONES Y RECOMENDACIONES

En esta sección se presentan las conclusiones a las que se llegó en el estudio, en relación a los objetivos planteados. Se hace una síntesis de los resultados obtenidos, se evalúa la relevancia y efectividad del Plan de Continuidad del Negocio implementado y se discuten las implicaciones y posibles aplicaciones de los resultados en otras organizaciones.

Además, se presentan una serie de recomendaciones para el mejoramiento y optimización del Plan de Continuidad del Negocio, basadas en las lecciones aprendidas y en la experiencia adquirida durante la implementación del plan. Se establecen también recomendaciones para futuras investigaciones en el tema, a partir de las limitaciones y alcances del estudio realizado.

REFERENCIAS BIBLIOGRÁFICAS

En esta sección se presentan las referencias bibliográficas utilizadas en el trabajo de investigación, ordenadas según las normas de citación correspondientes. Se incluyen tanto las fuentes consultadas como las citadas en el texto del trabajo, en formato APA7.

ANEXOS: Información complementaria o de apoyo

En esta sección se incluyen los anexos correspondientes al trabajo de investigación, tales como entrevistas realizadas, cuestionarios aplicados, registros y

documentos de apoyo, entre otros. Se presentan en un orden consecutivo y se indican en el texto principal del trabajo para facilitar su ubicación.

CAPÍTULO I: Antecedentes de Estudio

El presente capítulo presenta como objetivo facilitar una visión general de los antecedentes que respaldan el desarrollo del trabajo de investigación. En este sentido, se abordarán diferentes componentes que permitirán contextualizar y comprender la relevancia del tema de estudio. En primer lugar, se presentará el planteamiento del problema, con el fin de exponer la situación problemática que se aborda y su proyección a futuro.

Asimismo, se explicará cómo el trabajo de investigación contribuirá a la solución o mejora de esta situación. Posteriormente, se describirán los objetivos de la investigación. Estos objetivos son acciones concretas que se llevarán a cabo en el proceso de investigación para cumplir con el propósito general del estudio.

En relación a la metodología, se detallarán las operaciones metodológicas que se utilizarán para alcanzar los objetivos. Asimismo, se expondrá la justificación del estudio, presentando los motivos que fundamentan la factibilidad académica del plan de trabajo de investigación. En este sentido, se abordarán aspectos teóricos, metodológicos y prácticos que sustentan la relevancia y la contribución del estudio.

En la sección de definiciones fundamentales, se explicará el sentido que las variable(s) y/o tópicos principales del tema tienen para el trabajo de investigación o tesis. Este procedimiento permitirá contar con una comprensión detallada y exacta de los conceptos que se utilizarán durante la investigación.

El apartado de alcances y limitaciones describirá el ámbito geográfico, sectorial u organizacional que se abordará en el desarrollo de la investigación. De esta manera, se especificarán los límites y alcances del estudio. Finalmente, se presentará el cronograma de actividades, en un diagrama de Gantt, donde se detallarán las actividades que se realizarán durante el proceso de investigación y el tiempo que se

dedicará a cada una de ellas. De esta forma, se tendrá un plan detallado de la ejecución del estudio.

1.1. Título del Tema

Propuesta de mejora para la gestión de respaldos de información para la continuidad del negocio de la BVQ, 2022.

1.2. Planteamiento del Problema

1.3. Exposición del problema

El crecimiento descontrolado y la falta de estandarización en la gestión de la información almacenada en la BVQ han generado problemas de seguridad y de acceso a la información en numerosas ocasiones. A medida que ha transcurrido el tiempo, la generación de información dentro de la empresa ha aumentado considerablemente, lo que incluye bases de datos, aplicaciones informáticas en desarrollo y en producción, así como su código fuente e información digital generada por los usuarios a diario, la cual se considera de gran importancia para las tareas diarias de trabajo (BVQ, 2023).

A medida que se automatizan procesos, sistemas y se generan nuevos productos, la cantidad de información relacionada con líneas de código, programas y bibliotecas, así como los repositorios de bases de datos, también aumenta. La automatización avanza debido a la evolución natural de la tecnología, así como a eventos inesperados como los confinamientos ocasionados por pandemias y otros factores sociales y naturales. Con la creciente digitalización, los documentos físicos se han convertido en documentos digitales que se suman a la información existente, lo que aumenta rápidamente el número y tamaño de la información (Romero, 2019).

Además, existe la falta de un estándar para el almacenamiento óptimo de esta información, lo que incluye la falta de estándares para la nomenclatura de archivos, la

ubicación del almacenamiento, la categorización, la importancia, el contenido, el propietario, el tipo, la frecuencia y el tamaño. Esta falta de estandarización puede causar una serie de problemas, como la pérdida de información importante o la imposibilidad de recuperarla, la redundancia de datos, la falta de coherencia y la ineficiencia en la gestión de la información (Henao, 2021).

Por lo anteriormente expuesto, se puede indicar que la gestión efectiva de los respaldos de información es esencial para garantizar la continuidad del negocio, la eficiencia operativa y el cumplimiento normativo y legal. Por lo tanto, es importante abordar el problema de la falta de estandarización y el crecimiento descontrolado de la información almacenada en la BVQ, para mejorar la gestión de respaldos de información y garantizar que la información crítica esté disponible en todo momento.

1.4. Proyección del problema

Para almacenar adecuadamente la información es necesario conocer todos los detalles de la información, como es su tamaño, para en base a este poder dimensionar los medios y lugares de almacenamiento, ya que si no se controla adecuadamente; se corre el riesgo que la información no esté segura, y no se puedan gestionar los respaldos de una manera óptima y adecuada.

1.5. Necesidad del estudio

Es fundamental que la organización pueda garantizar la continuidad del negocio mediante un adecuado respaldo de la información crítica y su disponibilidad en el momento necesario. Sin embargo, debido al crecimiento descontrolado y la falta de estandarización en la gestión de la información almacenada, la BVQ ha enfrentado problemas de seguridad y acceso a la información en varias ocasiones. En este sentido, establecer directrices para un correcto manejo, administración y gestión de la información se vuelve crucial para garantizar la seguridad y disponibilidad de la

información crítica en todo momento, lo que permitirá que la institución opere de manera efectiva y eficiente a lo largo del tiempo.

1.6. Objetivos de la Investigación

1.7. Objetivo General

Establecer las directrices necesarias y plasmar en un documento; para mejorar sustancialmente el manejo, administración y gestión de los respaldos de información, para garantizar la continuidad del negocio de la Bolsa de Valores de Quito "BVQ".

1.8. Objetivos Específicos

Realizar un diagnóstico detallado del estado actual de los procesos de manejo, administración y gestión de los respaldos de información en la BVQ.

Diseñar una propuesta de mejora que contemple la implementación de procesos y procedimientos estandarizados para el manejo, administración y gestión de los respaldos de información en la BVQ, con el fin de garantizar la seguridad y disponibilidad de la información crítica.

Establecer los mecanismos de control necesarios para garantizar el cumplimiento de los procesos y procedimientos establecidos en la propuesta de mejora, incluyendo la definición de roles y responsabilidades, la implementación de herramientas tecnológicas.

Realizar recomendaciones específicas sobre el manejo, administración y gestión de los respaldos de información en la BVQ, con el objetivo de optimizar los procesos existentes y garantizar la continuidad del negocio ante posibles incidentes o desastres.

1.9. Metodología

En esta sección se describe la metodología que se utilizará para llevar a cabo el estudio de la gestión de la información y los respaldos en la empresa BVQ. La

metodología se enfoca en la recolección de información detallada de las bases de datos, aplicaciones y documentación generada por los diferentes departamentos y funcionarios de la organización. Además, se realizará un análisis exhaustivo de la información recopilada para identificar los problemas y oportunidades de mejora en la gestión de la información y los respaldos. La metodología también incluye la propuesta de un plan de acción para implementar cambios y establecer mecanismos de control para garantizar la correcta implementación y medir el éxito de la implementación de la propuesta. A continuación, se presentan los pasos necesarios para la mejora:

- Se realizará el levantamiento de información de las bases de datos, aplicaciones e información generada por cada departamento y funcionarios.
- Por cada grupo de información se recolectará la información referente a nombres de archivos, lugar de almacenamiento, categorización, importancia, contenido, propietario, tipo, frecuencia y tamaño. Y se documentará en una matriz.
- Se realizará el respectivo análisis de la información levantada y en función del análisis; se procederá a clasificar y estandarizar la información.
- Se realizará el inventario de los medios de almacenamiento, en donde se obtendrá su ubicación y tamaño de almacenamiento.
- Con la información obtenida, se presentará la propuesta para una mejor administración y gestión de respaldos, así como una adecuada gestión de la información en lo que se refiere a la estandarización de nombres y almacenamiento.

- Se diseñarán indicadores para medir el éxito de la implementación de la propuesta, tales como la frecuencia de respaldo, la disponibilidad de información y la eficacia de los mecanismos de control.
- Se establecerán mecanismos de control para garantizar la correcta implementación de la propuesta, y se diseñarán planes de acción para corregir desviaciones identificadas durante la implementación.
- Se realizarán recomendaciones adicionales para el manejo de la información, basadas en los hallazgos y análisis realizados.

1.10. Justificación

La presente investigación tiene como objetivo mejorar sustancialmente el manejo, administración y gestión de los respaldos de información en la BVQ, con el fin de garantizar la continuidad del negocio. La necesidad de esta propuesta surge debido al crecimiento descontrolado y no estandarizado de la información generada en la BVQ, lo que ha llevado a que la información no esté segura, no se respalde correctamente y en muchas ocasiones, no sea de fácil acceso o simplemente no se encuentre.

En la justificación teórica, se considerará la teoría y las recomendaciones de autores especializados en la gestión y administración de la información, tales como Davenport y Prusak (1997) mencionado en Villasana *et al.* (2021), quienes mencionan la importancia de contar con un buen sistema de gestión de la información para mejorar el rendimiento y la competitividad de las organizaciones. Además, se revisarán teorías y conceptos relacionados con la estandarización de nombres y almacenamiento de información para garantizar su fácil recuperación y acceso.

En la justificación metodológica, se utilizarán técnicas y herramientas como la recolección de datos y la elaboración de matrices para el levantamiento de

información. Además, se realizará un análisis de la información obtenida para clasificar y estandarizar la información, y se elaborará un inventario de los medios de almacenamiento. Con base en esta información, se presentará una propuesta para una mejor administración y gestión de respaldos, así como un adecuado manejo de la información.

En cuanto a la justificación práctica, se beneficiarán directamente la BVQ y sus trabajadores, quienes podrán contar con un sistema de gestión de información más eficiente y seguro, lo que se traducirá en una mejor continuidad del negocio y una mayor competitividad en el mercado de valores. Asimismo, se beneficiarán indirectamente los clientes y consumidores de la BVQ, quienes contarán con una institución más confiable y segura para realizar sus inversiones.

1.11. Principales definiciones

A continuación, se presenta una sección de definiciones clave que son relevantes para la comprensión del presente trabajo de fin de máster. Estas definiciones son necesarias para establecer una base conceptual sólida que permita una mejor comprensión de los conceptos y temas abordados en el estudio.

Administración de la información: Es la planificación, organización, dirección y control de los procesos y recursos involucrados en la gestión de la información de una organización, con el fin de asegurar su disponibilidad, integridad, confidencialidad y calidad (Nyemba, 2018).

Alertas de control de espacio y frecuencia: Son las notificaciones automáticas generadas por los sistemas de gestión de información de una organización para informar sobre la falta de espacio disponible en los medios de almacenamiento o la necesidad de realizar respaldos de forma periódica para asegurar la continuidad del negocio (Gupta y Goyalm, 2020).

Almacenamiento en la nube: Es una tecnología que permite almacenar, gestionar y acceder a datos y archivos a través de internet en servidores remotos en lugar de almacenarlos en dispositivos físicos locales, como discos duros o memorias USB (Gupta y Goyal, 2020).

Caseteras de cinta magnética (DAT): Son un tipo de dispositivo de almacenamiento de datos en cinta magnética que se utilizó principalmente en la década de 1990 para realizar copias de seguridad de datos y para el almacenamiento de archivos de audio digital. (Gupta y Goyal, 2020).

Categorización de información: Es el proceso de clasificar y agrupar la información de una organización en función de sus características, propiedades o atributos comunes, con el fin de facilitar su gestión y uso (Smallwood, 2019).

Copia Offsite: Se refiere a una copia de seguridad de datos que se almacena en un lugar fuera del sitio principal donde se encuentra la información original. Esta copia adicional es importante para garantizar la recuperación de datos en caso de un desastre o una falla en el sitio principal. Al mantener una copia de los datos fuera del sitio principal, se minimiza el riesgo de pérdida de datos en caso de incendio, inundación, terremoto u otra emergencia que pueda afectar al sitio principal (Smallwood, 2019).

Continuidad del negocio: Es la capacidad de una organización para mantener sus operaciones y servicios críticos ante situaciones de emergencia o desastres que puedan interrumpir su funcionamiento normal (Elder y Elder, 2019).

Estandarización de nombres y almacenamiento: Es el proceso de establecer reglas y convenciones para nombrar y organizar los archivos, así como carpetas que contienen la información de una organización, con el fin de facilitar su identificación, acceso y gestión (Smallwood, 2019).

Gestión de la información: Es el conjunto de procesos y herramientas utilizados para adquirir, organizar, almacenar, proteger, mantener, distribuir y utilizar la información de una organización de manera efectiva y eficiente (Nyemba, 2018).

Indicadores de crecimiento de información: Son las métricas o medidas utilizadas para evaluar y monitorear el aumento o disminución de la cantidad de información almacenada por una organización en un periodo determinado (Room *et al.*, 2021).

Log de almacenamiento: También conocido como registro de transacciones, es un archivo que registra todas las operaciones de escritura que ocurren en una base de datos o sistema de almacenamiento. Cada vez que se realiza una transacción o cambio en la base de datos, se registra en el log de almacenamiento para poder recuperar esa información en caso de un fallo del sistema o de la necesidad de hacer una copia de seguridad (Room *et al.*, 2021).

Medios de almacenamiento: Son los dispositivos físicos o virtuales utilizados para guardar y preservar la información de una organización, tales como discos duros, cintas magnéticas, nubes de almacenamiento, entre otros (Smallwood, 2019).

Memoria RAM: La memoria RAM (Random Access Memory) es un tipo de memoria de acceso aleatorio que se utiliza en los ordenadores para almacenar temporalmente los datos y programas que el procesador necesita para trabajar en tiempo real. La RAM se considera una memoria volátil, ya que su contenido se pierde cuando se apaga el ordenador (Gupta y Goyal, 2020).

Memoria ROM: La Memoria ROM (Read-Only Memory o memoria de solo lectura en español) es un tipo de memoria no volátil que se utiliza para almacenar datos que no necesitan ser modificados o borrados con frecuencia. A diferencia de la memoria RAM, que es de lectura y escritura, la memoria ROM es de solo lectura, lo que significa que solo se puede leer la información que se ha grabado en ella (Gupta y Goyal, 2020).

Propietario de la información: Es la persona o entidad responsable de la información de una organización, ya sea por haberla creado, adquirido o gestionado (Smallwood, 2019).

Respaldo de información: Es el proceso de crear y guardar copias de seguridad de los datos de una organización en un medio de almacenamiento secundario con el fin de protegerlos ante posibles pérdidas o daños (Nyemba, 2018).

Unidades de Disco Duro portátiles: Es un dispositivo de almacenamiento externo que se conecta a una computadora a través de un puerto USB y permite almacenar y transferir datos de manera portátil (Gupta y Goyal, 2020).

Unidades de Disco Rígido o “Duro”: Son dispositivos de almacenamiento de datos no volátiles que se utilizan en computadoras y otros dispositivos electrónicos para almacenar y recuperar información de forma digital. (Gupta y Goyal, 2020).

Unidades de Memoria Flash: Son dispositivos de almacenamiento de datos no volátiles que utilizan memoria flash para almacenar y recuperar información digital. Son pequeñas, portátiles y tienen una capacidad de almacenamiento que va desde unos pocos megabytes hasta varios terabytes. (Gupta y Goyal, 2020).

1.12. Alcances y limitaciones

La propuesta de mejora será realizada en la BVQ (Casa Matriz), ubicada en la Avenida Río Amazonas y Jerónimo Carrión N21-252 Edificio Londres, Quito, Ecuador. Además, el estudio se aplicará en el área de TI de la institución durante el periodo del mes de julio 2022 al mes de diciembre 2022. Por otra parte, se presentan las delimitaciones de esta investigación, con el fin de establecer con claridad los aspectos que no serán cubiertos en el desarrollo del estudio. Es importante mencionar que estas delimitaciones se han establecido con el objetivo de garantizar la viabilidad y la eficacia de la investigación, ya que se han identificado ciertos aspectos que se

escapan de las posibilidades del presente trabajo o que simplemente son inalcanzables en el marco de la presente investigación.

- No se incluirán aspectos relacionados con la infraestructura tecnológica de la BVQ, como la adquisición de nuevos servidores, redes de comunicación, entre otros.
- No se abordarán los temas relacionados con la seguridad de la información y su protección en caso de amenazas externas.
- No se incluirán aspectos relacionados con la migración de la información a nuevas plataformas o sistemas.
- No se abordarán los aspectos legales y normativos relacionados con la gestión y administración de la información.
- No se abordarán los temas relacionados con la gestión y administración de la información en departamentos y áreas no críticas para la continuidad del negocio.

CAPÍTULO II: Marco Teórico

Para el desarrollo del presente trabajo de investigación, es esencial comprender con claridad las definiciones que se derivan de cada una de las variables de estudio, incluyendo la información, la gestión de respaldos y el plan de continuidad. A medida que la tecnología avanza rápidamente, es importante recordar los conceptos y definiciones básicas y observar cómo ha evolucionado a lo largo del tiempo. Una vez que se tienen claros estos conceptos y definiciones, se pueden utilizar como guía para estructurar, desarrollar y proponer un plan de mejora para la gestión de respaldos de información y la continuidad del negocio de la BVQ.

2.1. Conceptualización de gestión de respaldos de información

En este apartado se presentan las conceptualizaciones de gestión de respaldos de información que fundamentan teóricamente el desarrollo del trabajo de titulación. La comprensión adecuada de los conceptos es fundamental para establecer el marco teórico y la base conceptual que sustentará el estudio. Para ello, se describen las definiciones y características relevantes de cada variable de estudio, lo que permitirá una mejor comprensión de las mismas y su relación con el tema de investigación. Asimismo, se identificarán y analizarán los principales conceptos relacionados con cada una de las variables de estudio, con el objetivo de establecer una perspectiva clara y precisa de los mismos.

2.1.1. Gestión de TI

La gestión de Tecnologías de la Información (TI) se refiere al conjunto de procesos y prácticas utilizados por una organización para administrar y controlar sus recursos de TI de manera efectiva y eficiente. Esto incluye la planificación, el diseño, la implementación y la supervisión de los sistemas de información y tecnologías en la organización, con el objetivo de garantizar que estén alineados con los objetivos

estratégicos y operativos de la empresa. La gestión de TI también implica la gestión de riesgos, la seguridad de la información, el cumplimiento normativo y la gestión de proyectos de TI (Gupta y Goyal, 2020).

Asimismo, según IBM (2023c) indica que la gestión de tecnologías de la información (TI) se refiere al proceso de planificación, organización, implementación y control de los recursos y tecnologías de información en una organización. Esto incluye la gestión de sistemas informáticos, redes, software, hardware y bases de datos, así como la gestión de la seguridad y privacidad de la información.

Del mismo modo, la Biblioteca de Infraestructura de Tecnología de la Información (ITIL) define la Gestión de Servicios de TI como un conjunto de prácticas que se enfocan en la entrega de servicios de TI de calidad para satisfacer las necesidades de los usuarios y la organización (ITIL, 2022). También, COBIT define la Gestión de TI como la responsabilidad de los líderes empresariales y de TI para aprovechar al máximo la tecnología de la información y crear valor para el negocio (ISACA, 2022).

De este concepto de gestión de TI se puede inferir que se trata de un conjunto de procesos, políticas, procedimientos y prácticas que se utilizan para administrar y controlar los recursos y tecnologías de la información de una organización. Su objetivo principal es garantizar que los sistemas de información y tecnología sean eficientes, efectivos y estén alineados con los objetivos de la organización. La gestión de TI también implica la toma de decisiones estratégicas y la planificación a largo plazo para asegurar que los recursos de TI se manejen de manera efectiva y eficiente para apoyar el crecimiento y la sostenibilidad de la organización.

2.1.1.1. Políticas y estrategias de gestión de información.

Las políticas y estrategias de gestión de información son un conjunto de principios, directrices y medidas planificadas para administrar la información de una organización de manera efectiva y eficiente. Estas políticas y estrategias establecen cómo se debe recopilar, almacenar, proteger, utilizar y compartir la información en una organización (Blair, 2021).

Del mismo modo, Smallwood (2019) indica que las políticas y estrategias de gestión de información son un marco de trabajo que establece las pautas y normas para que la información sea gestionada de manera adecuada en una organización. Estas políticas y estrategias se diseñan para garantizar que la información se utilice de manera efectiva para tomar decisiones y apoyar los objetivos de la organización, al mismo tiempo que se protege la información sensible y confidencial de posibles amenazas o riesgos.

Se puede deducir que las políticas y estrategias de gestión de información se refieren a las decisiones, directrices y acciones planificadas que una organización establece para gestionar y controlar la información de manera efectiva y eficiente. Estas políticas y estrategias están diseñadas para garantizar que la información se utilice de manera adecuada y responsable, así como para protegerla de pérdidas, daños o accesos no autorizados.

También, implican la identificación de las necesidades de información de la organización y la determinación de las fuentes, formatos, procedimientos y tecnologías adecuados para gestionar y utilizar esa información de manera efectiva. Concisamente, las políticas y estrategias de gestión de información son un conjunto de principios y prácticas diseñados para garantizar que la información se gestione de

manera efectiva, eficiente y segura para respaldar los objetivos y procesos de una organización.

2.1.1.2. Infraestructura de TI.

La infraestructura de TI se refiere al conjunto de componentes tecnológicos que permiten la gestión y operación de los sistemas, así como los servicios de información de una organización. Esto incluye hardware, software, redes, sistemas de almacenamiento, servidores, entre otros elementos necesarios para garantizar la disponibilidad, confiabilidad, seguridad y escalabilidad de los sistemas de información de una empresa u organización. La infraestructura de TI es esencial para el correcto funcionamiento de los procesos de negocio y la toma de decisiones en una organización (Lovatt, 2021).

Adicionalmente, Arabnia *et al.* (2019) indican que la infraestructura de TI se define como el conjunto de componentes físicos y lógicos que se utilizan para la gestión y procesamiento de datos, información y conocimiento en una organización. Asimismo, puede incluir hardware como servidores, dispositivos de almacenamiento y redes de comunicaciones, así como software de sistemas operativos, bases de datos, aplicaciones empresariales y herramientas de colaboración.

Se puede inferir que la infraestructura de TI es una parte fundamental para la gestión de la tecnología de la información en cualquier organización, ya que proporciona los recursos y medios necesarios para garantizar el funcionamiento de los sistemas informáticos y su disponibilidad para el uso de los usuarios. Sin embargo, es importante tener en cuenta que la infraestructura de TI no es una solución aislada para la gestión de TI, sino que debe estar integrada en una estrategia más amplia que abarque también otros aspectos clave como la planificación estratégica, la gestión de proyectos, la seguridad de la información, la gestión de los servicios de TI, entre otros.

Además, la infraestructura de TI también está sujeta a ciertos riesgos, como la obsolescencia tecnológica, la falta de escalabilidad, la incompatibilidad entre los diferentes sistemas, la falta de redundancia, entre otros. Por lo tanto, es importante que la gestión de TI tenga en cuenta estos riesgos y trabaje para mitigarlos a través de la implementación de mejores prácticas y la adopción de soluciones tecnológicas adecuadas.

2.1.1.3. Seguridad de la información.

La seguridad de la información se refiere a la protección de la información de una organización contra el acceso, uso, divulgación, interrupción, alteración o destrucción no autorizados. La seguridad de la información se enfoca en mantener la confidencialidad, integridad y disponibilidad de la información, asegurando que solo las personas autorizadas puedan acceder a ella y que no se modifique o elimine de manera no autorizada (Smallwood, 2019). Asimismo, para Vega (2021) comenta que también se refiere a la protección contra amenazas externas, como hackers y virus informáticos, y amenazas internas, como empleados deshonestos o descuidados.

También, Lundgren y Möller (2019) indican que en general, se refiere a la protección de la información y los sistemas que la almacenan, procesan y transmiten, para garantizar su confidencialidad, integridad y disponibilidad. También se mencionan otros aspectos, como la autenticidad, la no repudio y la privacidad. La seguridad de la información se considera un desafío multidimensional y en constante evolución, que requiere la participación de múltiples actores y la implementación de medidas técnicas, organizativas y legales.

Se puede inferir que la seguridad de la información es un tema crítico para cualquier organización y su importancia se ha vuelto cada vez más evidente a medida que la tecnología se ha vuelto más central en las operaciones empresariales. La

implementación de medidas de seguridad adecuadas y eficaces es un proceso continuo que requiere una combinación de políticas, prácticas, tecnología y capacitación de los empleados para proteger los datos de posibles amenazas y garantizar la privacidad, así como la confidencialidad de la información de los clientes y usuarios.

2.1.1.4. Continuidad del negocio.

La continuidad del negocio se refiere a la capacidad de una organización para mantener sus operaciones críticas en caso de interrupciones inesperadas. Esto incluye cualquier evento que pueda afectar la capacidad de una organización para operar, como desastres naturales, fallas de equipos, ciberataques o interrupciones en la cadena de suministro. Además, la continuidad es esencial para garantizar que una organización pueda recuperarse rápidamente de una interrupción y minimizar cualquier impacto negativo en sus operaciones, clientes y reputación. Implica la implementación de planes de respuesta a emergencias, la realización de pruebas y simulaciones, y la identificación, así como la gestión de riesgos potenciales (Kliem y Richie, 2015).

Del de misma forma, Gaspar (2010) lo define como la capacidad de una organización para mantener el funcionamiento de sus actividades y servicios esenciales en situaciones de crisis, emergencias o eventos imprevistos que puedan afectar su normal funcionamiento.

Se puede inferir que la continuidad del negocio es la importancia de contar con planes actualizados y bien estructurados, así como de la necesidad de tener una cultura organizacional que promueva la preparación para emergencias y la gestión de riesgos. Además, la continuidad del negocio debe ser considerada como un proceso continuo y no como un evento único, y debe estar integrada en la planificación estratégica y operativa de la organización.

Plan de continuidad.

Un plan de continuidad es un conjunto de acciones y procedimientos planificados que deben realizarse para garantizar la continuidad de las operaciones críticas de una organización en caso de que ocurra un evento disruptivo. Este plan establece los procedimientos y recursos necesarios para garantizar que la organización pueda continuar operando en el nivel mínimo necesario, o en un nivel reducido, durante un período de tiempo específico después de un evento adverso. El objetivo principal de un plan de continuidad es minimizar el impacto de los eventos disruptivos en la organización y asegurar la recuperación de las operaciones críticas en el menor tiempo posible (Kliem y Richie, 2015).

Además, Gaspar (2010) lo define como un documento que establece las estrategias, procedimientos y acciones necesarias para garantizar la continuidad de las actividades y servicios esenciales de una organización en situaciones de crisis o desastres.

Según Alnahari (2021) indica que un plan de continuidad es un documento que describe los procedimientos que una organización debe seguir para garantizar la continuidad de sus operaciones críticas en caso de desastres naturales, fallas técnicas, errores humanos u otros eventos que puedan afectar la disponibilidad de los recursos y sistemas de la empresa. Además, un análisis crítico de un plan de continuidad debe evaluar si el plan es completo, adecuado y efectivo para garantizar la continuidad de los procesos críticos de la organización. Algunos aspectos que se pueden considerar son:

- Identificación de los procesos críticos: el plan debe definir claramente cuáles son los procesos y sistemas más importantes para el negocio, y establecer procedimientos específicos para garantizar su continuidad.

- Evaluación de riesgos: es importante que el plan incluya un análisis de los posibles riesgos y amenazas que puedan afectar los procesos críticos, para que se puedan tomar medidas preventivas y de contingencia adecuadas.
- Procedimientos detallados: el plan debe incluir procedimientos detallados para cada uno de los escenarios de contingencia identificados, de manera que los empleados puedan seguirlos fácilmente en caso de emergencia.
- Pruebas y actualizaciones: el plan debe ser probado regularmente para asegurar que sea efectivo, y actualizado constantemente para incluir nuevos sistemas, procesos y cambios en las amenazas y riesgos.

De los autores mencionados se puede inferir que un plan de continuidad es un conjunto de estrategias y procedimientos que deben ser planificados y aplicados para garantizar la continuidad de las operaciones críticas de una organización en caso de eventos disruptivos, como desastres naturales, fallas técnicas o errores humanos. Además, un plan de continuidad debe identificar claramente los procesos críticos y establecer procedimientos específicos para garantizar su continuidad, evaluar los posibles riesgos y amenazas que puedan afectar los procesos críticos, y proporcionar procedimientos detallados para cada uno de los escenarios de contingencia identificados.

También se puede inferir que un plan de continuidad debe ser probado regularmente y actualizado constantemente para incluir nuevos sistemas, procesos y cambios en las amenazas, así como riesgos. Igualmente, se puede ver que un análisis crítico del plan de continuidad debe evaluar si el plan es completo, adecuado y efectivo para garantizar la continuidad de los procesos críticos de la organización. Por ello, los

autores mencionados ofrecen perspectivas complementarias y actualizadas sobre el concepto de plan de continuidad, lo que puede ser útil para la elaboración de un plan de continuidad efectivo para una organización.

Objetivos de un plan de continuidad.

Según Kliem y Richie (2015) los objetivos principales de un Plan de Continuidad de Negocio (PCN) son:

- Garantizar la continuidad del negocio: El principal objetivo de un PCN es garantizar que la empresa pueda continuar operando, incluso en situaciones de crisis o desastres.
- Minimizar los riesgos: El PCN tiene como objetivo minimizar los riesgos asociados a la interrupción del negocio, como la pérdida de ingresos, clientes, reputación, entre otros.
- Establecer una estructura organizativa: Un PCN debe establecer una estructura organizativa clara y definir las responsabilidades y roles de las personas que intervienen en la gestión de la contingencia.
- Maximizar la eficiencia y eficacia: El PCN debe garantizar la eficiencia y eficacia de las acciones llevadas a cabo durante la contingencia para minimizar el impacto sobre la organización.
- Mejorar la capacidad de recuperación: El PCN debe mejorar la capacidad de recuperación de la organización, permitiendo una rápida respuesta ante situaciones de crisis y minimizando el impacto sobre el negocio.

Asimismo, Alnahari (2021) indica que el establecimiento de los objetivos de un Plan de Continuidad es crucial para garantizar la supervivencia de la organización en situaciones de crisis. Estos objetivos deben ser realistas y alcanzables para evitar la

creación de expectativas irreales en la organización. Por otro lado, es importante que los objetivos sean específicos y adecuados a las necesidades de la organización. El plan debe ser personalizado a la organización, ya que cada una puede tener diferentes necesidades y requerimientos. Además, los objetivos deben ser evaluados periódicamente y ajustados según sea necesario para garantizar que sigan siendo relevantes y efectivos.

De acuerdo con los autores citados, se puede inferir que los objetivos de un plan de continuidad son garantizar la continuidad del negocio, minimizar los riesgos asociados a la interrupción del negocio, establecer una estructura organizativa clara, maximizar la eficiencia y eficacia de las acciones llevadas a cabo durante la contingencia, y mejorar la capacidad de recuperación de la organización. Además, se destaca la importancia de establecer objetivos realistas, específicos y adecuados a las necesidades de la organización, y de evaluar periódicamente, así como ajustar los objetivos según sea necesario para garantizar su relevancia y efectividad.

Etapas de un plan de continuidad.

Según Gaspar (2010) define las etapas de un plan de continuidad en cuatro fases principales:

- **Análisis de riesgos:** En esta fase se identifican y evalúan los posibles riesgos y amenazas que podrían afectar el negocio. También se analiza el impacto que tendrían estas situaciones y se establecen prioridades.
- **Diseño del plan:** Una vez que se han identificado los riesgos, se procede a diseñar un plan de acción que permita hacer frente a las situaciones identificadas en la fase anterior. Se establecen los procedimientos a seguir y se definen los roles y responsabilidades de cada persona involucrada.

- Implementación del plan: En esta fase se llevan a cabo las medidas y acciones necesarias para implementar el plan de continuidad. Es importante asegurarse de que el personal está capacitado y entrenado para actuar en caso de emergencia.
- Mantenimiento y actualización del plan: Un plan de continuidad no es estático, sino que debe ser revisado y actualizado periódicamente. En esta fase se realizan pruebas y simulaciones para evaluar su eficacia y se hacen los ajustes necesarios para mejorarlo.

Del mismo modo, Alnahari (2021) indica que las etapas de un Plan de Continuidad son los pasos necesarios para desarrollar e implementar un plan de continuidad de negocio. Estas etapas pueden variar según el autor o la fuente consultada, pero generalmente incluyen:

- Análisis de impacto en el negocio: En esta etapa se identifican los procesos críticos, los recursos necesarios para llevarlos a cabo y las posibles consecuencias de una interrupción.
- Evaluación de riesgos: Se identifican las amenazas y se evalúan los riesgos asociados a cada una de ellas. Se determinan las medidas preventivas y de contingencia necesarias para mitigar los riesgos.
- Desarrollo del plan: Se elabora el plan de continuidad de negocio, incluyendo los procedimientos y recursos necesarios para garantizar la continuidad de las operaciones críticas.
- Implementación del plan: Se ponen en marcha las medidas preventivas y de contingencia establecidas en el plan.

- Prueba y mantenimiento del plan: Se realizan pruebas para verificar la efectividad del plan y se realizan actualizaciones y mantenimiento periódico para asegurar su vigencia y eficacia.

Se puede inferir que las etapas de un Plan de Continuidad son fundamentales para garantizar la continuidad de las operaciones de una organización en situaciones de crisis. Ambos autores coinciden en que las etapas incluyen la identificación y evaluación de riesgos, el diseño de un plan de acción, la implementación de medidas y acciones, el mantenimiento y actualización periódica del plan. Además, es importante destacar que el plan debe ser personalizado a las necesidades y características específicas de cada organización y que su efectividad debe ser evaluada periódicamente a través de pruebas y simulaciones.

Tipos de plan de continuidad

Según Gaspar (2010) establece tres tipos de PCN que se indican seguidamente:

- Plan de Recuperación ante Desastres (DRP): Este tipo de plan se enfoca en la recuperación de la infraestructura de TI y los sistemas de información luego de un desastre natural o causado por el hombre, como un incendio o un ciberataque.
- Plan de Continuidad de Negocio (BCP): Este tipo de plan se enfoca en mantener las operaciones críticas del negocio en caso de un evento disruptivo, como un fallo del equipo o una interrupción del servicio de energía eléctrica.
- Plan de Contingencia: Este tipo de plan se enfoca en la respuesta inmediata y las acciones que deben tomarse en caso de un evento disruptivo, como un terremoto o una emergencia médica.

Adicionalmente, Kliem y Richie (2015) hacen referencia al Plan de crisis (Crisis Management Plan): Este tipo de plan se enfoca en la gestión de situaciones de crisis que pueden afectar la reputación y la imagen de la organización, incluyendo procedimientos de comunicación y coordinación con los medios de comunicación, las autoridades y las partes interesadas.

Se puede inferir que los autores mencionados identifican varios tipos de Planes de Continuidad que una organización debe tener en cuenta para proteger sus operaciones críticas y su reputación en caso de un evento disruptivo.

- En primer lugar, el Plan de Recuperación ante Desastres (DRP) es importante para garantizar la recuperación de la infraestructura de TI y los sistemas de información en caso de desastres naturales o provocados por el hombre, como incendios o ciberataques.
- En segundo lugar, el Plan de Continuidad de Negocio (BCP) es esencial para garantizar que las operaciones críticas del negocio puedan continuar en caso de un evento disruptivo, como un fallo del equipo o una interrupción del servicio de energía eléctrica.
- En tercer lugar, el Plan de Contingencia es importante para garantizar una respuesta inmediata y las acciones necesarias en caso de eventos disruptivos, como terremotos o emergencias médicas.
- Por último, el Plan de crisis (Crisis Management Plan) se enfoca en la gestión de situaciones de crisis que pueden afectar la reputación y la imagen de la organización, incluyendo procedimientos de comunicación y coordinación con los medios de comunicación, las autoridades y las partes interesadas.

En resumen, es importante que una organización tenga en cuenta todos estos tipos de Planes de Continuidad, ya que cada uno se enfoca en diferentes aspectos de la continuidad del negocio y puede ayudar a reducir el impacto de un evento disruptivo en la organización.

2.1.2. Respaldos de información

Para abordar esta variable de estudio, es fundamental comprender qué es la información, los diferentes tipos de información y su clasificación según su relevancia. Además, resulta crucial identificar quiénes son los responsables de generar la información, dónde se origina y cómo se relaciona con los procesos y actividades de la institución. De esta manera, se podrá establecer una adecuada organización y gestión de la información generada en la empresa. Por ello, con el objetivo de consolidar y precisar el concepto de información, es necesario revisar diversas definiciones y enfoques teóricos.

2.1.2.1. Información.

La información se define como datos procesados y organizados que tienen significado y relevancia en un contexto determinado. La información puede presentarse en diferentes formas, como texto, imágenes, audio o video, y puede ser almacenada y transmitida en varios medios y formatos, como papel, discos duros, nubes de almacenamiento, entre otros (Blair, 2021).

Además, la información puede ser clasificada según su tipo (por ejemplo, información financiera, información de recursos humanos, información de investigación) y según su importancia y valor para la organización. La gestión adecuada de la información es esencial para el éxito de una organización y la toma de decisiones informadas. En este contexto, los respaldos de información juegan un

papel crítico al asegurar la disponibilidad y recuperación de la información ante posibles pérdidas o fallas en los sistemas de almacenamiento (Blair, 2021).

Del mismo modo, Lundgren y Möller (2019) indican que la información se refiere a los datos procesados y organizados que tienen significado y relevancia en un contexto específico. Puede presentarse en diferentes formas, como texto, imágenes, audio o video, y puede ser almacenada, así como transmitida en diversos medios y formatos. La información es fundamental para la toma de decisiones, la comunicación, la investigación y el conocimiento en general.

El concepto de información descrito destaca la importancia de la organización y el significado de los datos procesados en un contexto determinado. También se menciona la clasificación de la información según su tipo e importancia para la organización, y cómo la gestión adecuada de la información es fundamental para la toma de decisiones informadas y el éxito de la organización. Además, se destaca el papel crítico que juegan los respaldos de información en la disponibilidad y recuperación de la información en caso de pérdidas o fallas en los sistemas de almacenamiento.

Según Chiavenato información es "el conjunto de datos procesados que tienen significado y utilidad para quien los utiliza" (Chiavenato, 2006, p.110). Además, el autor destaca que la información se puede presentar en diferentes formatos y medios, y que su adecuada gestión es fundamental para la toma de decisiones y el éxito de una organización.

Para Ferrell O. C. y Hirt Geoffrey definen información como "datos que han sido recopilados, organizados y procesados para tener significado y valor para quien los recibe" (Ferrell *et al.*, 2010, p.121). Esta definición enfatiza la importancia de la organización y el procesamiento de los datos para que la información tenga sentido y

valor para el receptor. Además, también sugiere que la información es un recurso valioso que puede ser utilizado para tomar decisiones informadas.

Según Czinkota y Kotabe (2001) definen la información como un conjunto de datos organizados que poseen significado y valor para una organización en un determinado contexto. La información puede adoptar diversas formas, como texto, imágenes, audio o video, y puede almacenarse y transmitirse mediante diferentes medios y formatos, como el papel o los dispositivos electrónicos. Además, la información puede ser clasificada según su tipo y su importancia para la organización. La adecuada gestión de la información es esencial para la toma de decisiones informadas y el éxito de una organización.

La definición de Czinkota y Kotabe destaca la importancia de la información en el contexto empresarial y su papel en la toma de decisiones informadas. Además, señala que la información puede presentarse en diferentes formas y medios, lo que sugiere que su gestión adecuada es fundamental para el éxito organizacional. Sin embargo, a diferencia de la definición previamente presentada, esta no menciona la importancia de la organización y clasificación de la información según su tipo e importancia.

Por lo tanto, podría decirse que esta definición es más enfocada en el papel de la información en la toma de decisiones empresariales, mientras que la definición anterior se centra en la importancia de su correcta gestión y clasificación. En cualquier caso, ambas definiciones enfatizan la importancia de la información y su gestión adecuada en la toma de decisiones informadas y el éxito organizacional.

Los autores Toffler y Toffler (2006) hacen referencia a la idea de que los datos por sí solos no son suficientes para proporcionar información valiosa. Según los autores, los datos son solo "materia prima" para la creación de información, y es

necesario procesarlos y contextualizarlos adecuadamente para obtener información útil y relevante. Los autores también señalan que la abundancia de datos en la era digital puede llevar a una "sobrecarga de información" o a una "infobesidad", donde la cantidad de información disponible supera la capacidad de procesamiento y uso efectivo por parte de las personas y las organizaciones. En este sentido, Toffler y Toffler destacan la importancia de la gestión de la información y el conocimiento en un mundo cada vez más digitalizado y conectado.

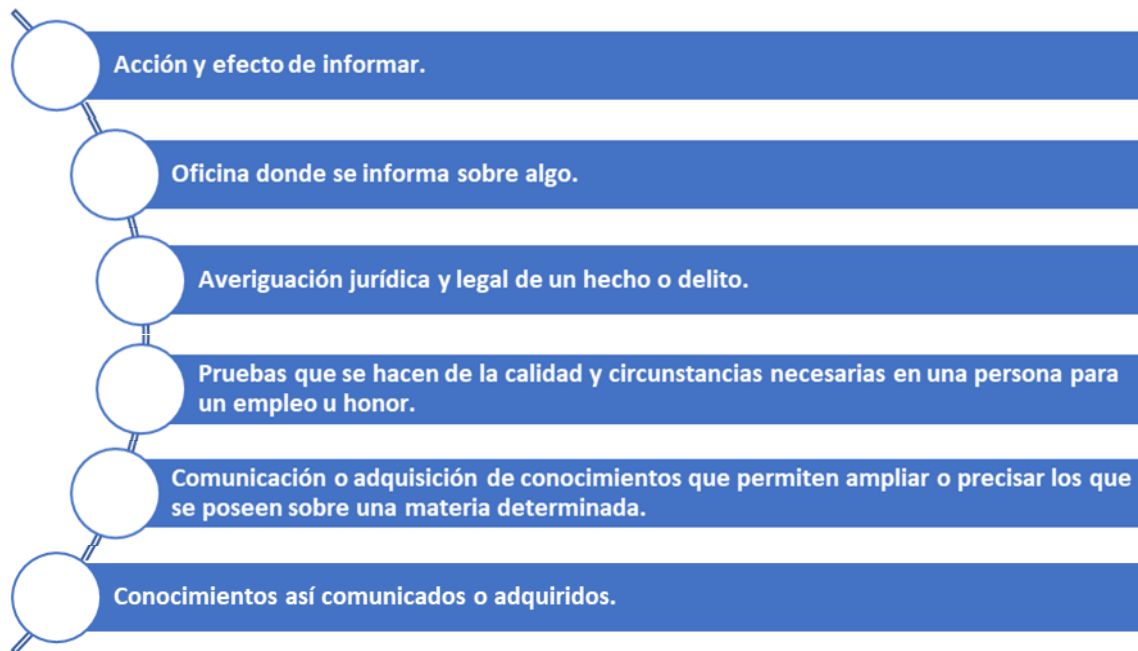
A partir de las definiciones proporcionadas, se puede observar que todas tienen en común el concepto de información como datos procesados y organizados que tienen significado y relevancia en un contexto determinado. Además, todas hacen hincapié en la importancia de la gestión adecuada de la información para el éxito de una organización y la toma de decisiones informadas.

La definición de Toffler y Toffler (2006) aporta una perspectiva interesante al enfatizar que la información es algo más que datos, es una forma de conocimiento que implica una comprensión profunda del contexto en el que se encuentra. Además, destacan la importancia de la creatividad y la innovación para la generación de nuevos conocimientos a partir de la información.

En general, todas las definiciones apuntan a la idea de que la información es un recurso valioso y estratégico que puede proporcionar ventajas competitivas a las organizaciones, siempre y cuando se gestionen adecuadamente. Por tanto, resulta fundamental para las empresas contar con una política adecuada de respaldos de información para protegerla y asegurar su disponibilidad ante posibles pérdidas o fallas en los sistemas de almacenamiento. En el mismo contexto, de acuerdo con los significados que se encuentran en el Diccionario de la Real Academia Española RAE (2023), se puede apreciar en la Figura 1 los diferentes usos de la palabra.

Figura 1

Usos de la palabra información



Nota: La figura representa el Usos de la palabra información. Tomado de: RAE (2023).

Tomando como base cada uno de los conceptos, definiciones e ideas citadas anteriormente, se puede definir la información como un conjunto de datos procesados y organizados que tienen significado y relevancia en un contexto determinado. Esta información puede presentarse en diferentes formas y ser almacenada y transmitida en varios medios y formatos. Además, es importante clasificarla según su tipo e importancia para la organización y gestionarla adecuadamente para lograr la toma de decisiones informadas y el éxito organizacional.

Por ello, la gestión adecuada de la información es fundamental para asegurar la disponibilidad y recuperación de la información ante posibles pérdidas o fallas en los sistemas de almacenamiento. Los autores también enfatizan que los datos por sí solos no son suficientes para proporcionar información valiosa y que es necesario procesarlos

y contextualizarlos adecuadamente. En este sentido, la sobrecarga de información puede llevar a una situación en la que la cantidad de información disponible supera la capacidad de procesamiento y uso efectivo por parte de las personas y las organizaciones. Por lo tanto, en un mundo cada vez más digitalizado y conectado, la gestión de la información y el conocimiento se convierte en un aspecto clave.

2.1.2.2. Ciclo de vida de la información.

Según SAP (2023) el ciclo de vida de la información se refiere al conjunto de fases por las que atraviesa la información desde su creación hasta su eventual disposición final. El ciclo de vida de la información consta de varias etapas:

- Creación: En esta etapa, la información se crea y se ingresa en el sistema de gestión de información.
- Almacenamiento: Después de que se crea la información, se almacena en un medio de almacenamiento, como un disco duro o un servidor.
- Uso: Durante esta etapa, la información se utiliza para la toma de decisiones y otros fines operativos.
- Mantenimiento: La información se mantiene durante un período determinado de tiempo para garantizar que esté disponible y sea precisa.
- Disposición: En esta etapa, la información se elimina o archiva para su futura referencia.

Cada una de estas etapas es importante en el ciclo de vida de la información, ya que ayuda a garantizar que la información sea precisa, relevante y esté disponible cuando sea necesario. Además, un ciclo de vida de información bien definido puede ayudar a garantizar la seguridad y privacidad de la información, así como a cumplir con las regulaciones y leyes aplicables (SAP, 2023).

También, Moulos et al. (2018) indican que el ciclo de vida de la información es el proceso que sigue la información desde su creación hasta su eliminación o archivo. Este ciclo se divide en diferentes etapas, que incluyen la creación o generación de la información, la captura, el almacenamiento, la gestión y el uso de la información, la conservación y el archivo, y finalmente, la eliminación de la información cuando ya no es necesaria. Por ello, el objetivo del ciclo de vida de la información es asegurar que la información se gestione de manera efectiva y eficiente durante todo su ciclo de vida, y que se proteja adecuadamente en cada etapa. De esta manera, se garantiza la disponibilidad, accesibilidad, integridad y seguridad de la información, y se cumple con las regulaciones y requisitos organizacionales en cuanto a la gestión de la información.

Se puede inferir que el ciclo de vida de la información es un proceso esencial para garantizar la gestión efectiva y eficiente de la información desde su creación hasta su eliminación o archivo, y que involucra diferentes etapas como la creación, almacenamiento, uso, mantenimiento y disposición de la información. Además, es importante tener un ciclo de vida bien definido para asegurar la precisión, relevancia y disponibilidad de la información, así como la seguridad y privacidad de la misma y el cumplimiento de las regulaciones y leyes aplicables. En general, los autores destacan la importancia de una gestión adecuada de la información en las organizaciones y el valor que tiene un ciclo de vida de la información bien establecido en este proceso.

2.1.2.3. Metodologías para gestionar el ciclo de vida de la información.

Existen varias metodologías que se utilizan para gestionar el ciclo de vida de la información. A continuación, se pueden mencionar las siguientes que son las más utilizadas:

- **Information Lifecycle Management (ILM):** Es una metodología que se enfoca en el ciclo de vida completo de la información, desde su creación

hasta su eliminación. Esta metodología se basa en el principio de que la información debe ser gestionada de forma diferente según su valor y su estado. ILM se utiliza principalmente en entornos empresariales y ayuda a las organizaciones a optimizar el almacenamiento, mejorar la eficiencia operativa y reducir los costos (SAP, 2023).

- **Enterprise Content Management (ECM):** Es una metodología que se enfoca en la gestión de todo el contenido de una organización, incluyendo documentos, imágenes, correos electrónicos y videos. ECM incluye la captura, almacenamiento, gestión, distribución y preservación del contenido. Esta metodología se utiliza principalmente en entornos empresariales y ayuda a las organizaciones a mejorar la eficiencia operativa y a reducir los riesgos legales (IBM, 2023b).
- **Data Lifecycle Management (DLM):** es una metodología que se enfoca en la gestión del ciclo de vida de los datos, desde su creación hasta su eliminación. DLM incluye la identificación, clasificación, almacenamiento, gestión y eliminación de los datos. Esta metodología se utiliza principalmente en entornos de tecnología de la información y ayuda a las organizaciones a optimizar el almacenamiento y la gestión de datos (IBM, 2023a).

2.1.2.4. Tipos de Información.

Es fundamental e imprescindible analizar los tipos de información, ya que será de mucha utilidad para la presente investigación el poder clasificar, administrar y almacenar la información de una manera estructurada y ordenada.

Los tipos de información se clasifica en:

Información Privilegiada.

Es aquella que se encuentra restringida a un grupo selecto de personas que tienen acceso a ella debido a su cargo o función dentro de la organización. Esta información puede estar relacionada con decisiones importantes, negociaciones comerciales o datos sensibles que deben ser protegidos por ley (García, 2019).

Según la National Institute of Standards and Technology (NIST) es aquella a la que solo tienen acceso ciertas personas en una organización debido a su posición o función. Esta información puede estar relacionada con decisiones importantes, negociaciones comerciales o datos sensibles que deben ser protegidos por ley (NIST, 2008).

Información Reservada.

Es aquella que, aunque no es clasificada como confidencial, se encuentra limitada en su acceso y difusión debido a su naturaleza o contenido, y su divulgación puede generar riesgos para la organización o para terceros. Puede incluir información estratégica, financiera, comercial o técnica (García, 2019).

Según la Ley 9/1968 de Secretos Oficiales de España, la información reservada se refiere a aquella información cuya divulgación puede causar daño al interés público, la seguridad del Estado o a las relaciones exteriores del país, y que, por lo tanto, requiere de una protección especial. Esta información está sujeta a una serie de medidas de seguridad y debe ser manejada y protegida adecuadamente (Ley BOE-A-1968-444, 1968).

Información Confidencial.

Es aquella que requiere de un nivel de protección más alto debido a su naturaleza sensible o a las implicaciones que su divulgación podría tener en la

organización o en terceros. Puede incluir datos personales, información financiera, estratégica o técnica, secretos comerciales, entre otros (García, 2019).

La NIST define la información confidencial como aquella que necesita una protección mayor debido a su carácter delicado o a las consecuencias que su divulgación podría tener. Esta información puede ser datos personales, empresariales, a nivel financiero, entre otros (NIST, 2008).

Información Pública.

Es aquella que está disponible para cualquier persona y que puede ser divulgada sin restricciones, ya que no tiene ningún tipo de limitación en cuanto a su acceso o difusión. Por ejemplo, los informes anuales de una organización o la información que se publica en su página web (García, 2019).

Según el artículo e de la Ley Orgánica de Transparencia y Acceso a la Información Pública de Ecuador, “Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado” (Ley 24, 2004, p. 2).

Información Privada.

Es aquella que se refiere a datos personales de individuos, como su nombre, dirección, número de identificación, entre otros. Esta información debe ser tratada con especial cuidado, ya que su divulgación o uso inadecuado puede afectar la privacidad y derechos de las personas (García, 2019).

La NIST define la información privada como datos personales, como el nombre, dirección, datos de identificación, entre otros, que deben ser protegidos, ya que su

difusión o uso indebido puede perturbar derechos y la privacidad de las personas (NIST, 2008).

Información Personal.

Es aquella que se relaciona con las opiniones, preferencias, creencias, hábitos o intereses de una persona, y que pueden ser utilizados para crear perfiles o para fines de investigación. Esta información también debe ser tratada con cuidado, ya que su uso indebido puede vulnerar los derechos de privacidad y protección de datos personales de las personas (García, 2019).

Según la Ley de Privacidad de la Información del Consumidor (CCPA), la información personal se refiere a cualquier información que identifique o pueda utilizarse para identificar a una persona en particular, como su nombre, dirección, número de teléfono, dirección de correo electrónico, número de seguridad social, entre otros datos (California Consumer Privacy Act, 2018).

Se puede inferir que clasificar la información en distintos tipos según su nivel de confidencialidad es un aspecto fundamental en cualquier organización. En el contexto de la gestión de respaldos de información, se hace aún más crítico, ya que se deben tomar medidas de seguridad adicionales para proteger los respaldos de información según su tipo.

La información privilegiada, reservada y confidencial son los tipos de información que requieren mayores medidas de seguridad, ya que su exposición podría poner en riesgo la estabilidad de la organización, su reputación y la seguridad de los clientes y usuarios. Por lo tanto, es importante que los respaldos de información de estos tipos se almacenen en medios seguros y se realicen de manera regular y verificando su correcta realización.

Además, es importante que las organizaciones clasifiquen la información según su nivel de confidencialidad y tomen medidas de seguridad adecuadas para garantizar la protección de los datos. En el contexto de la gestión de respaldos de información, esto implica tomar medidas adicionales para garantizar la integridad, disponibilidad y privacidad de los respaldos de información según su tipo.

2.1.2.5. Valor de la Información.

La gestión de la información se ha convertido en una tarea crítica en la mayoría de las organizaciones en la actualidad. Sin embargo, no toda la información tiene el mismo valor para todas las personas o situaciones. Es importante comprender los diferentes tipos de valores que puede tener la información para poder asignar adecuadamente los recursos de gestión de información. El valor de la información se puede clasificar en varios tipos, incluyendo valor normativo, valor realístico y valor subjetivo. En este marco teórico, se profundizará en cada uno de estos valores para proporcionar una base sólida para la propuesta de mejora de la gestión de respaldos de información de la BVQ en 2022.

Valor Normativo.

El valor normativo de la información se refiere a su capacidad para establecer normas o estándares de comportamiento. Por ejemplo, la información sobre leyes, regulaciones y políticas públicas puede tener un valor normativo al establecer los estándares y las expectativas de comportamiento para las personas y las organizaciones. Además, la información puede ser utilizada para influir en la opinión pública y en la toma de decisiones políticas, lo que también puede tener un valor normativo en la sociedad (García, 2019).

El valor normativo de la información se calcula utilizando modelos cuantitativos y se basa en la teoría de decisiones y la teoría de la utilidad para calcular la utilidad

esperada de un sistema de información dado. El enfoque analítico más completo es la Economía de la Información. Los modelos de simulación son otra forma de valorar la información. El principal problema del enfoque normativo es que es difícil de aplicar en situaciones no completamente estructuradas (Ahituv et al., 1981).

Valor Realístico.

El valor realístico es otro tipo de valor que se puede atribuir a la información. Este valor se refiere a la capacidad de la información para reflejar la realidad de manera precisa y fiable. En otras palabras, la información tiene un valor realístico cuando es exacta, completa y objetiva, y proporciona una imagen precisa de la realidad que describe. Por ejemplo, la información financiera que refleja de manera precisa la situación económica de una empresa tiene un alto valor realístico. Es importante destacar que el valor realístico está estrechamente relacionado con la calidad de la información, ya que la calidad de la información es un factor clave para garantizar su valor realístico (García, 2019).

El enfoque de valor realista de la información mide el valor de la información en términos de cambio en el rendimiento real debido a la introducción del sistema de información. Sin embargo, la conversión del valor de la información a valores monetarios solo es posible si las medidas de rendimiento en sí mismas pueden convertirse. Aunque conceptualmente simple, este enfoque no siempre es factible, ya que no siempre es posible demostrar una relación directa entre la nueva información y el cambio en el rendimiento. Además, se debe conocer el valor de la información de antemano, lo que hace que la predicción de los cambios de rendimiento sea aún más difícil. En conclusión, el enfoque de valor realista solo se puede utilizar para evaluar sistemas de información existentes (Ahituv et al., 1981).

Valor Subjetivo.

El valor subjetivo de la información se refiere a la percepción individual que cada persona tiene sobre la importancia, relevancia o utilidad de la información en cuestión. Este valor puede variar según las necesidades, intereses, conocimientos y experiencias de cada individuo, así como según el contexto en el que se encuentre. Por ejemplo, una misma información puede tener un alto valor subjetivo para una persona que la necesita para tomar una decisión importante, mientras que para otra persona puede tener poco o ningún valor debido a que no le afecta directamente o no le interesa (García, 2019).

En este enfoque, se pide a los usuarios que evalúen directamente algunos conjuntos de información dados. La herramienta de evaluación suele consistir en una lista de preguntas relacionadas con sus diversas características. La principal justificación de este enfoque es que combina la experiencia y la comprensión heurística de los usuarios e incorpora implícitamente factores humanos. Las evaluaciones subjetivas son relativamente fáciles de realizar, pero su principal desventaja es que no hay una relación directa entre sus resultados y algún valor real de la información. Sin embargo, se pueden usar para análisis comparativos (Ahituv et al., 1981)

Los tres valores mencionados (normativo, realístico y subjetivo) muestran cómo la valoración de la información puede ser influenciada por diversos factores. El valor normativo se basa en el grado de conformidad de la información con los estándares y regulaciones establecidos por una autoridad. El valor realístico, por otro lado, considera la utilidad práctica y objetiva de la información, es decir, su capacidad para ayudar en la toma de decisiones y el logro de objetivos específicos. Finalmente, el

valor subjetivo se refiere a la percepción personal y emocional de la importancia de la información, que puede variar significativamente entre individuos y organizaciones.

Es importante destacar que el valor de la información puede ser subjetivo y estar influenciado por diferentes perspectivas, experiencias y necesidades. En consecuencia, la valoración de la información puede variar entre los diferentes usuarios y contextos. Además, la valoración de la información también puede verse afectada por la precisión, la confiabilidad y la relevancia de la información. En este sentido, es esencial que las organizaciones comprendan y gestionen adecuadamente el valor de la información para maximizar su utilidad y minimizar los riesgos asociados con su uso.

2.1.2.6. Gestión de Respaldos.

La gestión de respaldos es una parte fundamental de la seguridad de la información en las instituciones, ya que permite garantizar la disponibilidad, integridad y confidencialidad de los datos críticos en caso de cualquier eventualidad. La información se considera el activo más valioso de cualquier organización, Por lo cual, su gestión adecuada se vuelve indispensable para el éxito de la institución.

Según Smallwood (2019) la gestión de respaldos es el conjunto de actividades y procesos que se llevan a cabo para asegurar la disponibilidad y la integridad de la información crítica de una organización en caso de fallos o desastres. Se trata de una parte fundamental de la gestión de la información, ya que los datos que maneja una organización son su activo más valioso, y su pérdida o corrupción puede tener graves consecuencias para la continuidad del negocio.

Asimismo, esta gestión involucra la definición de políticas y procedimientos para la creación, almacenamiento, monitoreo, prueba, recuperación y eliminación de los respaldos, así como la selección y mantenimiento de los medios de

almacenamiento adecuados para los mismos. La gestión de respaldos debe ser un proceso continuo y actualizado que asegure la disponibilidad de la información crítica en cualquier momento y ante cualquier eventualidad (Smallwood, 2019).

Del mismo modo, Hayes y Kotwica (2018) indican que la gestión de respaldos consiste en crear y mantener copias de la información crítica de una organización con el propósito de recuperar los datos perdidos o dañados. Esta tarea se vuelve más compleja debido al aumento constante de la cantidad de datos y la necesidad de hacer copias de seguridad en diferentes lugares. Además, las organizaciones necesitan implementar soluciones que permitan una fácil recuperación de los datos de respaldo y archivos según las necesidades del negocio. Este proceso también implica evaluar las tecnologías de respaldo, los requisitos de recuperación y retención de datos y aplicaciones, los métodos de respaldo y la arquitectura, así como los medios de almacenamiento de los respaldos.

Se puede inferir que la gestión de respaldos es fundamental para la seguridad de la información en cualquier organización, ya que permite garantizar la disponibilidad, integridad y confidencialidad de los datos críticos en caso de cualquier eventualidad, asegurando así la continuidad del negocio. Esto implica crear y mantener copias de la información crítica de una organización, definir políticas y procedimientos para la creación, almacenamiento, monitoreo, prueba, recuperación y eliminación de los respaldos, así como seleccionar y mantener los medios de almacenamiento adecuados para los mismos. Por lo tanto, la gestión de respaldos es un proceso continuo y actualizado que implica evaluar las tecnologías de respaldo, los requisitos de recuperación, retención de datos, aplicaciones, los métodos de respaldo y la arquitectura, así como los medios de almacenamiento de los respaldos. En resumen, la gestión de respaldos es crucial para garantizar la protección y

disponibilidad de la información crítica de una organización y asegurar su continuidad en caso de desastres o fallos en el sistema.

2.1.2. Medios de Almacenamiento

Los medios de almacenamiento son dispositivos o sistemas que se utilizan para guardar y conservar información de manera física o digital. Estos medios permiten el almacenamiento de datos de manera permanente o temporal, para que puedan ser recuperados en el futuro. Asimismo, existen diferentes tipos de medios de almacenamiento, tanto físicos como digitales. Entre los medios de almacenamiento físicos se encuentran los discos duros, las unidades de estado sólido, los CD y DVD, las cintas magnéticas, entre otros. Por otro lado, los medios de almacenamiento digitales incluyen el almacenamiento en la nube, la memoria USB, las tarjetas de memoria, entre otros (Petrenko, 2021).

En este mismo contexto, la elección del medio de almacenamiento adecuado dependerá de la cantidad y tipo de información que se desee almacenar, así como de la duración del almacenamiento y los recursos disponibles para la gestión de la información. Es importante tener en cuenta que el medio de almacenamiento utilizado debe ser confiable, seguro y garantizar la integridad de la información almacenada (Petrenko, 2021).

De acuerdo con el concepto presentado, se puede inferir que los medios de almacenamiento son herramientas utilizadas para guardar y preservar información, y que existen diferentes tipos de medios de almacenamiento, tanto físicos como digitales. Además, la elección del medio de almacenamiento adecuado dependerá de la cantidad y tipo de información que se desee almacenar, así como de la duración del almacenamiento y los recursos disponibles para la gestión de la información. Por último,

se destaca la importancia de que el medio de almacenamiento utilizado sea confiable, seguro y garantice la integridad de la información almacenada.

Tipos de Respaldo.

A continuación, se enumeran los distintos tipos de respaldos que serán analizados en esta sección. Es significativo destacar que se realizará una comparativa entre ellos para determinar cuál es el más adecuado para el tema de investigación:

- Respaldo completo: Es un tipo de respaldo que copia toda la información y archivos de un sistema o dispositivo de almacenamiento a otro medio, como un disco duro externo o una cinta de backup. Este tipo de respaldo es útil para la recuperación completa del sistema en caso de una falla, pero también puede consumir mucho tiempo y espacio de almacenamiento (Petrenko, 2021).

Del mismo modo, Hayes y Kotwica (2018) definen un respaldo completo o full backup es una técnica de copia de seguridad en la que se realiza una copia completa de todos los datos y archivos en los sistemas de producción en un momento determinado. Este tipo de respaldo puede ser útil en situaciones de desastre, ya que permite restaurar toda la información en su estado original en caso de que se produzca una pérdida completa de datos en el sistema de producción.

Sin embargo, los respaldos completos suelen ser más lentos y consumir más recursos que los respaldos incrementales o diferenciales, ya que copian toda la información de los sistemas de producción cada vez que se realizan. Además, estos respaldos requieren una cantidad significativa de espacio de almacenamiento, lo que puede hacer que su implementación sea costosa. Por lo tanto, es común que las

organizaciones combinen los respaldos completos con otros tipos de respaldo para optimizar el proceso de respaldo y recuperación de datos (Hayes y Kotwica, 2018).

- Respaldo incremental: Este tipo de respaldo sólo copia los cambios realizados desde la última copia de seguridad completa o incremental. Por ejemplo, si se realiza un respaldo completo el lunes y un respaldo incremental el martes, este último sólo copiará los archivos y cambios realizados desde el lunes. Este tipo de respaldo es útil para reducir el tiempo y el espacio de almacenamiento necesario para la copia de seguridad, pero puede ser más complejo de recuperar en caso de una falla (Petrenko, 2021).

Asimismo, Hayes y Kotwica (2018) definen el respaldo incremental como una técnica de copia de seguridad que permite respaldar sólo los datos que han cambiado desde el último respaldo completo o incremental. Esta técnica puede resultar muy útil para reducir el tiempo y espacio de almacenamiento necesario para hacer copias de seguridad, ya que sólo se copian los datos nuevos o modificados desde el último respaldo. Sin embargo, puede ser más lento a la hora de restaurar los datos, ya que en caso de pérdida de información se debe primero restaurar el último respaldo completo y luego aplicar los incrementales. También es importante tener en cuenta que si se realizan muchos respaldos incrementales, se puede generar una gran cantidad de archivos de copia de seguridad, lo que puede aumentar la complejidad de la gestión de las copias de seguridad y recuperación de datos (Hayes y Kotwica, 2018).

- Respaldo diferencial: Es similar al respaldo incremental, pero en este caso, se copian los cambios realizados desde el último respaldo completo. Por lo tanto, el primer respaldo diferencial será igual al completo, pero los siguientes sólo copiarán los cambios realizados desde ese momento. Este tipo de respaldo también reduce el tiempo y el espacio necesario para la copia de seguridad, pero puede ser más rápido de recuperar que el incremental (Petrenko, 2021).

También, Hayes y Kotwica (2018) definen el respaldo diferencial (también conocido como backup acumulativo): Es una copia de seguridad de los datos que han cambiado desde el último respaldo completo. Esto significa que el tamaño del respaldo diferencial es mayor que el del respaldo incremental, lo que puede resultar en un mayor tiempo y espacio de almacenamiento requerido para hacer el respaldo. Sin embargo, el proceso de restauración es más rápido que con el respaldo incremental, ya que solo se necesita restaurar el último respaldo completo y el último respaldo diferencial. Además, el respaldo diferencial permite una mayor flexibilidad en la retención de los respaldos, ya que solo se necesita guardar el último respaldo completo y el último respaldo diferencial para tener acceso a todos los datos respaldados.

Seguidamente, se presenta en la

Tabla 1 una comparativa de los tipos de respaldo según (Petrenko, 2021).

Tabla 1*Comparativa de tipos de respaldo*

	Respaldo completo	Respaldo incremental	Respaldo diferencial
Características	Se realiza una copia completa de todos los datos	Solo se copian los datos que han cambiado desde el último respaldo	Solo se copian los datos que han cambiado desde el último respaldo completo
Ventajas	Fácil y rápido de restaurar datos	Menor tiempo y espacio de almacenamiento requerido	Solo se necesitan dos copias (la última copia completa y la última copia diferencial)
Desventajas	Requiere mucho tiempo y espacio de almacenamiento	Restauración más lenta y compleja que con un respaldo completo	Requiere más espacio de almacenamiento que un respaldo incremental
Adecuado para	Situaciones en las que se dispone de tiempo y espacio suficiente	Situaciones en las que el tiempo y el espacio de almacenamiento son limitados y se realizan copias de seguridad frecuentes	Situaciones en las que el tiempo y el espacio de almacenamiento son limitados, pero se realizan copias de seguridad con menos frecuencia que con un respaldo incremental

Nota: Esta tabla muestra una comparación de los tipos de respaldo. Adaptado de: Petrenko (2021).

Es importante tener en cuenta que la elección del tipo de respaldo adecuado dependerá de las necesidades y recursos de cada institución. En el caso de tu tema de investigación, es necesario evaluar cuánto espacio de almacenamiento y tiempo se tienen disponibles para realizar los respaldos, así como la frecuencia con la que se deben realizar. En base a esto, podrás determinar cuál es el tipo de respaldo más adecuado para tu caso específico.

2.2. Importancia de la variable gestión de respaldos de información

En el contexto de la gestión de tecnologías de la información, es fundamental entender los conceptos y las ideas que los expertos han desarrollado acerca de los temas clave. Estos temas son relevantes para entender cómo se maneja la información en una organización, y cómo se puede asegurar su continuidad en caso

de eventos disruptivos. En este sentido, se han analizado las perspectivas de varios autores acerca de los medios de almacenamiento, los tipos de planes de continuidad, y los procesos de gestión de cambios. En este apartado, se presentan los conceptos de cada autor y la importancia de estos tópicos en la gestión de tecnologías de la información. Esto permitirá comprender la relevancia de estos temas y su impacto en la gestión de la información en una organización.

Tabla 2

Relevancia - gestión de TI

Nro.	Autor	Definición	Relevancia
1	(Gupta y Goyalm, 2020).	La gestión de TI se refiere a procesos para administrar los recursos de TI de una organización. Incluye la planificación, implementación, supervisión y alineación con objetivos de la empresa. También involucra gestión de riesgos, seguridad, cumplimiento normativo y gestión de proyectos de TI.	La gestión de Tecnologías de la Información (TI) es un tema de gran importancia en la actualidad debido a la creciente dependencia de las empresas en la tecnología para operar y competir en el mercado. Los conceptos de gestión de TI de autores como Gupta y Goyalm, IBM, ITIL y ISACA, destacan la importancia de
2	IBM (2023c)	La gestión de TI se refiere a la planificación, implementación y control de los recursos y tecnologías	la planificación, diseño, implementación, supervisión, alineación con objetivos empresariales,

		de información, incluyendo gestión de riesgos, la gestión de sistemas seguridad, privacidad, informáticos, redes, cumplimiento normativo y software, hardware y bases entrega de servicios de de datos, así como la calidad. Continuar seguridad y privacidad de la estudiando y aplicando los información. principios y prácticas de la
3	(ITIL, 2022)	La Gestión de Servicios de gestión de TI permitirá a las TI como un conjunto de organizaciones mejorar su prácticas que se enfocan en eficiencia, efectividad y la entrega de servicios de TI competitividad en un de calidad para satisfacer entorno tecnológico en las necesidades de los constante evolución. usuarios y la organización.
4	(ISACA, 2022)	Gestión de TI la define como la responsabilidad de los líderes empresariales y de TI para aprovechar al máximo la tecnología de la información y crear valor para el negocio.

Nota: Esta tabla presenta la relevancia de la gestión de TI.

Tabla 3

Relevancia - políticas y estrategias de gestión de información

Nro.	Autor	Definición	Relevancia
1	(Blair, 2021)	Las políticas y estrategias de gestión de información son medidas planificadas para administrar la información de una organización de manera efectiva y eficiente, estableciendo cómo se debe recopilar, almacenar, proteger, utilizar y compartir la información.	La gestión efectiva de la información es crucial en cualquier organización, y las políticas y estrategias de gestión de información son fundamentales para lograr esto. Al establecer pautas y normas claras sobre cómo se debe recopilar, almacenar, proteger, utilizar y compartir la información en una
2	Smallwood (2019)	Las políticas y estrategias de gestión de información son un marco de trabajo que establece pautas y normas para la gestión adecuada de la información en una organización, asegurando su uso efectivo y protegiendo la información sensible y confidencial.	organización, se garantiza que la información se utilice de manera efectiva para tomar decisiones y apoyar los objetivos de la organización. Además, la protección de la información sensible y confidencial es esencial para mitigar posibles riesgos y amenazas. Por lo tanto, seguir estudiando y desarrollando políticas y estrategias de gestión de

información es fundamental para el éxito de cualquier organización.

Nota: Esta tabla presenta la relevancia de las políticas y estrategias de gestión de información.

Tabla 4

Relevancia - infraestructura de TI

Nro.	Autor	Definición	Relevancia
1	(Lovatt, 2021)	La infraestructura de TI es el conjunto de componentes tecnológicos que permiten la gestión y operación de los sistemas y servicios de información de una organización, es esencial para el correcto funcionamiento de los procesos de negocio y la toma de decisiones.	Es importante seguir estudiando el tema de la infraestructura de TI, ya que esta es esencial para el correcto funcionamiento de los procesos de negocio y la toma de decisiones en una organización. Además, la infraestructura de TI es un conjunto complejo de componentes tecnológicos
2	(Arabnia et al., 2019)	La infraestructura de TI es un conjunto de componentes físicos y lógicos que se usan para procesar información en datos,	que permiten la gestión y operación de los sistemas, y que se utilizan para la gestión y procesamiento de información y

una organización, que conocimiento en una incluyen hardware, software organización, lo que hace y redes. necesario un conocimiento profundo y actualizado de estas tecnologías para poder mantener y mejorar la eficiencia, eficacia y seguridad de los sistemas de información de una organización.

Nota: Esta tabla presenta la relevancia de la infraestructura de TI.

Tabla 5

Relevancia - seguridad de la información

Nro.	Autor	Definición	Relevancia
1	(Smallwood, 2019)	La seguridad de la información protege la información de una organización contra el acceso no autorizado y la alteración, y mantiene su confidencialidad, integridad y disponibilidad.	La seguridad de la información es un tema crítico en el mundo actual, ya que las organizaciones dependen cada vez más de los sistemas informáticos y la información digital. Las amenazas a la seguridad de
2	(Vega, 2021)	Se refiere a la protección contra amenazas externas,	la información son constantes y cambiantes, lo

3	(Lundgren y Möller, 2019)	<p>como hackers y virus que significa que es informáticos, y amenazas necesario mantenerse internas, como empleados actualizado y tomar deshonestos o descuidados medidas proactivas para proteger la información. La seguridad de la información es la protección de la información y los sistemas para garantizar su legal y ético en muchas confidencialidad, integridad industrias y países. Por lo tanto, es esencial seguir considerando un desafío estudiando este tema para multidimensional que garantizar la protección requiere la participación de adecuada de la información múltiples actores y la y la continuidad del negocio. implementación de medidas técnicas, organizativas y legales.</p>
---	---------------------------	---

Nota: Esta tabla presenta la relevancia de la seguridad de la información.

Tabla 6

Relevancia - continuidad del negocio

Nro.	Autor	Definición	Relevancia
1	(Kliem y Richie, 2015)	Un plan de continuidad es un conjunto de acciones planificadas que garantizan	La relevancia de seguir estudiando el tema del Plan de Continuidad radica en

-
- la continuidad de las que es fundamental para operaciones críticas de una garantizar la supervivencia organización después de un de una organización ante evento disruptivo, con el situaciones de crisis o objetivo de minimizar su desastres que puedan impacto y asegurar la interrumpir sus operaciones recuperación en el menor críticas. Un plan de tiempo posible. continuidad bien diseñado y
- 2 (Gaspar, 2010) Un plan de continuidad es ejecutado puede minimizar un documento que el impacto de eventos establece las estrategias, disruptivos en la procedimientos y acciones organización, proteger la necesarias para garantizar seguridad de la información la continuidad de las y reducir las pérdidas actividades y servicios económicas. Además, un esenciales de una análisis crítico y organización en situaciones actualización periódica del de crisis o desastres. plan de continuidad es
- 3 (Alnahari, 2021) El plan de continuidad como esencial para asegurar que un conjunto de el plan siga siendo efectivo procedimientos planificados y adecuado ante posibles que garantizan la cambios en el entorno de la continuidad de las organización. En resumen, operaciones críticas de una la implementación de un organización en caso de un plan de continuidad puede
-

evento disruptivo, como un ser clave para la desastre natural o una falla supervivencia y éxito a largo técnica. El plan describe las plazo de una organización. estrategias, procedimientos y acciones necesarias para asegurar la continuidad de las actividades esenciales de la empresa. Es importante que el plan sea completo, adecuado y efectivo para garantizar la continuidad de los procesos críticos.

Nota: Esta tabla presenta la relevancia de la continuidad del negocio.

Tabla 7

Relevancia – plan de continuidad

Nro.	Autor	Definición	Relevancia
1	(Kliem y Richie, 2015)	Un plan de continuidad es un conjunto de acciones y procedimientos planificados que garantizan la continuidad de las operaciones críticas de una organización durante y	La relevancia de seguir estudiando el tema del plan de continuidad se puede resaltar en los siguientes aspectos:

	después de un evento disruptivo. Su objetivo principal es minimizar el impacto de los eventos disruptivos en la organización y asegurar la recuperación de las operaciones críticas en el menor tiempo posible.	<ul style="list-style-type: none"> • Garantizar la continuidad de las operaciones críticas de una organización en caso de eventos disruptivos, lo que puede evitar pérdidas económicas significativas y proteger la reputación y la confianza de la organización.
2	(Gaspar, 2010) Un Plan de Continuidad es un documento que describe las estrategias, procedimientos y acciones necesarias para garantizar la continuidad de las actividades y servicios esenciales de una organización durante situaciones de crisis o desastres.	<ul style="list-style-type: none"> • Minimizar el impacto de los eventos disruptivos en la organización, lo que puede contribuir a reducir los riesgos asociados a la interrupción de los procesos y la pérdida de datos críticos.
3	(Alnahari, 2021) Un plan de continuidad es un documento que establece los procedimientos y estrategias que deben	<ul style="list-style-type: none"> • Asegurar la recuperación de las

seguirse para garantizar la continuidad de las operaciones críticas de una organización en caso de eventos disruptivos, y debe ser evaluado para asegurar su efectividad.

operaciones críticas en el menor tiempo posible, lo que puede mejorar la resiliencia de la organización y aumentar su capacidad para responder a situaciones de emergencia.

- Evaluar si el plan es completo, adecuado y efectivo para garantizar la continuidad de los procesos críticos de la organización, lo que puede mejorar la eficiencia y efectividad del plan en caso de un evento disruptivo.

En resumen, seguir estudiando y mejorando los planes de continuidad es

esencial para garantizar la supervivencia y el éxito de las organizaciones en un entorno cada vez más complejo y cambiante.

Nota: Esta tabla presenta la relevancia del plan de continuidad.

Tabla 8

Relevancia – objetivos de un plan de continuidad

Nro.	Autor	Definición	Relevancia
1	(Kliem y Richie, 2015)	El objetivo principal de un Plan de Continuidad de Negocio (PCN) es garantizar la continuidad del negocio en situaciones de crisis o desastres, minimizando los riesgos y estableciendo una estructura organizativa clara. Además, busca maximizar la eficiencia y eficacia de las acciones durante la contingencia, así como mejorar la capacidad de recuperación de la	El tema de los objetivos en un plan de continuidad es crucial para garantizar la supervivencia de una organización en situaciones de crisis. Es importante comprender los objetivos principales de un plan de continuidad, como garantizar la continuidad del negocio, minimizar los riesgos, establecer una estructura organizativa, maximizar la eficiencia y mejorar la

		organización para una capacidad de recuperación. rápida respuesta ante situaciones de crisis y minimizar el impacto sobre el negocio.	Además, es fundamental adaptar estos objetivos a las necesidades específicas de la organización y evaluarlos
2	(Alnahari, 2021)	La definición de objetivos realistas y específicos fundamental en un Plan de Continuidad para asegurar la supervivencia de la organización durante situaciones de crisis. Es necesario personalizar el plan a las necesidades de la organización y evaluar los objetivos de manera periódica para garantizar que sigan siendo efectivos y adecuados.	periódicamente para asegurarse de que sigan siendo relevantes y efectivos. Seguir estudiando este tema puede ayudar a las organizaciones a estar mejor preparadas para hacer frente a situaciones de crisis y garantizar su supervivencia a largo plazo.

Nota: Esta tabla presenta la relevancia de los objetivos de un plan de continuidad.

Tabla 9

Relevancia – etapas de un plan de continuidad

Nro.	Autor	Definición	Relevancia
------	-------	------------	------------

-
- 1 (Gaspar, 2010) El plan de continuidad El estudio del tema de los
consta de cuatro etapas objetivos de un plan de
principales. La primera fase continuidad es crucial para
es el análisis de riesgos, garantizar la supervivencia
donde se identifican y de una organización ante
evalúan las posibles situaciones de crisis. Tanto
amenazas. La segunda fase Gaspar (2010) como
es el diseño del plan, donde Alnahari (2021) coinciden
se establecen los en que las etapas del plan
procedimientos y roles de de continuidad son
cada persona involucrada. fundamentales para
La tercera fase es la identificar y evaluar los
implementación del plan, riesgos y amenazas que
donde se llevan a cabo las podrían afectar el negocio,
medidas necesarias y se diseñar un plan de acción
capacita al personal. La que permita hacer frente a
cuarta y última fase es el las situaciones
mantenimiento y identificadas, implementar
actualización del plan, las medidas y acciones
donde se revisa necesarias para llevar a
periódicamente para cabo el plan, y mantenerlo
mejorar su eficacia. actualizado, así como
- 2 (Alnahari, 2021) Las etapas de un plan de efectivo a través de pruebas
continuidad incluyen la y simulaciones. La
identificación de procesos continuidad de las
-

críticos y riesgos, el operaciones críticas de una desarrollo de un plan de organización es esencial continuidad, su para su supervivencia y la implementación, y pruebas implementación de un plan y mantenimiento periódico. de continuidad adecuado puede marcar la diferencia en su capacidad para hacer frente a situaciones de crisis. Por lo tanto, seguir estudiando este tema es esencial para garantizar la resiliencia y el éxito de las organizaciones en un mundo en constante cambio e incertidumbre.

Nota: Esta tabla presenta la relevancia de las etapas de un plan de continuidad.

Tabla 10

Comparativo – tipos de plan de continuidad

Nro.	Autor	Definición	Relevancia
1	(Gaspar, 2010)	Plan de Recuperación ante Desastres (DRP): Este tipo de plan se enfoca en la recuperación de la infraestructura de TI y los	El tema de los planes de continuidad de negocio es de gran importancia para las organizaciones en la actualidad, ya que la

sistemas de información interdependencia entre los
luego de un desastre natural sistemas de información y la
o causado por el hombre, infraestructura tecnológica
como un incendio o un es cada vez mayor. Los
ciberataque. eventos disruptivos, ya sean
Plan de Continuidad de naturales o provocados por
Negocio (BCP): Este tipo de el hombre, pueden tener un
plan se enfoca en mantener impacto significativo en las
las operaciones críticas del operaciones de una
negocio en caso de un organización y su capacidad
evento disruptivo, como un para mantener la
fallo del equipo o una continuidad del negocio.
interrupción del servicio de Por lo tanto, es fundamental
energía eléctrica. que las empresas cuenten
Plan de Contingencia: Este con planes de contingencia
tipo de plan se enfoca en la y de recuperación ante
respuesta inmediata y las desastres, así como con
acciones que deben planes de continuidad de
tomarse en caso de un negocio y de gestión de
evento disruptivo, como un crisis, para garantizar que
terremoto o una emergencia puedan seguir operando en
médica caso de eventos imprevistos

2 (Kliem y Richie, Plan de crisis (Crisis y minimizar los riesgos
2015) Management Plan): Este asociados. Además, la
tipo de plan se enfoca en la implementación de estos

gestión de situaciones de crisis que pueden afectar la reputación y la imagen de la organización, incluyendo procedimientos de comunicación y coordinación con los medios de comunicación, las autoridades y las partes interesadas.

planes puede ayudar a las organizaciones a mejorar su resiliencia y su capacidad para adaptarse a situaciones cambiantes y desafiantes en el futuro. En resumen, seguir estudiando y mejorando los planes de continuidad de negocio es esencial para proteger la viabilidad y la sostenibilidad de las empresas en un entorno cada vez más competitivo y cambiante.

Nota: Esta tabla presenta la relevancia de los tipos de plan de continuidad.

Tabla 11

Relevancia – información

Nro.	Autor	Definición	Relevancia
1	(Blair, 2021).	La información es datos organizados que tienen significado y pueden ser presentados en diferentes formas y medios.	La gestión adecuada de la información es esencial para el éxito de una organización y la toma de decisiones informadas. En

2	(Lundgren y Möller, 2019)	La información es un conjunto de datos organizados y procesados que tienen significado y relevancia en un contexto determinado.	un mundo donde la cantidad de datos disponibles es cada vez mayor, el dominio de la información se ha vuelto crítico para muchas áreas de la sociedad, desde
3	(Chiavenato, 2006)	“El conjunto de datos procesados que tienen significado y utilidad para quien los utiliza”	la economía y los negocios hasta la ciencia y la tecnología. Por lo tanto, seguir estudiando sobre la
4	(Ferrell et al., 2010)	“Datos que han sido recopilados, organizados y procesados para tener significado y valor para quien los recibe”	información y su gestión es clave para aprovechar al máximo su valor y tomar decisiones bien fundamentadas. Además, la
5	(Czinkota y Kotabe, 2001)	La información es un conjunto de datos organizados que poseen significado y valor para una organización en un contexto determinado, puede adoptar diferentes formas y almacenada y transmitida por diferentes medios. Es importante para el éxito de	evolución constante de las tecnologías de la información y comunicación, hace que sea importante estar actualizados para enfrentar los retos que surgen en el manejo de grandes cantidades de información en diferentes contextos.

		una organización gestionar adecuadamente la información.
6	(Toffler & Toffler, 2006)	Los datos sin procesar no proporcionan información valiosa. Es necesario contextualizarlos adecuadamente. La abundancia de datos puede llevar a una "infobesidad". Toffler y Toffler destacan la importancia de la gestión de la información en un mundo cada vez más digitalizado.

Nota: Esta tabla presenta la relevancia de la información.

Tabla 12

Relevancia – ciclo de vida de la información

Nro.	Autor	Definición	Relevancia
1	(SAP, 2023)	El ciclo de vida de la información es el conjunto de etapas por las que atraviesa la información desde su creación hasta su eliminación o archivo, que	La relevancia de seguir estudiando el ciclo de vida de la información radica en que, en la era digital actual, las organizaciones manejan grandes cantidades de

incluyen creación, información, la cual puede almacenamiento, uso, ser crítica para el éxito de mantenimiento y sus operaciones y disposición. Cada etapa es decisiones. Por lo tanto, es importante para garantizar crucial contar con un la precisión, relevancia y proceso bien definido para disponibilidad de la el manejo de la información información y cumplir con durante todo su ciclo de regulaciones y leyes vida, desde su creación aplicables. hasta su disposición final.

- 2 (Moulos *et al.*, El ciclo de vida de la Además, el estudio del ciclo 2018) información es el proceso de vida de la información que sigue la información permite comprender la desde su creación hasta su importancia de la gestión eliminación o archivo. El adecuada de la información, objetivo es garantizar que lo cual incluye su se gestione de manera almacenamiento, gestión, efectiva y se proteja uso, conservación y adecuadamente en cada eliminación. Esto permite etapa, para asegurar su que la información esté disponibilidad, disponible y sea precisa accesibilidad, integridad y cuando sea necesaria, así seguridad, y cumplir con las como garantizar su regulaciones y requisitos seguridad y privacidad en organizacionales todo momento.
-

Nota: Esta tabla presenta la relevancia del ciclo de vida de la información.

Tabla 13

Comparativo – metodologías para gestionar el ciclo de vida de la información

Nro.	Autor	Definición	Relevancia
1	(SAP, 2023)	<p>Information Lifecycle Management (ILM): Es una metodología que se enfoca en el ciclo de vida completo de la información, desde su creación hasta su eliminación. Esta metodología se basa en el principio de que la información debe ser gestionada de forma diferente según su valor y su estado. ILM se utiliza principalmente en entornos empresariales y ayuda a las organizaciones a optimizar el almacenamiento, mejorar la eficiencia operativa y reducir los costos.</p>	<p>Es importante destacar la relevancia de seguir estudiando el ciclo de vida de la información y las metodologías que se utilizan para su gestión, ya que en la actualidad la cantidad de información que se genera y almacena en las organizaciones es cada vez mayor y más compleja. Una correcta gestión del ciclo de vida de la información permite a las organizaciones optimizar el almacenamiento y el acceso a los datos, mejorar la eficiencia operativa, reducir los costos y los riesgos</p>

2	(IBM, 2023b)	Enterprise Content Management (ECM):	<p>legales, así como también contribuye a una mejor toma de decisiones. Además, las metodologías como ILM, el contenido de una ECM y DLM se adaptan a las necesidades específicas de cada organización y pueden ser implementadas en diferentes entornos empresariales, tecnológicos y de gestión de la información.</p> <p>Esta metodología se utiliza Por lo tanto, seguir principalmente en entornos estudiando y empresariales y ayuda a las actualizándose en cuanto a las metodologías para la eficiencia operativa y a gestión del ciclo de vida de reducir los riesgos legales. la información resulta fundamental para cualquier organización que desee mantenerse competitiva y eficiente en el mercado actual, donde la gestión de la información se ha convertido en un elemento</p>
3	(IBM, 2023a)	Data Lifecycle Management (DLM):	<p>fundamental para cualquier organización que desee mantenerse competitiva y eficiente en el mercado actual, donde la gestión de la información se ha convertido en un elemento</p>

identificación, clasificación, clave para el éxito almacenamiento, gestión y empresarial. eliminación de los datos. Esta metodología se utiliza principalmente en entornos de tecnología de la información y ayuda a las organizaciones a optimizar el almacenamiento y la gestión de datos.

Nota: Esta tabla presenta la metodologías para gestionar el ciclo de vida de la información.

Tabla 14

Relevancia – tipos de información

Nro.	Autor	Definición	Relevancia
Información Privilegiada:			El estudio de los tipos de
1	(García, 2019)	Información restringida a un grupo selecto de personas debido a su cargo o función en la organización, relacionada con decisiones importantes, negociaciones comerciales o datos	información y su protección es relevante en la actualidad debido a la creciente cantidad de datos que se generan y manejan en diferentes entornos, lo que aumenta los riesgos de

		sensibles que deben ser protegidos por ley.	vulneración de la privacidad y seguridad de las personas
2	(NIST, 2008)	Información restringida a ciertas personas en una organización por su posición o función, que puede estar relacionada con decisiones importantes, que negociaciones comerciales o datos sensibles que deben ser protegidos por ley.	y organizaciones. Además, la existencia de regulaciones y leyes sobre la protección de la información hace necesario que las empresas y organizaciones tomen decisiones importantes que comprendan la importancia de manejar y proteger adecuadamente la información que manejan,
		Información Reservada:	
3	(García, 2019)	Información limitada en su acceso y difusión debido a su contenido y riesgos asociados a su divulgación. Incluye información estratégica, financiera, comercial o técnica.	para evitar consecuencias legales y daños reputacionales. En resumen, seguir estudiando este tema es crucial para asegurar la privacidad y seguridad de la información
4	(Ley BOE-A-1968-444, 1968).	La información reservada es aquella que debe ser protegida debido a su importancia para el interés	en la era digital actual.

público o la seguridad del Estado.

Información Confidencial:

5 (García, 2019) Información confidencial es sensible y requiere protección para evitar su divulgación. Incluye datos personales, financieros, estratégicos, técnicos y secretos comerciales.

6 (NIST, 2008) La información confidencial es delicada y necesita protección debido a sus consecuencias. Puede incluir datos personales, empresariales o financieros.

Información Pública:

7 (García, 2019) Disponible para cualquier persona sin restricciones de acceso o difusión, como los informes anuales de una organización o información en una página web.

8 (Ley 24, 2004) La información pública es todo documento en

cualquier formato que está en poder de instituciones públicas o personas jurídicas, creados o obtenidos por ellas y que se encuentran bajo su responsabilidad o se hayan producido con recursos del Estado.

Información Privada:

- 9 (García, 2019) Información personal sensible. Comprende datos personales como nombre, dirección, número de identificación, entre otros, que deben ser tratados con cuidado debido a su sensibilidad y al riesgo de afectar la privacidad y derechos de las personas.
- 10 (NIST, 2008) Información privada son los datos personales que deben ser protegidos para evitar la perturbación de los
-

derechos y la privacidad de las personas.

Información Personal:

- 11 (García, 2019) Información Personal: datos relacionados con las opiniones, preferencias y hábitos de una persona, que deben ser protegidos para no vulnerar su privacidad y derechos.
- 12 (California Consumer Privacy Act, 2018) La información personal es cualquier dato que identifique a una persona, como su nombre, dirección, número de teléfono, correo electrónico o número de seguridad social.

Nota: Esta tabla presenta la relevancia de los tipos de información.

Tabla 15

Relevancia – valor de la información

Nro.	Autor	Definición	Relevancia
Valor Normativo:			Es importante seguir
1	(García, 2019)	El valor normativo de la información establece	estudiando los diferentes tipos de valor

normas y estándares de de la información, comportamiento, como incluyendo el valor la información sobre normativo, el valor leyes y regulaciones que realístico y el valor influye en la opinión subjetivo, ya que cada pública y en la toma de uno ofrece una decisiones políticas. perspectiva diferente

- 2 (Ahituv et al., 1981) Valor normativo de la sobre cómo se puede información: se estima valorar la información. con modelos Además, entender estos cuantitativos y se basa conceptos puede ayudar en teorías de decisiones a las organizaciones y a y utilidad para calcular la los individuos a tomar utilidad esperada de un decisiones informadas sistema de información. sobre cómo manejar la La economía de la información y cómo información es el asignar recursos para enfoque analítico más adquirirla y gestionarla. completo. Los modelos de simulación también pueden ser utilizados. El problema principal es su dificultad para aplicarse en situaciones no
-

completamente
estructuradas.

Valor Realístico:

- 3 (García, 2019) El valor realístico de la información se refiere a su capacidad de reflejar la realidad con precisión y fiabilidad. Es importante destacar que la calidad de la información es un factor clave para garantizar su valor realístico.
- 4 (Ahituv et al., 1981) El enfoque de valor realista mide el valor de la información en términos de cambio en el rendimiento debido a la introducción del sistema de información. La conversión a valores monetarios solo es posible si las medidas de rendimiento pueden convertirse. No siempre
-

es posible demostrar una relación directa entre la información y el cambio en el rendimiento, lo que dificulta la predicción. Este enfoque solo se puede utilizar para evaluar sistemas de información existentes.

Valor Subjetivo:

- 5 (García, 2019) El valor subjetivo de la información varía según las necesidades, intereses y experiencias de cada persona, así como el contexto en el que se encuentra.
- 6 (Ahituv et al., 1981) El enfoque subjetivo consiste en que los usuarios evalúen directamente algunos conjuntos de información dados a través de una
-

herramienta de evaluación que consta de una lista de preguntas. Aunque es fácil de realizar, su principal desventaja es que no hay una relación directa entre sus resultados y algún valor real de la información, pero se pueden usar para análisis comparativos.

Nota: Esta tabla presenta la relevancia del valor de la información.

Tabla 16

Relevancia – gestión de respaldos

Nro.	Autor	Definición	Relevancia
1	(Smallwood, 2019)	La gestión de respaldos es el conjunto de actividades para asegurar la disponibilidad y la integridad de la información crítica de una organización en caso de fallos o desastres.	La gestión de respaldos es un tema de gran importancia en la actualidad debido a la creciente cantidad de información crítica que manejan las organizaciones y la necesidad de garantizar

	<p>Involucra definir políticas y su disponibilidad y procedimientos para crear, almacenar, monitorear, probar, recuperar y eliminar respaldos, así como seleccionar y mantener medios de almacenamiento adecuados. Es un proceso continuo y actualizado que asegura la disponibilidad de la información crítica en cualquier momento y ante cualquier eventualidad.</p>	<p>La pérdida o corrupción de esta información puede tener graves consecuencias para la continuidad del negocio, por lo que es esencial contar con políticas y procedimientos actualizados y eficaces para la creación, almacenamiento, monitoreo, prueba, recuperación y eliminación de los respaldos.</p>
<p>2 (Hayes y Kotwica, 2018)</p>	<p>La gestión de respaldos implica crear y mantener copias de información crítica para recuperar datos perdidos o dañados. Se vuelve más compleja con el aumento de la cantidad de datos y la necesidad de hacer copias de seguridad en diferentes lugares. También implica evaluar tecnologías, requisitos de</p>	<p>Además, es importante evaluar y seleccionar adecuadamente las tecnologías de respaldo, los métodos de respaldo y la arquitectura, así como los medios de almacenamiento de los respaldos. Por lo tanto, seguir estudiando y actualizándose en este tema es fundamental para</p>

recuperación y retención, y garantizar la seguridad y
 medios de almacenamiento. continuidad de la información
 crítica de una organización.

Nota: Esta tabla presenta la relevancia de la gestión de respaldos.

Tabla 17

Relevancia – tipos de respaldos

Nro.	Autor	Definición	Relevancia
1	(Petrenko, 2021)	Respaldo completo: Copia de todo el sistema o dispositivo de almacenamiento en otro medio. Útil para recuperación completa en caso de falla, pero puede consumir mucho tiempo y espacio.	El tema de los tipos de respaldo es relevante para cualquier organización que maneje datos importantes y desee protegerlos de posibles pérdidas. Es importante entender las diferencias entre los distintos tipos de respaldo,
2	(Hayes y Kotwica, 2018)	Respaldo completo: Copia completa de todos los datos en un sistema de producción en un momento determinado. Útil en desastres, pero lento y requiere mucho espacio de	como el completo, incremental y diferencial, ya que cada uno tiene sus ventajas y desventajas en términos de tiempo, espacio y complejidad de recuperación. Al

-
- almacenamiento. Se comprender los distintos combinan con otros tipos de tipos de respaldo, las respaldo para optimizar el organizaciones pueden proceso de respaldo y diseñar un plan de copia de recuperación de datos. seguridad efectivo que les
- 3 (Petrenko, 2021) El respaldo incremental permita proteger sus datos copia sólo los cambios críticos de forma eficiente y realizados desde la última eficaz. Además, conocer los copia completa o diferentes tipos de respaldo incremental, lo que reduce puede ayudar a las tiempo y espacio de organizaciones a tomar almacenamiento, pero decisiones informadas puede ser más complejo de sobre la gestión de sus recuperar en caso de una datos y el uso de recursos falla. de almacenamiento. En
- 4 (Hayes y Kotwica, 2018) El respaldo incremental es resumen, el tema de los una técnica de copia de tipos de respaldo es seguridad que respalda solo relevante y necesario seguir los datos que han cambiado estudiando para cualquier desde el último respaldo persona u organización que completo o incremental, lo busque proteger sus datos que reduce el tiempo y importantes. espacio de almacenamiento necesario. Sin embargo, puede ser más lento de
-

restaurar y generar una gran cantidad de archivos de copia de seguridad, lo que aumenta la complejidad de la gestión y recuperación de datos.

5 (Petrenko, 2021) Respaldo diferencial: se copian los cambios realizados desde el último respaldo completo, reduciendo el tiempo y espacio necesario para la copia de seguridad. Es más rápido de recuperar que el respaldo incremental.

6 (Hayes y Kotwica, 2018) El respaldo diferencial es una copia de seguridad de los datos que han cambiado desde el último respaldo completo. Es más grande que el respaldo incremental, pero más rápido de restaurar. Se necesita guardar el último respaldo completo y el último

respaldo diferencial para tener acceso a todos los datos respaldados.

Nota: Esta tabla presenta la relevancia de los tipos de respaldos.

2.3. Análisis comparativo

El análisis comparativo es una herramienta fundamental para evaluar las diferencias y similitudes entre dos o más conceptos, estrategias, procesos o herramientas. Este método permite identificar las ventajas y desventajas de cada opción y seleccionar la que mejor se adapte a las necesidades de la organización. En el contexto de la gestión de respaldos de información, el análisis comparativo es esencial para determinar cuál es el tipo de respaldo más adecuado para una empresa en particular. En este sentido, se realizará un análisis comparativo para determinar la mejor opción para mejorar la gestión de respaldos de información en la BVQ.

Tabla 18

Comparativo - gestión de TI

Nro.	Autor	Definición	Análisis
1	(Gupta y Goyal, 2020).	La gestión de TI se refiere a procesos para administrar los recursos de TI de una organización. Incluye planificación, implementación, supervisión y alineación con objetivos de la empresa.	En el ámbito de la gestión de tecnologías de la información (TI), se han desarrollado diversas metodologías y técnicas para administrar y controlar de manera efectiva y eficiente los recursos y

		También involucra gestión sistemas de información de de riesgos, seguridad, una organización. En este cumplimiento normativo y análisis comparativo, se gestión de proyectos de TI. destacan las similitudes y
2	IBM (2023c)	La gestión de TI se refiere a diferencias entre las la planificación, definiciones y enfoques implementación y control de propuestos por diferentes los recursos y tecnologías autores y entidades. de información, incluyendo En primer lugar, tanto Gupta la gestión de sistemas y Goyal (2020) como IBM informáticos, redes, (2023c) coinciden en que la software, hardware y bases gestión de TI abarca la de datos, así como la planificación, organización, seguridad y privacidad de la implementación y control de información. los recursos y tecnologías
3	(ITIL, 2022)	La Gestión de Servicios de de información en una TI como un conjunto de organización. Esto incluye prácticas que se enfocan en la gestión de sistemas la entrega de servicios de TI informáticos, redes, de calidad para satisfacer software, hardware, bases las necesidades de los de datos y la seguridad de la usuarios y la organización. información.
4	(ISACA, 2022)	Gestión de TI la define como Por otro lado, ITIL (2022) se la responsabilidad de los centra en la Gestión de líderes empresariales y de Servicios de TI como un

TI para aprovechar al conjunto de prácticas para máximo la tecnología de la la entrega de servicios de TI información y crear valor de calidad que satisfagan para el negocio.

las necesidades de los usuarios y la organización.

Mientras que COBIT (ISACA, 2022) define la gestión de TI como la responsabilidad de los líderes empresariales y de TI para aprovechar al máximo la tecnología de la información y crear valor para el negocio.

En resumen, si bien todos los autores y entidades abordan la gestión de TI desde diferentes perspectivas, todas coinciden en que se trata de un conjunto de procesos y prácticas que buscan optimizar los recursos y tecnologías de información en una organización para

alcanzar los objetivos estratégicos y operativos. La diferencia radica en la manera en que se enfocan estas prácticas, ya sea en la entrega de servicios de calidad, la responsabilidad de los líderes empresariales y de TI o en la gestión de riesgos y seguridad de la información.

Nota: Esta tabla presenta el análisis de la gestión de TI.

Tabla 19

Comparativo - políticas y estrategias de gestión de información

Nro.	Autor	Definición	Análisis
1	(Blair, 2021)	Las políticas y estrategias de gestión de información son medidas planificadas para administrar la información de una organización de manera efectiva y eficiente, estableciendo cómo se debe recopilar, almacenar,	Al comparar las definiciones de políticas y estrategias de gestión de información proporcionadas por Blair (2021) y Smallwood (2019), se puede identificar una similitud en el enfoque en la planificación y establecimiento de pautas y

		proteger, utilizar y compartir la información.	normas para el manejo de la información dentro de una organización. Ambos autores destacan la importancia de diseñar políticas y estrategias para garantizar el uso efectivo de la información y la protección de la información sensible y confidencial.
2	Smallwood (2019)	Las políticas y estrategias de gestión de información son un marco de trabajo que establece pautas y normas para la gestión adecuada de la información en una organización, asegurando su uso efectivo y protegiendo la información sensible y confidencial.	Sin embargo, una diferencia clave entre las definiciones radica en la profundidad y alcance de las políticas y estrategias. Blair (2021) se enfoca en las medidas específicas que deben establecerse para recopilar, almacenar, proteger, utilizar y compartir la información de manera efectiva, mientras que Smallwood (2019) describe las políticas y estrategias como un marco de trabajo más amplio que establece las pautas y

normas para el manejo de la información en general.

Además, mientras que Blair (2021) se enfoca en las políticas y estrategias de gestión de información como un conjunto de principios y directrices, Smallwood (2019) describe estas políticas y estrategias como un marco de trabajo que ayuda a garantizar que la información se utilice de manera efectiva para tomar decisiones y apoyar los objetivos de la organización.

En resumen, tanto Blair (2021) como Smallwood (2019) enfatizan la importancia de diseñar políticas y estrategias para el manejo efectivo de la información dentro de una organización, aunque difieren en la profundidad y alcance

de estas políticas y estrategias y en cómo se definen exactamente.

Nota: Esta tabla presenta el análisis de las políticas y estrategias de gestión de información.

Tabla 20

Comparativo - infraestructura de TI

Nro.	Autor	Definición	Análisis
1	(Lovatt, 2021)	La infraestructura de TI es el conjunto de componentes tecnológicos que permiten la gestión y operación de los sistemas y servicios de información de una organización, es esencial para el correcto funcionamiento de los procesos de negocio y la toma de decisiones.	En cuanto a la definición de infraestructura de TI, ambos autores concuerdan en que se trata de un conjunto de componentes tecnológicos que permiten la gestión y operación de los sistemas de información de una organización. Sin embargo, Arabnia et al. (2019) amplían esta definición al
2	(Arabnia et al., 2019)	La infraestructura de TI es un conjunto de componentes físicos y lógicos que se usan para procesar información en	incluir el procesamiento de datos, información y conocimiento en la organización, y mencionan específicamente algunos

una organización, que elementos de hardware y software que pueden formar parte de la infraestructura de TI. incluyen hardware, software y redes.

En cuanto a la importancia de la infraestructura de TI, ambos autores destacan que es esencial para el correcto funcionamiento de los procesos de negocio y la toma de decisiones en una organización.

En cuanto a las diferencias, se puede mencionar que Lovatt se centra más en la importancia de la infraestructura de TI para la gestión y operación de los sistemas de información, mientras que Arabnia et al. amplían la definición para incluir el procesamiento de datos, información y conocimiento en la organización.

En resumen, ambos autores concuerdan en que la infraestructura de TI es esencial para la gestión y operación de los sistemas de información de una organización, pero Arabia et al. (2019) ofrecen una definición más amplia e incluyen algunos elementos específicos de hardware y software que pueden formar parte de la infraestructura de TI.

Nota: Esta tabla presenta el análisis de la infraestructura de TI.

Tabla 21

Comparativo - seguridad de la información

Nro.	Autor	Definición	Análisis
1	(Smallwood, 2019)	La seguridad de la información protege la información de una organización contra el acceso no autorizado y la alteración, y mantiene su	En cuanto a la definición de la seguridad de la información, los autores citados comparten la idea de que se trata de proteger la información de una

		confidencialidad, integridad y disponibilidad.	organización	contra amenazas y riesgos, ya sean internos o externos, para mantener la confidencialidad, integridad y disponibilidad de la información.
2	(Vega, 2021)	Se refiere a la protección contra amenazas externas, como hackers y virus informáticos, y amenazas internas, como empleados deshonestos o descuidados		
3	(Lundgren y Möller, 2019)	La seguridad de la información es la protección de la información y los sistemas para garantizar su confidencialidad, integridad y disponibilidad. También se considera un desafío multidimensional que requiere la participación de múltiples actores y la implementación de medidas técnicas, organizativas y legales.	(2019) hace hincapié en la importancia de mantener la información protegida contra posibles alteraciones no autorizadas, mientras que Vega (2021) destaca la importancia de protegerse contra amenazas externas, como hackers y virus informáticos, así como internas, como empleados deshonestos o descuidados.	<p>Por otro lado, Lundgren y Möller (2019) amplían la perspectiva al mencionar la autenticidad, la no repudio y</p>

la privacidad como aspectos importantes de la seguridad de la información, además de la confidencialidad, integridad y disponibilidad. En cuanto a la forma de abordar la seguridad de la información, todos los autores mencionan la necesidad de implementar medidas técnicas, organizativas y legales, además, reconocen que se trata de un desafío multidimensional y en constante evolución que requiere la participación de múltiples actores.

Nota: Esta tabla presenta el análisis de la seguridad de la información.

Tabla 22

Comparativo - continuidad del negocio

Nro.	Autor	Definición	Análisis
1	(Kliem y Richie, 2015)	Un plan de continuidad es un conjunto de acciones	En cuanto a la comparación de los conceptos de

		planificadas que garantizan continuidad del negocio, se la continuidad de las puede observar que ambos operaciones críticas de una autores coinciden en que se organización después de un refiere a la capacidad de evento disruptivo, con el una organización para objetivo de minimizar su mantener sus operaciones impacto y asegurar la críticas en caso de recuperación en el menor interrupciones inesperadas. tiempo posible. Además, ambas
2	(Gaspar, 2010)	Un plan de continuidad es definiciones mencionan la un documento que importancia de la establece las estrategias, implementación de planes procedimientos y acciones de respuesta a necesarias para garantizar emergencias, la realización la continuidad de las de pruebas y simulaciones, actividades y servicios y la identificación y gestión esenciales de una de riesgos potenciales. organización en situaciones Sin embargo, hay algunas de crisis o desastres. diferencias entre ambas
3	(Alnahari, 2021)	El plan de continuidad como definiciones. Kliem y Richie un conjunto de (2015) mencionan que la procedimientos planificados continuidad del negocio es que garantizan la esencial para garantizar que continuidad de las una organización pueda operaciones críticas de una recuperarse rápidamente de

organización en caso de un evento disruptivo, como un desastre natural o una falla técnica. El plan describe las estrategias, procedimientos y acciones necesarias para asegurar la continuidad de las actividades esenciales de la empresa. Es importante que el plan sea completo, adecuado y efectivo para garantizar la continuidad de los procesos críticos.

una interrupción y minimizar cualquier impacto negativo en sus operaciones, clientes y reputación, mientras que Gaspar (2010) lo define como la capacidad de una organización para mantener el funcionamiento de sus actividades y servicios esenciales en situaciones de crisis, emergencias o eventos imprevistos que puedan afectar su normal funcionamiento.

Además, la definición de Kliem y Richie (2015) es más amplia al mencionar que cualquier evento que pueda afectar la capacidad de una organización para operar, como desastres naturales, fallas de equipos, ciberataques o interrupciones en la cadena de suministro, puede ser

considerado una interrupción inesperada, mientras que Gaspar (2010) se enfoca más en situaciones de crisis o emergencias.

Nota: Esta tabla presenta el análisis de la continuidad del negocio.

Tabla 23

Comparativo – plan de continuidad

Nro.	Autor	Definición	Análisis
1	(Kliem y Richie, 2015)	Un plan de continuidad es un conjunto de acciones y procedimientos planificados que garantizan la continuidad de las operaciones críticas de una organización durante y después de un evento disruptivo. Su objetivo principal es minimizar el impacto de los eventos disruptivos en la organización y asegurar la recuperación de las	En cuanto a las similitudes entre los autores, todos coinciden en que un plan de continuidad es fundamental para garantizar la capacidad de una organización para mantener sus operaciones críticas en caso de interrupciones inesperadas. Además, todos destacan la importancia de la identificación de los procesos críticos y la evaluación de riesgos para

		operaciones críticas en el menor tiempo posible.	la elaboración de un plan efectivo.
2	(Gaspar, 2010)	Un Plan de Continuidad es un documento que describe las estrategias, procedimientos y acciones necesarias para garantizar la continuidad de las actividades y servicios esenciales de una organización durante situaciones de crisis o desastres.	En cuanto a las diferencias, Alnahari (2021) destaca la importancia de realizar un análisis crítico del plan de continuidad para evaluar si es completo, adecuado y efectivo para garantizar la continuidad de los procesos críticos de la organización. Kliem y Richie (2015) se centran más en los
3	(Alnahari, 2021)	Un plan de continuidad es un documento que establece procedimientos y estrategias que deben seguirse para garantizar la continuidad de las operaciones críticas de una organización en caso de eventos disruptivos, y debe ser evaluado para asegurar su efectividad.	procedimientos y recursos necesarios para garantizar que la organización pueda continuar operando en el nivel mínimo necesario o en un nivel reducido durante un período de tiempo específico después de un evento adverso. Por su parte, Gaspar (2010) hace hincapié en la necesidad de establecer estrategias,

procedimientos y acciones para garantizar la continuidad de las actividades y servicios esenciales de una organización en situaciones de crisis o desastres.

Además, Alnahari (2021) destaca la importancia de incluir procedimientos detallados en el plan de continuidad para cada uno de los escenarios de contingencia identificados, de manera que los empleados puedan seguirlos fácilmente en caso de emergencia, mientras que Kliem y Richie (2015) mencionan la necesidad de realizar pruebas y simulaciones para asegurar la efectividad del plan, y Gaspar (2010) resalta la importancia de actualizar

constantemente el plan para incluir nuevos sistemas, procesos y cambios en las amenazas y riesgos..

Nota: Esta tabla presenta el análisis del plan de continuidad.

Tabla 24

Comparativo – objetivos de un plan de continuidad

Nro.	Autor	Definición	Análisis
1	(Kliem y Richie, 2015)	El objetivo principal de un Plan de Continuidad de Negocio (PCN) es garantizar la continuidad del negocio en situaciones de crisis o desastres, minimizando los riesgos y estableciendo una estructura organizativa clara. Además, busca maximizar la eficiencia y eficacia de las acciones durante la contingencia, así como mejorar la capacidad de recuperación de la organización para una	En cuanto a los objetivos de un plan de continuidad de negocio, ambos autores coinciden en que el principal objetivo es garantizar la continuidad de las operaciones críticas de la organización en caso de situaciones de crisis o desastres. Además, ambos autores coinciden en que el plan de continuidad debe minimizar los riesgos asociados a la interrupción del negocio y establecer una estructura organizativa clara

		rápida respuesta ante para la gestión de la situaciones de crisis y contingencia.
		minimizar el impacto sobre el negocio. Además, Kliem y Richie (2015) mencionan que el
2	(Alnahari, 2021)	La definición de objetivos plan de continuidad debe ser realistas y específicos es fundamental en un Plan de Continuidad para asegurar la supervivencia de la organización durante el impacto sobre las situaciones de crisis. Es necesario personalizar el plan a las necesidades de la organización y evaluar los objetivos de manera periódica para garantizar que sigan siendo efectivos y adecuados. Es maximizar la eficiencia y eficacia de las acciones llevadas a cabo durante la contingencia para minimizar el impacto sobre la organización, así como mejorar la capacidad de recuperación de la organización para permitir una rápida respuesta ante situaciones de crisis y minimizar el impacto sobre el negocio. Por otro lado, Alnahari enfatiza la importancia de que los objetivos sean realistas, específicos y adecuados a las necesidades de la organización. También destaca la necesidad de

evaluar periódicamente y ajustar los objetivos del plan según sea necesario.

En general, ambos autores destacan la importancia de los objetivos en un plan de continuidad de negocio y comparten algunos objetivos clave, como garantizar la continuidad del negocio y minimizar los riesgos asociados a la interrupción del mismo. Sin embargo, Kliem y Richie (2015) se centran en la eficiencia, la eficacia y la capacidad de recuperación de la organización, mientras que Alnahari (2021) se centra en la personalización de los objetivos del plan y su evaluación periódica.

Nota: Esta tabla presenta el análisis de los objetivos de un plan de continuidad.

Tabla 25*Comparativo – etapas de un plan de continuidad*

Nro.	Autor	Definición	Análisis
1	(Gaspar, 2010)	<p>El plan de continuidad consta de cuatro etapas principales. La primera fase es el análisis de riesgos, donde se identifican y evalúan las posibles amenazas. La segunda fase es el diseño del plan, donde se establecen los procedimientos y roles de cada persona involucrada.</p> <p>La tercera fase es la implementación del plan, donde se llevan a cabo las medidas necesarias y se capacita al personal. La cuarta y última fase es el mantenimiento y actualización del plan.</p>	<p>Ambos autores coinciden en la importancia de planificar y diseñar un plan de continuidad de negocio para garantizar la supervivencia de la organización en situaciones de crisis. Sin embargo, presentan algunas diferencias en cuanto a las etapas que conforman el plan.</p> <p>Gaspar (2010) propone cuatro etapas principales: análisis de riesgos, diseño del plan, implementación del plan, mantenimiento y actualización del plan. Por otro lado, Alnahari (2021) propone cinco etapas: análisis de impacto en el negocio, evaluación de riesgos, desarrollo del plan,</p>

2 (Alnahari, 2021) Las etapas de un plan de implementación del plan, continuidad incluyen la prueba y mantenimiento del identificación de procesos plan. críticos y riesgos, el A pesar de las diferencias desarrollo de un plan de en la forma de estructurar continuidad, su las etapas del plan, ambos implementación, y pruebas autores coinciden en la y mantenimiento periódico. importancia de llevar a cabo un análisis de riesgos y una evaluación de los impactos en el negocio, para identificar los procesos críticos y las posibles consecuencias de una interrupción. Asimismo, ambos autores enfatizan en la importancia de implementar el plan y realizar pruebas para verificar su eficacia, así como en la necesidad de actualizar y mantener el plan periódicamente para garantizar su vigencia.

En general, aunque hay algunas diferencias en la forma en que se estructuran las etapas del plan de continuidad de negocio, ambos autores coinciden en la importancia de llevar a cabo un análisis riguroso de los riesgos y en la necesidad de mantener el plan actualizado y realizar pruebas para garantizar su eficacia.

Nota: Esta tabla presenta el análisis de las etapas de un plan de continuidad.

Tabla 26

Comparativo – tipos de plan de continuidad

Nro.	Autor	Definición	Análisis
1	(Gaspar, 2010)	Plan de Recuperación ante Desastres (DRP): Este tipo de plan se enfoca en la recuperación de la infraestructura de TI y los sistemas de información luego de un desastre natural	En cuanto a los tipos de Plan de Continuidad, tanto Gaspar como Kliem y Richie (2015) coinciden en la importancia de establecer diferentes tipos de planes en función del tipo de evento

o causado por el hombre, que pueda afectar al como un incendio o un negocio, aunque presentan ciberataque.

algunas diferencias en la Plan de Continuidad de tipología.

Negocio (BCP): Este tipo de Gaspar (2010) propone tres plan se enfoca en mantener tipos de planes: el Plan de las operaciones críticas del Recuperación ante negocio en caso de un Desastres (DRP), el Plan de evento disruptivo, como un Continuidad de Negocio fallo del equipo o una (BCP) y el Plan de interrupción del servicio de Contingencia. El DRP se enfoca en la recuperación energía eléctrica.

Plan de Contingencia: Este de la infraestructura de TI y tipo de plan se enfoca en la los sistemas de información respuesta inmediata y las luego de un desastre natural acciones que deben o causado por el hombre, tomarse en caso de un como un incendio o un evento disruptivo, como un ciberataque. El BCP se terremoto o una emergencia enfoca en mantener las médica operaciones críticas del

- 2 (Kliem y Richie, Plan de crisis (Crisis negocio en caso de un 2015) Management Plan): Este evento disruptivo, como un tipo de plan se enfoca en la fallo del equipo o una gestión de situaciones de interrupción del servicio de crisis que pueden afectar la energía eléctrica. Por
-

reputación y la imagen de la organización, incluyendo procedimientos de comunicación y coordinación con los medios de comunicación, las autoridades y las partes interesadas. último, el plan de contingencia se enfoca en la respuesta inmediata y las acciones que deben tomarse en caso de un evento disruptivo, como un terremoto o una emergencia médica.

Por otro lado, Kliem y Richie (2015) añaden un cuarto tipo de plan, el Plan de Crisis, que se enfoca en la gestión de situaciones de crisis que pueden afectar la reputación y la imagen de la organización, incluyendo procedimientos de comunicación y coordinación con los medios de comunicación, las autoridades y las partes interesadas.

En resumen, ambos autores coinciden en la necesidad de contar con diferentes

tipos de planes de continuidad para hacer frente a eventos disruptivos, aunque difieren en la tipología exacta de los mismos. Mientras Gaspar (2010) propone tres tipos de planes, Kliem y Richie (2015) añaden un cuarto tipo, el Plan de Crisis, que se enfoca en la gestión de situaciones de crisis de reputación.

Nota: Esta tabla presenta el análisis de los tipos de plan de continuidad.

Tabla 27

Comparativo – información

Nro.	Autor	Definición	Análisis
1	(Blair, 2021).	La información es datos organizados que tienen significado y pueden ser presentados en diferentes formas y medios.	En las diferentes definiciones presentadas, se puede observar que la información se refiere a datos procesados y
2	(Lundgren y Möller, 2019)	La información es un conjunto de datos	organizados que tienen significado y relevancia en

-
- organizados y procesados un contexto específico. La que tienen significado y información puede relevancia en un contexto presentarse en diferentes determinado. formas y medios, y puede
- 3 (Chiavenato, 2006) “El conjunto de datos ser clasificada según su tipo procesados que tienen e importancia para la significado y utilidad para organización. Además, la quien los utiliza” gestión adecuada de la
- 4 (Ferrell et al., 2010) “Datos que han sido información es fundamental recopilados, organizados y para el éxito de una procesados para tener organización y la toma de significado y valor para decisiones informadas. quien los recibe” Aunque existen algunas
- 5 (Czinkota y Kotabe, 2001) La información es un diferencias en las conjunto de datos definiciones, la mayoría de organizados que poseen los autores enfatizan la significado y valor para una importancia de la organización en un contexto organización y el determinado, puede adoptar procesamiento de los datos diferentes formas y ser para obtener información almacenada y transmitida útil y relevante. Asimismo, por diferentes medios. Es todos los autores importante para el éxito de concuerdan en que la una organización gestionar gestión adecuada de la
-

	adecuadamente	la	información es fundamental
	información.		para la toma de decisiones
6	(Toffler & Toffler, 2006)	Los datos sin procesar no proporcionan información valiosa. Es necesario contextualizarlos adecuadamente.	informadas y el éxito de una organización. Cabe destacar que los autores Toffler y Toffler (2006) enfatizan la necesidad de procesar y contextualizar adecuadamente los datos para obtener información valiosa y relevante, así como alertan sobre la sobrecarga de información o infobesidad que puede ser contraproducente. En resumen, todas las definiciones destacan la importancia de la información en la toma de decisiones y la gestión empresarial.

Nota: Esta tabla presenta el análisis de la información.

Tabla 28*Comparativo – ciclo de vida de la información*

Nro.	Autor	Definición	Análisis
1	(SAP, 2023)	El ciclo de vida de la información es el conjunto de etapas por las que atraviesa la información desde su creación hasta su eliminación o archivo, que incluyen creación, almacenamiento, uso y mantenimiento y disposición. Cada etapa es importante para garantizar la precisión, relevancia y disponibilidad de la información y cumplir con regulaciones y leyes aplicables.	El ciclo de vida de la información es un concepto fundamental en la gestión de la información y es abordado por diferentes autores. En este caso, se compararán las similitudes y diferencias entre la propuesta de SAP (2023) y Moulos et al. (2018). En cuanto a las similitudes, ambos autores coinciden en que el ciclo de vida de la información se refiere al proceso que sigue la información desde su creación hasta su eliminación o archivo. Asimismo, los dos autores consideran que el ciclo de vida de la información consta de varias etapas,
2	(Moulos <i>et al.</i> , 2018)	El ciclo de vida de la información es el proceso que sigue la información desde su creación hasta su eliminación o archivo. El objetivo es garantizar que	

se gestione de manera que incluyan la creación o efectiva y se proteja generación de la adecuadamente en cada información, el etapa, para asegurar su almacenamiento, la gestión disponibilidad, y el uso de la información, la accesibilidad, integridad y conservación, el archivado, seguridad, y cumplir con las y la eliminación de la regulaciones y requisitos información cuando ya no organizacionales es necesaria.

Además, SAP (2023) y Moulos et al. (2018) coinciden en que el objetivo del ciclo de vida de la información es asegurar que la información se gestione de manera efectiva y eficiente durante todo su ciclo de vida, y que se proteja adecuadamente en cada etapa. De esta manera, se garantiza la disponibilidad, accesibilidad, integridad y seguridad de la información, así como cumplir con las

regulaciones y requisitos organizacionales en cuanto a la gestión de la información.

Por otro lado, existen algunas diferencias entre las propuestas de SAP (2023) y Moulos et al. (2018). Una diferencia importante es que SAP (2023) considera la etapa de mantenimiento, mientras que Moulos et al. (2018) incluyen la captura de la información. La etapa de mantenimiento, según SAP (2023), se refiere al período determinado de tiempo en que la información se mantiene para garantizar que esté disponible y sea precisa, mientras que la captura, según Moulos et al. (2018), se refiere a la adquisición de la

información en el momento en que se crea.

Otra diferencia significativa es que SAP (2023) enfatiza en la disposición final de la información, mientras que Moulos et al. (2018) se centran más en la conservación y el archivo de la información. En la propuesta de SAP (2023), la disposición final de la información se refiere a la eliminación o el archivado para su futura referencia, mientras que en la propuesta de Moulos et al. (2018), la conservación y el archivo de la información se consideran una etapa importante para asegurar la disponibilidad, accesibilidad, integridad y seguridad de la información.

En resumen, ambas propuestas tienen en común la comprensión del ciclo de vida de la información como un proceso que sigue la información desde su creación hasta su eliminación o archivo. Sin embargo, difieren en la consideración de ciertas etapas, como la captura o el mantenimiento, y en el énfasis en la disposición final o en la conservación y el archivo de la información.

Nota: Esta tabla presenta el análisis del ciclo de vida de la información.

Tabla 29

Comparativo – metodologías para gestionar el ciclo de vida de la información

Nro.	Autor	Definición	Análisis
1	(SAP, 2023)	Information Lifecycle Management (ILM): Es una metodología que se enfoca en el ciclo de vida completo de la información, desde su	Lifecycle En cuanto a las metodologías para gestionar el ciclo de vida de la información, se pueden observar las siguientes similitudes y diferencias:

2	(IBM, 2023b)	<p>Enterprise Content Management (ECM): Es una metodología que se enfoca en la gestión de todo el contenido de una organización, incluyendo documentos, imágenes, correos electrónicos y videos. ECM incluye la captura, almacenamiento, gestión, distribución y</p>	<p>Similitudes:</p>	<ul style="list-style-type: none"> • Todas las metodologías mencionadas se enfocan en la gestión del ciclo de vida de la información, desde su creación hasta su eliminación o archivo. • Las tres metodologías tienen como objetivo mejorar la eficiencia operativa y reducir costos o riesgos legales. • Las tres metodologías son utilizadas en entornos empresariales.
			<p>Diferencias:</p>	

3	(IBM, 2023a)	<p>preservación del contenido. Esta metodología se utiliza principalmente en entornos empresariales y ayuda a las organizaciones a mejorar la eficiencia operativa y a reducir los riesgos legales.</p> <p>Data Lifecycle Management (DLM): es una metodología que se enfoca en la gestión del ciclo de vida de los datos, desde su creación hasta su eliminación. DLM incluye la identificación, clasificación, almacenamiento, gestión y eliminación de los datos. Esta metodología se utiliza principalmente en entornos de tecnología de la información y ayuda a las organizaciones a optimizar el almacenamiento y la gestión de datos.</p>	<ul style="list-style-type: none"> • La metodología ILM se enfoca en la gestión de la información según su valor y estado, mientras que ECM se enfoca en la gestión de todo el contenido de una organización y DLM se enfoca en la gestión del ciclo de vida de los datos. • ECM incluye la captura, distribución y preservación del contenido, mientras que ILM y DLM no abordan estos aspectos. • DLM incluye la identificación y clasificación de los datos, mientras que ILM y ECM no lo hacen.
---	--------------	--	--

En resumen, se puede indicar que cada una de estas metodologías tiene su propia área de enfoque, pero todas tienen como objetivo principal gestionar el ciclo de vida de la información para mejorar la eficiencia y reducir los costos o riesgos.

Nota: Esta tabla presenta el análisis de la metodologías para gestionar el ciclo de vida de la información.

Tabla 30

Comparativo – tipos de información

Nro.	Autor	Definición	Análisis
Información Privilegiada:			El análisis comparativo de
1	(García, 2019)	Información restringida a un grupo selecto de personas debido a su cargo o función en la organización, relacionada con decisiones importantes, negociaciones comerciales o datos	los conceptos o teorías relacionados con la información privilegiada, reservada, confidencial, pública, privada y personal, destaca varias similitudes y diferencias entre ellos, tal

		sensibles que deben ser protegidos por ley.	como se describe a continuación:
2	(NIST, 2008)	<p>Información restringida a ciertas personas en una organización por su posición o función, que puede estar relacionada con decisiones importantes, negociaciones comerciales o datos sensibles que deben ser protegidos por ley.</p>	<p>Similitudes:</p> <ul style="list-style-type: none"> • La información que se considera privilegiada, reservada, confidencial, privada o personal debe ser protegida adecuadamente para evitar su divulgación o uso indebido.
		Información Reservada:	
3	(García, 2019)	<p>Información limitada en su acceso y difusión debido a su contenido y riesgos asociados a su divulgación. Incluye información estratégica, financiera, comercial o técnica.</p>	<ul style="list-style-type: none"> • La naturaleza y el contenido de la información son los principales factores que determinan el nivel de protección que se debe otorgar.
4	(Ley BOE-A-1968-444, 1968).	<p>La información reservada es aquella que debe ser protegida debido a su importancia para el interés</p>	<ul style="list-style-type: none"> • La divulgación de la información puede generar riesgos para

	público o la seguridad del Estado.	la organización, terceros o la privacidad y derechos de las personas.
	Información Confidencial:	
5	(García, 2019) Información confidencial es sensible y requiere protección para evitar su divulgación. Incluye datos personales, financieros, estratégicos, técnicos y secretos comerciales.	<ul style="list-style-type: none"> • La información pública es aquella que está disponible para cualquier persona y que no tiene ningún tipo de limitación en cuanto a su acceso o difusión.
6	(NIST, 2008) La información confidencial es delicada y necesita protección debido a sus consecuencias. Puede incluir datos personales, empresariales o financieros.	<p>Diferencias:</p> <ul style="list-style-type: none"> • La información privilegiada está restringida a un grupo selecto de personas que tienen acceso a ella debido a su cargo o función dentro de la organización,
	Información Pública:	
7	(García, 2019) Disponible para cualquier persona sin restricciones de acceso o difusión, como los informes anuales de una organización o información en una página web.	
8	(Ley 24, 2004) La información pública es todo documento en	

cualquier formato que está en poder de instituciones públicas o personas jurídicas, creados o obtenidos por ellas y que se encuentran bajo su responsabilidad o se hayan producido con recursos del Estado.

mientras que la información reservada está limitada en su acceso y difusión debido a su naturaleza o contenido.

Información Privada:

9 (García, 2019)

Información personal sensible. Comprende datos personales como nombre, dirección, número de identificación, entre otros, que deben ser tratados con cuidado debido a su sensibilidad y al riesgo de afectar la privacidad y derechos de las personas.

- La información confidencial requiere de un nivel de protección más alto que la información reservada debido a su naturaleza sensible o a las implicaciones que su divulgación podría tener en la organización o en terceros.

10 (NIST, 2008)

Información privada son los datos personales que deben ser protegidos para evitar la perturbación de los

- La información privada se refiere a datos personales de
-

derechos y la privacidad de las personas.

individuos, mientras que la información personal se relaciona con las opiniones, preferencias, creencias, hábitos o intereses de una persona.

Información Personal:

11 (García, 2019) Información Personal: datos relacionados con las opiniones, preferencias y hábitos de una persona, que deben ser protegidos para no vulnerar su privacidad y derechos.

- La información pública se refiere a documentos en cualquier formato que se encuentran en poder de las instituciones públicas y de las personas jurídicas, mientras que la información privada y personal se relaciona con datos personales de individuos.
- Los criterios para definir la información privilegiada,

12 (California Consumer Privacy Act, 2018) La información personal es cualquier dato que identifique a una persona, como su nombre, dirección, número de teléfono, correo electrónico o número de seguridad social.

reservada,
confidencial, privada o
personal pueden
variar dependiendo
de la fuente citada y la
legislación aplicable
en cada país.

En resumen, mientras que todas estas categorías de información comparten la necesidad de ser protegidas adecuadamente, existen diferencias en cuanto a la naturaleza y el nivel de protección que se les debe otorgar. Por lo tanto, es importante tener en cuenta las similitudes y diferencias entre estos conceptos o teorías al momento de manejar y proteger la información en una organización o contexto personal.

Nota: Esta tabla presenta el análisis de los tipos de información.

Tabla 31*Comparativo – valor de la información*

Nro.	Autor	Definición	Análisis
Valor Normativo:			El análisis comparativo
1	(García, 2019)	El valor normativo de la información establece normas y estándares de comportamiento, como la información sobre leyes y regulaciones que influye en la opinión pública y en la toma de decisiones políticas.	de los conceptos de valor de la información propuestos por los diferentes autores se puede resumir en las siguientes similitudes y diferencias: Similitudes: <ul style="list-style-type: none">• Todos los autores
2	(Ahituv et al., 1981)	Valor normativo de la información: se estima con modelos cuantitativos y se basa en teorías de decisiones y utilidad para calcular la utilidad esperada de un sistema de información. La economía de la información es el enfoque analítico más completo. Los modelos	coinciden en que el valor de la información varía según el contexto, las necesidades y los intereses de las personas que la utilizan. <ul style="list-style-type: none">• Los tres tipos de valor de la

		de simulación también pueden ser utilizados. El problema principal es su dificultad para aplicarse en situaciones no completamente estructuradas.	información propuestos (normativo, realístico y subjetivo) se basan en diferentes criterios para
Valor Realístico:			
3	(García, 2019)	El valor realístico de la información se refiere a su capacidad de reflejar la realidad con precisión y fiabilidad. Es importante destacar que la calidad de la información es un factor clave para garantizar su valor realístico.	valorar la información. <ul style="list-style-type: none"> • Todos los autores destacan la importancia de la calidad de la información para garantizar su valor realístico. Diferencias:
4	(Ahituv et al., 1981)	El enfoque de valor realista mide el valor de la información en términos de cambio en el rendimiento debido a la introducción del sistema de información.	<ul style="list-style-type: none"> • El valor normativo se refiere a la capacidad de la información para establecer normas o

	<p>La conversión a valores monetarios solo es posible si las medidas de rendimiento pueden convertirse. No siempre es posible demostrar una relación directa entre la información y el cambio en el rendimiento, lo que dificulta la predicción. Este enfoque solo se puede utilizar para evaluar sistemas de información existentes.</p>	<p>estándares de comportamiento, mientras que el valor realístico se refiere a la capacidad de la información para reflejar la realidad de manera precisa y fiable. Mientras, el valor subjetivo se refiere a la percepción individual que</p>
<p>Valor Subjetivo:</p>		<p>cada persona</p>
<p>5 (García, 2019)</p>	<p>El valor subjetivo de la información varía según las necesidades, intereses y experiencias de cada persona, así como el contexto en el que se encuentra.</p>	<p>tiene sobre la importancia, relevancia o utilidad de la información en cuestión.</p>
<p>6 (Ahituv et al., 1981)</p>	<p>El enfoque subjetivo consiste en que los</p>	<p>• El enfoque de valor normativo se basa en la</p>

usuarios evalúen directamente algunos conjuntos de información dados a través de una herramienta de evaluación que consta de una lista de preguntas. Aunque es fácil de realizar, su principal desventaja es que no hay una relación directa entre sus resultados y algún valor real de la información, pero se pueden usar para análisis comparativos.

teoría de decisiones y la teoría de la utilidad para calcular la utilidad esperada de un sistema de información dado, mientras que el enfoque de valor realístico mide el valor de la información en términos de cambio en el rendimiento real debido a la introducción del sistema de información. El enfoque de valor subjetivo se basa en las evaluaciones

directas de los usuarios.

- El enfoque normativo es más difícil de aplicar en situaciones no completamente estructuradas, mientras que el enfoque de valor realista solo se puede utilizar para evaluar sistemas de información existentes. Por otro lado, el enfoque subjetivo es relativamente fácil de realizar, pero no hay una relación directa entre sus resultados y
-

algún valor real de la información.

En resumen, cada enfoque propuesto para valorar la información tiene sus propias ventajas y desventajas. Por ello, la elección del enfoque dependerá del contexto y de los objetivos específicos de la gestión de la información.

Nota: Esta tabla presenta el análisis del valor de la información.

Tabla 32

Comparativo – gestión de respaldos

Nro.	Autor	Definición	Análisis
1	(Smallwood, 2019)	La gestión de respaldos es el conjunto de actividades para asegurar la disponibilidad y la integridad de la información crítica de una organización en caso de fallos o desastres.	La gestión de respaldos es una práctica esencial en la gestión de la información y la seguridad de la información en cualquier organización. Smallwood (2019) y Hayes, así como

	<p>Involucra definir políticas y procedimientos para crear, almacenar, monitorear, probar, recuperar y eliminar respaldos, así como seleccionar y mantener medios de almacenamiento adecuados. Es un proceso continuo y actualizado que asegura la disponibilidad de la información crítica en cualquier momento y ante cualquier eventualidad.</p>	<p>Kotwica (2018) coinciden en que la gestión de respaldos implica la creación y mantenimiento de copias de seguridad de la información crítica de la organización. Ambos autores destacan la importancia de la disponibilidad, integridad y confidencialidad de los datos críticos en caso de una eventualidad, y la necesidad de definir</p>
<p>2 (Hayes y Kotwica, 2018)</p>	<p>La gestión de respaldos implica crear y mantener copias de información crítica para recuperar datos perdidos o dañados. Se vuelve más compleja con el aumento de la cantidad de datos y la necesidad de hacer copias de seguridad en diferentes lugares. También implica evaluar tecnologías, requisitos de</p>	<p>políticas y procedimientos para garantizar que la gestión de respaldos sea un proceso continuo y actualizado. No obstante, hay algunas diferencias en la forma en que cada autor aborda la gestión de respaldos. Smallwood (2019) se centra en el conjunto de actividades y procesos que</p>

recuperación y retención, y se llevan a cabo para medios de almacenamiento. asegurar la disponibilidad y la integridad de la información crítica en caso de fallos o desastres. En cambio, Hayes y Kotwica (2018) enfatizan en la complejidad creciente de la tarea debido al aumento constante de la cantidad de datos y la necesidad de hacer copias de seguridad en diferentes lugares. Además, Hayes y Kotwica (2018) sugieren que las organizaciones necesitan implementar soluciones que permitan una fácil recuperación de los datos de respaldo y archivos según las necesidades del negocio, y evaluar las tecnologías de respaldo, los requisitos de recuperación, retención de datos,

aplicaciones, los métodos de respaldo y la arquitectura, así como los medios de almacenamiento de los respaldos.

En resumen, ambos autores están de acuerdo en la importancia de la gestión de respaldos en la seguridad de la información y la continuidad del negocio, aunque abordan el tema de manera ligeramente diferente, con un enfoque más amplio por parte de Hayes y Kotwica (2018) y un enfoque más específico en los procesos de gestión de respaldos por parte de Smallwood (2019).

Nota: Esta tabla presenta el análisis de la gestión de respaldos.

Tabla 33

Comparativo – tipos de respaldos

Nro.	Autor	Definición	Análisis
-------------	--------------	-------------------	-----------------

-
- 1 (Petrenko, 2021) Respaldo completo: Copia En cuanto a los tipos de de todo el sistema o respaldo, se pueden dispositivo de identificar tres principales: almacenamiento en otro respaldo completo, respaldo medio. Útil para incremental y respaldo recuperación completa en diferencial. caso de falla, pero puede El respaldo completo copia consumir mucho tiempo y toda la información y espacio. archivos de un sistema o
- 2 (Hayes y Respaldo completo: Copia dispositivo de Kotwica, 2018) completa de todos los datos almacenamiento a otro en un sistema de medio, lo que puede ser útil producción en un momento para la recuperación determinado. Útil en completa del sistema en desastres, pero lento y caso de una falla, pero requiere mucho espacio de consume mucho tiempo y almacenamiento. Se espacio de combinan con otros tipos de almacenamiento. Por otro respaldo para optimizar el lado, el respaldo proceso de respaldo y incremental solo copia los recuperación de datos. cambios realizados desde la
- 3 (Petrenko, 2021) El respaldo incremental última copia de seguridad copia sólo los cambios completa o incremental, lo realizados desde la última que reduce el tiempo y el copia completa o espacio de almacenamiento
-

-
- incremental, lo que reduce necesario para la copia de tiempo y espacio de seguridad, pero puede ser almacenamiento, pero más complejo de recuperar puede ser más complejo de en caso de una falla. El recuperar en caso de una respaldo diferencial, por su falla. parte, es similar al respaldo
- 4 (Hayes y Kotwica, 2018) El respaldo incremental es incremental, pero en este una técnica de copia de caso, se copian los cambios seguridad que respalda solo realizados desde el último los datos que han cambiado respaldo completo, lo que desde el último respaldo reduce el tiempo y el completo o incremental, lo espacio necesario para la que reduce el tiempo y copia de seguridad. espacio de almacenamiento En cuanto a las similitudes, necesario. Sin embargo, se puede destacar que los puede ser más lento de tres tipos de respaldo tienen restaurar y generar una como objetivo la gran cantidad de archivos recuperación de de copia de seguridad, lo información en caso de que aumenta la complejidad pérdida de datos, y que de la gestión y recuperación todos ellos requieren de de datos. cierto espacio de
- 5 (Petrenko, 2021) Respaldo diferencial: se almacenamiento y tiempo copian los cambios para ser realizados. realizados desde el último Asimismo, es posible
-

6	(Hayes y Kotwica, 2018)	<p>El respaldo diferencial es una copia de seguridad de los datos que han cambiado desde el último respaldo completo. Es más grande que el respaldo incremental, pero más rápido de restaurar. Se necesita guardar el último respaldo completo y el último respaldo diferencial para tener acceso a todos los datos respaldados.</p>	<p>respaldo completo, combinando diferentes tipos de respaldos para optimizar el espacio necesario para el proceso de respaldo y copia de seguridad. Es más rápido de recuperar que el respaldo incremental. En cuanto a las diferencias, se puede destacar que el respaldo completo es el más completo y seguro en cuanto a la recuperación de información, pero es el que consume más tiempo y espacio de almacenamiento. Por otro lado, el respaldo incremental es más rápido y consume menos espacio, pero es más complejo de recuperar en caso de falla, ya que se necesita restaurar primero el último respaldo completo y luego aplicar los incrementales. El respaldo diferencial, por su parte, es más rápido de recuperar que el incremental, ya que</p>
---	-------------------------	--	--

solo se necesita restaurar el último respaldo completo y el último respaldo diferencial, pero requiere de un mayor espacio de almacenamiento que el incremental.

En conclusión, la elección del tipo de respaldo a utilizar dependerá de las necesidades y características específicas de cada caso. En general, se recomienda utilizar una combinación de diferentes tipos de respaldo para optimizar el proceso de respaldo y recuperación de datos.

Nota: Esta tabla presenta el análisis de los tipos de respaldos.

2.4. Análisis crítico

Después de analizar y comparar las metodologías y técnicas presentadas, puedo decir que estoy de acuerdo en que todas las metodologías y técnicas tienen fortalezas y debilidades. Sin embargo, me gustaría profundizar en algunos puntos.

En cuanto a la metodología del ciclo de vida de la información, es cierto que presenta una estructura clara para la gestión de la información, lo que es beneficioso para garantizar que se cumplan los requisitos de almacenamiento y acceso. Sin embargo, otros autores también mencionan que su enfoque en la fase de disposición puede ser limitado y no tener en cuenta la necesidad de conservar información valiosa para futuras investigaciones. Es importante destacar que la fase de disposición es crucial para garantizar que la información obsoleta o innecesaria se elimine adecuadamente y no se convierta en una carga innecesaria para el almacenamiento y acceso. Además, se puede aplicar una política de retención para conservar información valiosa para futuras investigaciones.

En cuanto a la metodología de gestión de documentos electrónicos, es cierto que su objetivo es garantizar que los documentos sean auténticos y confiables, lo que es esencial en entornos empresariales o gubernamentales. Sin embargo, algunos autores mencionan que su enfoque puede ser demasiado centrado en el control y la seguridad, lo que puede dificultar el acceso a la información para los usuarios. Es importante destacar que la seguridad y el control son fundamentales para garantizar la integridad y autenticidad de los documentos, pero también es importante equilibrar estos objetivos con la necesidad de acceso a la información para los usuarios autorizados.

En cuanto a la técnica de backup y recuperación, es cierto que puede ser muy efectiva para garantizar la disponibilidad de la información en caso de desastres o pérdidas de datos. Sin embargo, algunos autores también mencionaron que puede ser costosa y requerir una planificación cuidadosa para asegurar que se realicen los respaldos adecuados y se puedan recuperar los datos cuando sea necesario. Es importante destacar que la realización de respaldos y recuperación es crucial para

garantizar la disponibilidad de la información, pero también es importante asegurarse de que la técnica de backup sea eficiente y eficaz en términos de costos, y que se realicen pruebas regulares para garantizar que se pueda recuperar la información de manera efectiva en caso de un desastre.

En conclusión, es importante reconocer que cada metodología y técnica de gestión de información tiene sus propias fortalezas y debilidades. Es fundamental comprender estas fortalezas y debilidades para poder elegir la metodología y técnica adecuadas para la gestión de la información en una organización.

Por lo anteriormente expuesto, la BVQ es una institución financiera que maneja una gran cantidad de información crítica relacionada con las transacciones bursátiles de sus clientes. Para garantizar la seguridad y disponibilidad de esta información, es fundamental contar con procesos y procedimientos estandarizados para el manejo, administración y gestión de los respaldos de información. Por esta razón, se ha planteado la necesidad de realizar un diagnóstico detallado del estado actual de estos procesos y diseñar una propuesta de mejora que permita optimizarlos y garantizar la continuidad del negocio ante posibles incidentes o desastres. Además, se busca establecer mecanismos de control que permitan garantizar el cumplimiento de los procesos y procedimientos establecidos en la propuesta de mejora, así como realizar recomendaciones específicas basadas en las mejores prácticas y normas internacionales en la materia.

En este contexto, el presente proyecto tiene como objetivo principal contribuir a la mejora de la gestión de los respaldos de información en la BVQ, con el fin de garantizar la seguridad y disponibilidad de la información crítica, optimizar los procesos existentes y asegurar la continuidad del negocio ante posibles incidentes o

desastres. Por ello, se presentan las siguientes acciones para cumplir con los objetivos específicos mencionados:

- Realizar un diagnóstico detallado: Se requiere llevar a cabo un estudio exhaustivo y detallado de los procesos actuales de manejo, administración y gestión de los respaldos de información en la BVQ. Es necesario identificar los puntos críticos, los riesgos y las vulnerabilidades existentes en el sistema actual, para poder diseñar una propuesta de mejora efectiva.
- Diseñar una propuesta de mejora: Se debe elaborar una propuesta que contemple la implementación de procesos y procedimientos estandarizados para el manejo, administración y gestión de los respaldos de información en la BVQ. Esta propuesta debe garantizar la seguridad y disponibilidad de la información crítica.
- Establecer los mecanismos de control necesarios: Es importante definir los mecanismos de control necesarios para garantizar el cumplimiento de los procesos y procedimientos establecidos en la propuesta de mejora. Esto incluye la definición de roles y responsabilidades, la implementación de herramientas tecnológicas y la capacitación del personal encargado de la gestión de la información.
- Realizar recomendaciones específicas: Se deben hacer recomendaciones específicas sobre el manejo, administración y gestión de los respaldos de información en la BVQ, con el objetivo de optimizar los procesos existentes y garantizar la continuidad del negocio ante posibles incidentes o desastres. Estas recomendaciones deben estar basadas en las mejores prácticas y normas internacionales en la materia.

CAPITULO III: Marco Referencial

3.1. Reseña histórica

La BVQ C.A. se estableció por medio de escrituras públicas otorgadas ante el Notario Cuarto del Cantón Quito el 4 y 25 de agosto de 1969, y fueron inscritas en el Registro Mercantil del Cantón Quito el 30 de septiembre de 1969. Posteriormente, la sociedad se transformó en una Corporación Civil mediante una escritura pública celebrada el 13 de mayo de 1994 ante el Notario Primero del Cantón Quito, la cual fue aprobada por la Superintendencia de Compañías a través de la Resolución No. 94.1.1.1.1131 de 27 de mayo de 1994. Finalmente, la Corporación Civil se transformó en una Sociedad Anónima por medio de una escritura pública celebrada el 24 de julio de 2016 ante el Notario Décimo Tercero del Cantón Quito, la cual fue aprobada por la Superintendencia de Compañías, Valores y Seguros a través de la Resolución No. SCVS.IRQ.DRMV.2016.1745 de 20 de julio de 2016.

La BVQ se dedica principalmente a proporcionar servicios y mecanismos para la negociación de valores. Además, puede llevar a cabo otras actividades relacionadas que sean necesarias para el adecuado desarrollo del mercado de valores, previa autorización de la Junta de Política y Regulación Monetaria y Financiera, a través de normas de carácter general. Para cumplir con su objeto, la BVQ tiene la capacidad de realizar toda clase de actos, contratos y negocios jurídicos que se relacionen directamente, en su totalidad o en parte, con su objeto, así como establecer otros servicios que sean afines y compatibles con el mismo.

3.1.1. Obligaciones

La BVQ sociedad Anónima, como parte de su objeto, deberá cumplir con las siguientes obligaciones Figura 2.

Figura 2

Obligaciones de BVQ

Regular y supervisar, en el ámbito de su competencia, las operaciones de los participantes, y velar porque se cumplan las disposiciones de la Ley

Proporcionar a los intermediarios de valores la infraestructura física y tecnológica que les permita el acceso transparente de las propuestas de compra y venta de valores inscritos

Brindar a los intermediarios autorizados, a través del Sistema Único Bursátil SIUB, el mecanismo para la negociación bursátil de los valores e instrumentos financieros

Ser accionista de la compañía anónima proveedora y administradora del sistema único bursátil

Contratar los servicios de la Sociedad Proveedora y Administradora del Sistema Único Bursátil

Divulgar y mantener a disposición del mercado y del público en general información simétrica, veraz, completa y oportuna, sobre las cotizaciones de los valores, intermediarios y las operaciones efectuadas en bolsas de valores, así como sobre la situación económica financiera y los hechos relevantes de los emisores.

Entregar en tiempo real a los depósitos de compensación y liquidación de valores información relacionada con las negociaciones del mercado de valores.

Mantener estándares de seguridad informática tales como protección de los sistemas informáticos, respaldos de la información en sede distinta al lugar donde opere la Bolsa de Valores de Quito BVQ Sociedad Anónima, medidas de gestión del riesgo legal, operativo y financiero, de acuerdo a lo que determine la Junta de Política y Regulación Monetaria y Financiera, en cuanto a parámetros y tiempo de exigibilidad.

Publicar y certificar la información de precios, tasas, rendimientos, montos, volúmenes y toda la información que la Superintendencia de Compañías, Valores y Seguros considere pertinente, de las operaciones efectuadas en bolsa de valores, y el registro de los intermediarios, operadores de valores, emisores y valores inscritos. Esta información debe ser pública y de libre acceso para toda persona, en la manera que la Junta de Política y Regulación Monetaria y Financiera lo establezca y de conformidad con las disposiciones legales vigentes.

Cumplir con los principios de transparencia y objetividad que garanticen la adopción de buenas prácticas corporativas.

Inscribir y registrar emisores y valores para la negociación en bolsa de valores, así como suspender o cancelar su inscripción.

Sancionar a las personas jurídicas y personas naturales sometidas a su control, por transgresiones a las normas de autorregulación.

Las demás que, de acuerdo a esta Ley, en uso de sus atribuciones, disponga la Junta de Política y Regulación Monetaria y Financiera.

Nota: La figura representa las obligaciones de BVQ.

3.2. Filosofía organizacional

3.2.1. Visión

Ser la primera alternativa en el sistema financiero para el ahorro, la inversión y el financiamiento, con el mejor precio y el menor costo.

3.2.2. Misión

Apoyar la creación y correcta distribución de la riqueza mediante un mercado de valores institucionalizado, promoviendo la cultura bursátil y las prácticas de Buen Gobierno Corporativo, con miras a la integración de los mercados.

3.3. Política de calidad

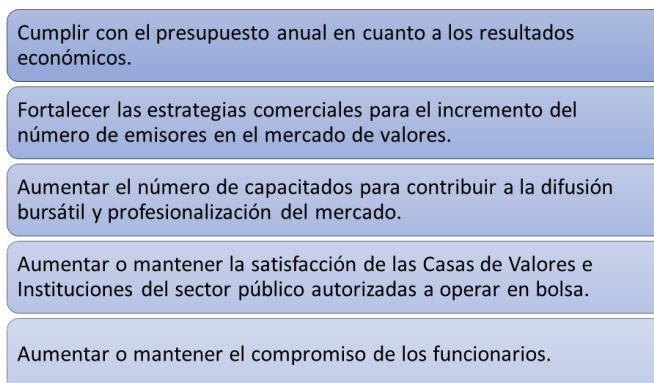
BVQ tiene una política de calidad basada en ofrecer servicios de calidad, costo adecuado, equidad, transparencia y competencia a sus clientes, con el objetivo de incrementar la rentabilidad, promover la cultura bursátil y la satisfacción del cliente. Cuenta con un equipo humano competente, procesos controlados, prácticas de gobierno corporativo y un nivel tecnológico adecuado para lograr su propósito.

3.3.1. Objetivos

La BVQ Sociedad Anónima, presenta los siguientes objetivos que se presentan en la Figura 3.

Figura 3

Objetivos de la BVQ



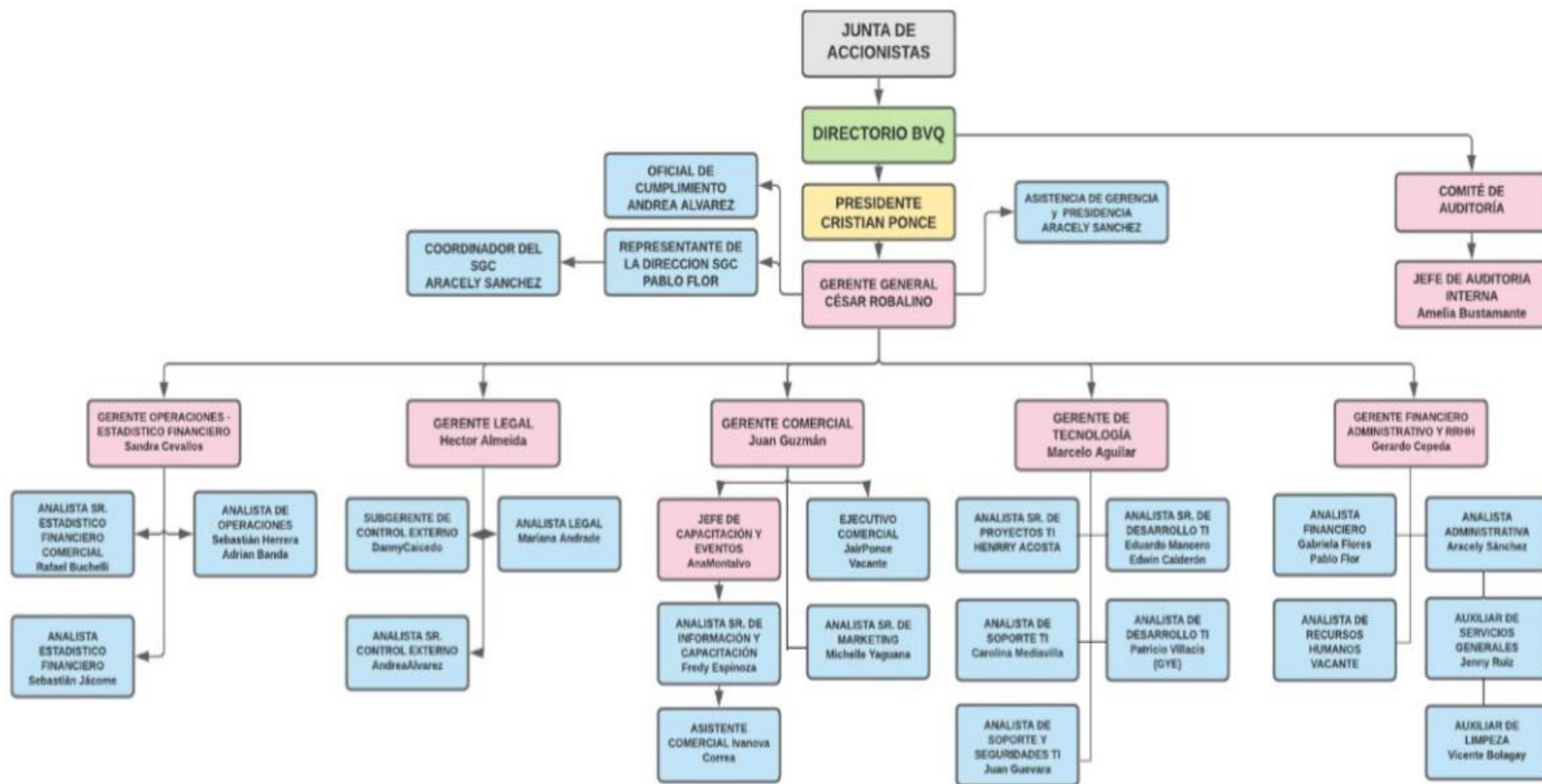
Nota: La figura representa los objetivos de la BVQ.

3.4. Diseño organizacional

3.4.1. Estructura organizacional

Figura 4

Estructura organizacional de BVQ



Nota: La figura representa la estructura organizacional de BVQ.

3.4.2. Funciones de las gerencias (áreas)

3.4.2.1. Gerencia de Operaciones.

La elaboración y divulgación de datos de mercado con el propósito de satisfacer los requerimientos regulatorios, apoyar la toma de decisiones de los distintos agentes del mercado y aumentar las ganancias de la organización. Seguidamente, en la Figura 5 se presentan las funciones gerenciales de BVQ.

Figura 5

Funciones gerenciales de BVQ

Controlar el correcto desenvolvimiento de los mecanismos de negociación de la BVQ.
Administrar los procesos operativos en cumplimiento de Leyes, reglamentos y normas de autorregulación.
Realizar el control de operaciones bursátiles y las aprobaciones que amerite.
Asesorar a la Institución en temas operativos.
Asesorar a los partícipes del mercado en manejo del sistema transaccional y ejecución de operaciones bursátiles.
Supervisar las tareas operativas respecto al mantenimiento de bases de datos de operaciones bursátiles.
Analizar e implementar nuevos productos bursátiles.
Elaboración y análisis de estadísticas bursátiles.
Administrar la información estadística de la BVQ.
Capacitar a funcionarios de la BVQ y de Casas de Valores sobre la operativa bursátil del mercado, para que conozcan y comprendan los instrumentos financieros y sus operaciones.
Portafolio de inversiones de la BVQ: Administrar el portafolio dentro de la política de inversión definida, recomendando a la Gerencia las inversiones y desinversiones para mejorar el rendimiento y proteger el riesgo del portafolio, generando ingresos de acuerdo al presupuesto.
Administración de estadísticas: preparar estadísticas e información de mercado (información diaria, reportes históricos, boletines e informes), publicando la misma a través de los diferentes medios para los diferentes actores de mercado (casas de valores, emisores, inversionistas, administradoras de fondos, aseguradoras, público en general).
Venta de información: liderar la estrategia de venta de información de la institución, identificando clientes prospectos, y negociando contratos y tarifas por la venta de información para generar ingresos en línea con el presupuesto.
Modelo CRM: manejar las relaciones con los clientes del Área, atender los requerimientos de información y realizar visitas y llamadas para dar seguimiento a las necesidades de los diferentes segmentos de clientes.

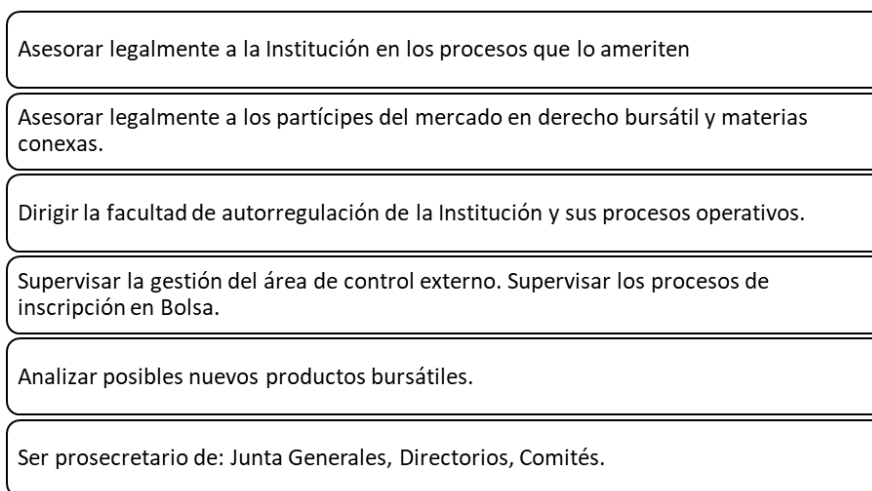
Nota: La figura representa las funciones gerenciales de BVQ.

3.4.2.2. Gerencia Legal.

Proporcionar asesoramiento jurídico a la BVQ y llevar a cabo la gestión de los distintos procesos legales que la institución emprende para cumplir con su finalidad social. Seguidamente, en la Figura 6 se presenta los lineamientos de la gerencia legal de BVQ.

Figura 6

Gerencia legal de BVQ



Nota: La figura representa la gerencia legal de BVQ.

3.4.2.3. Gerencia Comercial.

En la Figura 7 se presenta los lineamientos de la gerencia comercial de BVQ.

Figura 7

Gerencia comercial de BVQ

Fomentar la participación de emisores e inversionistas de diversos sectores de la economía, con el fin de impulsar el mercado de valores ecuatoriano y generar mayores ingresos para la institución. Dirigir el modelo de Customer Relationship Management (CRM) para diferentes segmentos de clientes, diseñar estrategias de marketing y promoción para difundir la cultura bursátil, y colaborar en la creación de nuevos productos y soluciones.

Elaborar y llevar a cabo estrategias comerciales que definan los clientes de la institución y su propuesta de valor, coordinando las actividades de las diferentes áreas y proponiendo precios para los productos, es una de las principales tareas.

Diseñar y aplicar estrategias por segmento de cliente para fomentar la participación de más inversionistas e identificar y coordinar visitas a potenciales emisores para atraer a más actores al mercado.

Liderar y coordinar la relación diaria con los diferentes segmentos de clientes y promover el uso de la herramienta de CRM, además de liderar las actividades de educación financiera y difusión bursátil.

Crear y promocionar nuevos productos y servicios de la Bolsa y el mercado de capitales mediante la identificación y coordinación de su diseño, así como la realización de actividades promocionales.

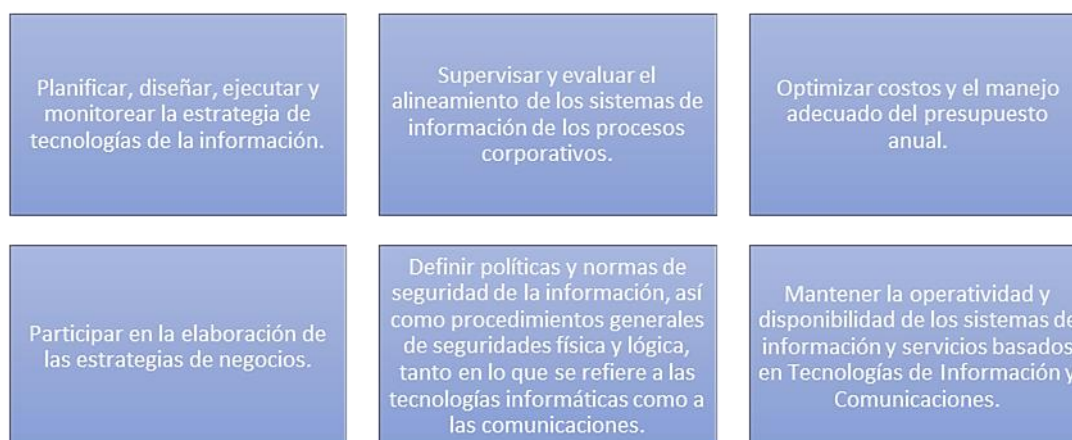
Nota: La figura representa la gerencia comercial de BVQ.

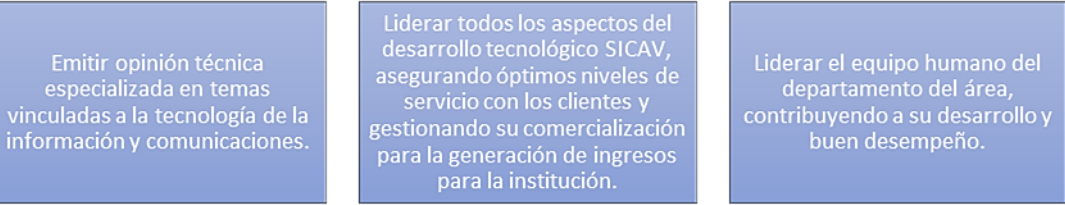
3.4.2.4. Gerencia de Tecnología.

El objetivo de la gestión de plataformas tecnológicas es optimizar y mejorar los procesos y servicios de la empresa. Es esencial garantizar el uso efectivo de los recursos tecnológicos para resolver las necesidades informáticas y coordinar la planificación estratégica. La tecnología de la información se utiliza para maximizar las capacidades de la empresa. En la Figura 8 se presentan los lineamientos de la gerencia de tecnología.

Figura 8

Gerencia de tecnología de BVQ





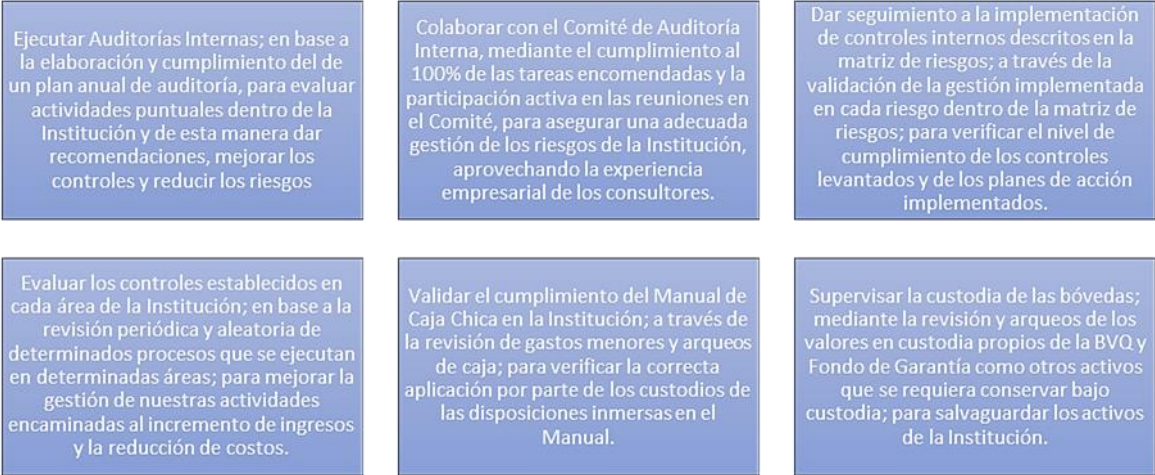
Nota: La figura representa la gerencia de tecnología de BVQ.

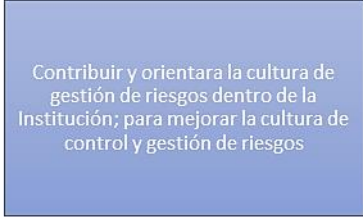
3.4.2.5. Gerencia Administrativa, Financiera y Recursos Humanos.

La Gerencia Administrativa, Financiera y Recursos Humanos es responsable de velar por la eficiencia de los procesos, la gestión de riesgos y el cumplimiento de los objetivos y metas de la institución. Para lograrlo, se llevan a cabo auditorías internas para revisar y monitorear los diversos procesos de acuerdo con el sistema de control interno y otros factores implementados. De esta manera, se busca mejorar la eficacia de los procesos y los controles establecidos. En la Figura 9 se presentan los lineamientos de esta gerencia.

Figura 9

Lineamientos de la Gerencia administrativa, Financiera y Recursos Humanos





Contribuir y orientara la cultura de gestión de riesgos dentro de la Institución; para mejorar la cultura de control y gestión de riesgos

Nota: La figura representa los lineamientos de la gerencia administrativa, Financiera y Recursos Humanos.

3.5. Productos y/o servicios

La BVQ tiene como objetivo principal ofrecer los servicios y herramientas necesarios para llevar a cabo la compraventa de títulos valores, además de realizar otras actividades conexas que sean necesarias para el adecuado desarrollo del mercado de valores, siempre y cuando se cuente con la autorización previa de la Junta de Política y Regulación Monetaria y Financiera. Para lograr este objetivo, la BVQ puede realizar toda clase de actos, contratos y negocios jurídicos que se realicen directamente, entera o parcialmente, con su objeto, así como establecer otros servicios que sean afines y compatibles con el mismo.

Sin embargo, la gestión adecuada de respaldos de información es crucial para el buen funcionamiento de la BVQ. Actualmente, se ha identificado que no se está aplicando un adecuado manejo de respaldos y estándares, lo que puede generar riesgos e interrupciones en la operación diaria de la empresa. Es fundamental que la BVQ tome medidas para mejorar su gestión de respaldos y aplicar estándares que garanticen la disponibilidad, integridad y confidencialidad de la información crítica de la empresa, como parte de su compromiso con la calidad y la satisfacción del cliente.

3.6. Diagnóstico organizacional

Con el objetivo realizar un diagnóstico organizacional y poder establecer las directrices en el manejo, administración y gestión de los respaldos de información,

para garantizar la continuidad del negocio de la BVQ, se llevó a cabo un proceso de levantamiento de información. Este proceso tuvo como objetivo identificar los medios de almacenamiento disponibles y sus características de usabilidad para garantizar la seguridad de la información crítica para la BVQ. Además, se aplicó un instrumento de recolección de datos dentro de la institución, el cual sirvió para la recopilación de información generada en la BVQ dispuesto en el Anexo 2, seguido por los resultados de la información generada en la BVQ en el Anexo 3, luego se presenta la encuesta técnica (Analista Senior de Soporte y Seguridad) en el Anexo 4 y por último los resultados de la Encuesta técnica (Análisis Senior de Soporte y Seguridad TI) en el Anexo 5.

Una vez realizado el levantamiento de información, este revela algunas debilidades en el proceso de respaldo de datos de la empresa BVQ.

En primer lugar, aunque la empresa realiza copias de seguridad de la información crítica y de apoyo de cada funcionario, el hecho de que estos respaldos se almacenen en varios dispositivos diferentes (nube, servidor, discos externos, PC personales) puede generar un problema de gestión y coordinación en caso de una falla o pérdida de información. Sería conveniente que la empresa considere centralizar el almacenamiento de sus respaldos de datos en un solo lugar, preferiblemente en un dispositivo de almacenamiento externo que permita una mayor capacidad y control.

En segundo lugar, aunque la empresa tiene en cuenta el tipo de respaldo y el tiempo de recuperación de los datos, es necesario tener un plan de contingencia que incluya la definición de tiempos máximos de recuperación en caso de una falla del sistema. La empresa debe establecer un proceso de recuperación de datos detallado y documentado que permita minimizar el impacto de una interrupción en la operación diaria de la empresa.

En tercer lugar, la empresa realiza test de recuperación de datos únicamente de las bases de datos de forma mensual. Sería recomendable que la empresa realice pruebas de recuperación de datos de forma regular, incluyendo pruebas de recuperación de datos de los demás dispositivos de almacenamiento, para asegurarse de que los respaldos son efectivos y que se puede recuperar la información en caso de una emergencia.

En cuarto lugar, la empresa no cuenta con dispositivos de redundancia para almacenamiento. La implementación de dispositivos de redundancia permitiría garantizar la continuidad de la operación en caso de una falla de hardware o pérdida de información. Es importante que la empresa considere invertir en este tipo de dispositivos para mejorar su capacidad de respuesta en situaciones de emergencia.

Asimismo, siguiendo con el proceso de levantamiento de información, se identificó la información considerada crítica para la continuidad del negocio de la BVQ y se categorizó según distintas características tales como tipo, importancia, nivel de confidencialidad, tamaño, lugar de almacenamiento, frecuencia, entre otros. Como resultado de este proceso, se determinó que la BVQ cuenta actualmente con varios lugares de almacenamiento, los cuales se detallan en la Tabla 34.

Tabla 34

Lugares actuales de almacenamiento

Lugar Almacenamiento	Ubicación	Tamaño	Detalle
SharePoint	Cuenta Office 365	1.4 TB	Información generada en los respectivos departamentos.
OneDrive	Cuenta Office 365	1 TB (por usuario)	Información de generada por los funcionarios, respecto al trabajo que desempeñan.
Disco .47	Data Center	4 TB	Respaldos de bases de datos históricos.
Disco .35	Data Center	500 GB	Respaldo de bases de datos temporales. Respaldo de información de funcionarios y archivos de correos electrónicos.

Servidor BDT	Nube Azure	126 GB (C:)	Servidor de Bases de Datos y LOG de Bases de Datos.
		510 GB (F:)	
		510 GB (G:)	

Nota: Esta tabla presenta los lugares actuales de almacenamiento.

La Tabla 34 muestra los diferentes medios de almacenamiento que contienen toda la información crítica para el funcionamiento de la institución y que garantizan la continuidad del negocio. A pesar de la distribución adecuada de la información en cada una de las unidades, el análisis llevado a cabo revela una falta de estandarización apropiada de la misma.

Además, en la Tabla 35 y la gráfica de la

Figura 10 se puede apreciar claramente el crecimiento de la información en los últimos cinco años, expresado en gigabytes. Este hecho subraya la importancia de una gestión adecuada de la información y la necesidad de establecer políticas y estrategias eficaces para su manejo y control.

Tabla 35

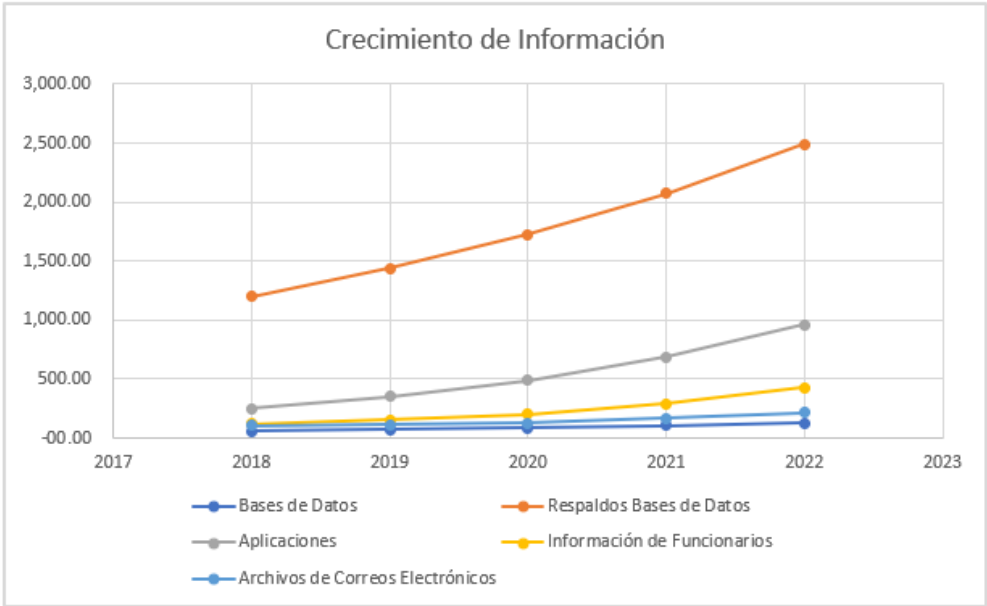
Crecimiento de Información

Información	2018	2019	2020	2021	2022
Bases de Datos	60.00	72.00	86.40	103.68	124.42
Respaldos Bases de Datos	1,200.00	1,440.00	1,728.00	2,073.60	2,488.32
Aplicaciones	250.00	350.00	490.00	686.00	960.40
Información de funcionarios	120.00	156.00	202.80	294.06	426.39
Archivos de Correos Electrónicos	105.00	115.50	127.05	165.17	214.71

Nota: Esta tabla presenta el crecimiento de información.

Figura 10

Crecimiento de Información



Nota: La figura representa el crecimiento de información.

Asimismo, el conjunto de datos que se presenta a continuación, ha experimentado un crecimiento constante en cada uno de los años evaluados, tal como se observa en la Tabla 36 adjunta.

Tabla 36

Crecimiento porcentual (constante)

Información	Crecimiento (entre 2018 y 2022)
Bases de Datos	20%
Respaldos Bases de Datos	20%
Aplicaciones	40%

Nota: Esta tabla presenta el crecimiento porcentual (constante).

Es importante destacar que, durante el periodo de estudio, comprendido entre los años 2020 y 2021, se ha registrado un notable aumento en la información, tal como se evidencia en la Tabla 37. Este incremento se ha atribuido a factores inesperados como el confinamiento generado por la pandemia.

Tabla 37

Crecimiento porcentual (variación)

Información	Crecimiento (entre 2018 y 2019)	Crecimiento (entre 2020 y 2022)
Información de funcionarios	30%	45%
Archivos de Correos Electrónicos	10%	25%

Nota: Esta tabla presenta el crecimiento porcentual (*variación*).

Según los datos obtenidos anteriormente, se lograron los siguientes detalles, los cuales fueron analizados y utilizados para proponer mejoras en la gestión:

- Información duplicada.
- Nombres de archivos no estandarizados.
- No se encuentran catalogados con un nivel de importancia.
- No se encuentran organizados (tipo - tamaño).
- No se encuentran definidos si son confidenciales.

La gestión y administración de la información es un aspecto fundamental. En este sentido, es importante conocer la forma en que se maneja y almacena la información, y quiénes son los responsables de su gestión en cada área de la organización.

En este contexto, se ha desarrollado una matriz de información que permitirá identificar los datos que manejan los funcionarios de cada uno de los departamentos de la BVQ. Este registro detallado de la información es crucial para la evaluación y análisis que se llevará a cabo en la propuesta de mejora de la gestión de respaldos de información. A través de la matriz presentada en la Figura 11, se podrá identificar de manera precisa los datos que maneja cada funcionario, permitiendo así una mejor comprensión del flujo de información en la organización y la identificación de los puntos críticos en los procesos de respaldo de información.

Figura 11

Matriz de información por cada funcionario/departamento

Funcionario	SLC	SLC_BVG	Documex	SicavSA	Insoft	InsoftNIIIF	Nomina	GfondosNII	SicavVGR	SicavFG
ACOSTA CASTILLO HENRY RAMIRO	Rdp41	Rdp41	Rdp41	PP	PP	PP	App41	PP	PP	Rdp41
AGUILAR SALSUERO MARCELO DAVID	---	---	---	---	---	---	---	---	---	---
ALMEDA GRANJA HECTOR EDUARDO	---	---	---	---	---	---	---	Rdp41	---	---
ALVAREZ BUSTAMANTE ANDREA PAULINA	Rdp41	---	Rdp41	PP	---	Rdp41	---	Rdp41	---	---
ANDRADE BORGES MARIANA ODETE	---	---	---	Rdp41	---	---	---	Rdp41	---	---
CRISTHIAN PAUL MADERA MORALES	Rdp41-App41	Rdp41	Rdp41	---	---	Rdp41	---	---	PP	---
BOLAGAY IZA VICENTE OLMEDO	---	---	---	Rdp41	PP	---	---	---	---	---
TREJO MISHELL	PP	---	---	---	---	---	---	Rdp41	---	---
BUSTAMANTE RODRIGUEZ AMELIA DEL CISNE	Rdp41	---	Rdp41	---	PP	Rdp41	---	---	Rdp41	---
CAICEDO YANEZ DANNY ORLANDO	Rdp41	---	---	Rdp41	---	---	---	Rdp41	---	---
CALDERON ZAMBRANO EDWIN VINICIO	---	---	---	---	---	---	---	---	Rdp41	---
CEPEDA PEÑAHERRERA GERARDO ALEJANDRO	---	---	Rdp41	PP	PP	Rdp41	App41	---	---	Rdp41
CEVALLOS ARIAS SANDRA JUDITH	PP	---	---	---	Rdp41	---	---	Rdp41	---	---
CORREA VINUEZA JAHAIRA IVANOVA	---	---	---	PP	---	---	---	---	Rdp41	---
ESPINOSA VILLAMARIN JORGE FREDY	Rdp41	---	Rdp41	PP	Rdp41	Rdp41	---	---	---	---
BRYAN MOISES KHARBOUCH CEPEDA	PP	---	---	PP	---	---	---	Rdp41	---	PP
FLORES ALVEAR SANDRA GABRIELA	Rdp41	---	---	PP	---	---	App41	---	Rdp41	Rdp41
SUEVARA PAZ Y MIRO JUAN DIEGO	---	---	---	---	Rdp41	---	---	---	---	---
GERENTE COMERCIAL	---	---	---	---	---	---	---	Rdp41	---	---
HERRERA YANEZ JOFRE SEBASTIAN	Rdp41-App41	Rdp41	Rdp41	PP	PP	Rdp41	---	---	Rdp41	---
JACOME PANCHI JUAN SEBASTIAN	---	---	---	---	---	---	---	---	---	---
MANCERO NOBOA EDUARDO DANIEL	---	---	---	---	---	---	---	---	---	---
MEDIAVILLA HERRERA VANESSA CAROLINA	---	---	---	---	PP	---	---	---	---	---
MONTALVO NOBOA ANITA PAULINA	---	---	Rdp41	Rdp41	---	Rdp41	---	Rdp41	---	---
SABRINA CRIOLLO	---	---	---	---	---	---	---	---	Rdp41	---
RUIZ VINUEZA JENNY EDITH	---	---	Rdp41	Rdp41	---	Rdp41	---	---	---	---
SANCHEZ DELGADO ROSA ARACELY	---	---	PP	---	PP	---	---	---	---	---
VILLACIS GUILLEN PATRICIO JOSE	---	---	---	---	---	---	---	Rdp41	---	---
YAGUANA MOREIRA MICHELLE CAROLINA	---	---	---	Rdp41	---	---	---	---	Rdp41	---
CESAR ROBALINO	---	---	---	---	---	---	---	Rdp41	---	---
ASISTENTE-FINANCIERO	---	---	Rdp41	---	---	---	---	---	Rdp41	---

Nota: La figura representa la matriz de información por cada funcionario / departamento.

Una vez realizada la matriz en el marco del proceso de diagnóstico, también se realizó un análisis detallado de la gestión de la información, y se presentaron los resultados en la Figura 12. En esta tabla se puede apreciar, de manera detallada, la información que es gestionada y administrada por cada funcionario, de acuerdo con sus funciones establecidas. Estos hallazgos son relevantes para entender la forma en que se maneja la información en la organización y para diseñar estrategias de mejora en la gestión de los respaldos de información. Además, esta información es importante para poder clasificarla y estandarizarla.

Figura 12

Tipo de información por funcionario

Funcionario	Area	Correo Electrónico	Archivos Excel	Archivos Word	Archivos PDF	Imágenes	Archivos TXT	Archivos XML
ACOSTA CASTILLO HENRY RAMIRO	Tecnología	SI	SI	SI	SI	SI	SI	SI
AGUILAR SALGUERO MARCELO DAVID	Tecnología	SI	SI	SI	SI	SI	SI	SI
ALMEIDA GRANJA HECTOR EDUARDO	Legal	SI	NO	SI	SI	NO	NO	SI
ALVAREZ BUSTAMANTE ANDREA PAULINA	Legal	SI	NO	SI	SI	NO	NO	SI
ANDRADE BORGES MARIANA ODETE	Legal	SI	NO	SI	SI	NO	NO	SI
CRISTHIAN PAUL MADERA MORALES	Operaciones	SI	SI	SI	SI	NO	SI	SI
BOLAGAY IZA VICENTE OLMEDO	Servicios	SI	NO	NO	NO	NO	NO	SI
TREJO MISHELL	Comercial	SI	SI	SI	SI	NO	SI	NO
BUSTAMANTE RODRIGUEZ AMELIA DEL CISNE	Auditoría	SI	SI	SI	SI	NO	NO	NO
CAICEDO YANEZ DANNY ORLANDO	Legal	SI	SI	SI	SI	NO	NO	NO
CALDERON ZAMBRANO EDWIN VINICIO	Tecnología	SI	SI	SI	SI	SI	SI	SI
CEPEDA PEÑAHERRERA GERARDO ALEJANDRO	Talento Humano	SI	SI	SI	SI	SI	NO	NO
CEVALLOS ARIAS SANDRA JUJUTH	Operaciones	SI	SI	SI	SI	NO	NO	NO
CORREA VINUEZA JAHAIRA IVANOVA	Estadísticas	SI	SI	SI	SI	NO	NO	NO
ESPINOSA VILLAMARIN JORGE FREDY	Comercial	SI	SI	SI	SI	NO	NO	NO
BRYAN MOISES KHARBOUCH CEPEDA	Financiero	SI	SI	NO	NO	SI	NO	NO
FLORES ALVEAR SANDRA GABRIELA	Financiero	SI	SI	NO	NO	SI	NO	NO
GUEVARA PAZ Y MIÑO JUAN DIEGO	Tecnología	SI	SI	SI	SI	SI	SI	SI
HERRERA YANEZ JOFFRE SEBASTIAN	Operaciones	SI	SI	SI	SI	NO	SI	NO
JACOME PANCHI JUAN SEBASTIAN	Estadísticas	SI	SI	SI	SI	NO	NO	NO
IMANCERO NOBOA EDUARDO DANIEL	Tecnología	SI	SI	SI	SI	SI	SI	SI
MEDIAVILLA HERRERA VANESSA CAROLINA	Tecnología	SI	SI	SI	SI	SI	SI	SI
MONTALVO NOBOA ANITA PAULINA	Comercial	SI	SI	SI	SI	NO	NO	NO
SABRINA CRIOLLO	Comercial	SI	SI	SI	SI	NO	NO	NO
RUIZ VINUEZA JENNY EDITH	Servicios	SI	NO	NO	NO	NO	NO	NO
SANCHEZ DELGADO ROSA ARACELY	Administración	SI	SI	SI	SI	NO	NO	NO
VILLACIS GUILLEN PATRICIO JOSE	Tecnología	SI	SI	SI	SI	SI	SI	SI
YAGUANA MOREIRA MICHELLE CAROLINA	Marketing	SI	NO	NO	NO	SI	NO	NO

Nota: La figura representa el tipo de información por funcionario.

Asimismo, para tener una visión más clara de la situación actual en relación a la gestión de respaldos en la BVQ, se procederá a realizar un análisis FODA que se presenta en la Figura 13. Este análisis permitirá identificar las fortalezas, oportunidades, debilidades y amenazas que enfrenta la empresa en cuanto a la gestión de información y respaldos, lo que permitirá diseñar estrategias efectivas para mejorar la gestión de información y garantizar la continuidad de la operación diaria de la empresa.

Figura 13

Diagnóstico organizacional (FODA)



Nota: La figura representa el diagnóstico organizacional (FODA).

El análisis FODA realizado para la BVQ revela varios aspectos importantes. En cuanto a las fortalezas, la BVQ cuenta con una amplia experiencia en el mercado de valores y una posición dominante en el mercado local. Además, la BVQ ofrece una amplia gama de servicios y herramientas para la compraventa de títulos valores, lo que le permite brindar soluciones integrales a sus clientes. Por otro lado, las debilidades identificadas en el análisis FODA incluyen la falta de un adecuado manejo de respaldos y estándares, lo que puede generar riesgos e interrupciones en la operación diaria de la empresa.

En cuanto a las oportunidades, la BVQ tiene un gran potencial de crecimiento en el mercado de valores a nivel nacional e internacional. La BVQ también puede

expandir su oferta de servicios y herramientas para adaptarse a las necesidades cambiantes de sus clientes y del mercado en general. Por último, en cuanto a las amenazas, la BVQ enfrenta una competencia cada vez mayor en el mercado de valores local, lo que puede reducir su participación de mercado. Además, la volatilidad del mercado y las fluctuaciones económicas pueden afectar negativamente el desempeño de la BVQ y la demanda de sus servicios y herramientas.

En general, el análisis FODA muestra que la BVQ tiene fortalezas significativas, pero también hay debilidades y amenazas que deben ser abordadas. La BVQ puede aprovechar sus fortalezas para capitalizar las oportunidades y superar las debilidades y amenazas, mediante la implementación de estrategias sólidas y una gestión efectiva de respaldos y estándares de información.

Asimismo, la gestión adecuada de la información es esencial para el funcionamiento óptimo de cualquier empresa. En el caso de la empresa BVQ, se ha identificado un problema relacionado con la gestión de respaldos de información, lo que ha generado problemas de seguridad y de acceso a la información en numerosas ocasiones. Ante esta situación, se ha decidido llevar a cabo una propuesta de mejora de la gestión de respaldos de información de la empresa.

Para poder abordar el problema de manera efectiva, es necesario realizar un análisis detallado de las posibles causas que lo han generado. Para esto, se ha utilizado la herramienta del diagrama de Ishikawa, también conocido como "espina de pescado" o "diagrama de causa y efecto". Este diagrama permite identificar las causas raíz del problema y, de esta manera, enfocar los esfuerzos en las áreas que requieren mayor atención. A continuación, se presenta en la Figura 14 el diagrama de Ishikawa elaborado para el problema de gestión de respaldos de información de la empresa BVQ.

Figura 14

Diagrama de Ishikawa



Nota: La figura representa el diagrama de Ishikawa de la empresa BVQ.

Tras haber realizado un análisis exhaustivo del problema de gestión de respaldos de información en la empresa BVQ, y haber utilizado la herramienta del diagrama de Ishikawa para identificar las posibles causas raíz, se ha llegado a un análisis detallado de las causas del problema y sus posibles soluciones. A continuación, se presenta un análisis detallado de las causas identificadas y se discuten posibles estrategias para mejorar la gestión de respaldos de información en la empresa BVQ.

- **Procesos:** Uno de los principales factores que contribuyen al problema de gestión de respaldos de información en la empresa BVQ es la falta de procesos claramente definidos y estandarizados para realizar y gestionar las copias de seguridad. Además, la falta de documentación en los procesos de respaldo y restauración dificultan aún más el problema.
- **Recursos:** La limitada capacidad para invertir en nuevas tecnologías y servicios debido a restricciones financieras puede ser un factor que contribuye a la debilidad de la empresa en la gestión de respaldos de información. La falta de recursos también puede estar afectando la capacidad de la empresa para implementar medidas de seguridad adicionales, como la implementación de dispositivos de redundancia.
- **Tecnología:** La tecnología es una de las principales oportunidades que tiene la empresa para mejorar su gestión de respaldos de información. La implementación de nuevas tecnologías y herramientas para el almacenamiento, gestión y recuperación de información pueden mejorar significativamente la eficiencia y calidad de los servicios ofrecidos.

- Comunicación: La falta de comunicación clara entre los diferentes departamentos de la empresa puede estar afectando la gestión de respaldos de información. La falta de comunicación puede dar lugar a la falta de entendimiento de los requisitos de respaldo y restauración de información, lo que a su vez puede generar riesgos e interrupciones en la operación diaria de la empresa.

- Política: Ciertamente, la restricción financiera es un problema que afecta a la empresa y puede impactar su capacidad para competir y mantenerse al día con las tendencias del mercado financiero. Si bien es importante mantener un equilibrio financiero sólido, es igualmente importante reconocer la necesidad de invertir en nuevas tecnologías y servicios para mantenerse a la vanguardia del mercado y seguir siendo competitivos. Por lo tanto, es necesario evaluar cuidadosamente las opciones de inversión y considerar cómo estas pueden generar beneficios a largo plazo para la empresa. La falta de inversión en nuevas tecnologías y servicios puede limitar la capacidad de la empresa para expandir su oferta de servicios y herramientas, lo que a su vez puede limitar su capacidad para atraer y retener a nuevos clientes.

Es importante que la gerencia evalúe de manera objetiva las oportunidades de inversión y considere la posibilidad de obtener financiamiento externo si es necesario.

En general, la gestión de respaldos de información es un aspecto crítico para la continuidad de la operación de la empresa, y es necesario que se realicen mejoras en este proceso para minimizar el riesgo de interrupción en caso de una falla de sistema o pérdida de información. La implementación de un plan de contingencia

detallado, la realización regular de pruebas de recuperación de datos y la consideración de dispositivos de redundancia son algunas de las acciones que la empresa puede tomar para mejorar su capacidad de respuesta en situaciones de emergencia.

CAPITULO IV: Resultados

4.1. Propuesta de mejora

4.1.1. Diagnóstico

En el presente trabajo de titulación, se ha llevado a cabo un diagnóstico sobre la situación actual de la BVQ en materia de gestión de respaldos de información. Tras realizar una exhaustiva investigación y análisis de la empresa, se ha identificado que existe una inadecuada aplicación en el manejo de respaldos y estándares, lo que puede generar riesgos e interrupciones en la operación diaria de la empresa. Es por ello, que se ha diagnosticado que la BVQ necesita implementar medidas para mejorar su gestión de respaldos y aplicar estándares que garanticen la disponibilidad, integridad y confidencialidad de la información crítica de la empresa.

Además, se ha llevado a cabo un análisis detallado de la situación actual de la BVQ en cuanto a su gestión de respaldos de información. Se ha identificado un inadecuado manejo de respaldos y estándares que puede generar problemas en la continuidad del negocio, así como riesgos en cuanto a la seguridad de la información. Por tanto, se utilizará toda la información recopilada durante el proceso de investigación para identificar los diferentes elementos que componen el problema analizado, y proponer medidas concretas para su solución.

Por ello, los resultados esperados de la implementación de medidas de mejora en la gestión de respaldos de información en la BVQ se enfocan en la reducción de los riesgos asociados a la falta de disponibilidad, integridad y confidencialidad de la información crítica de la empresa. Asimismo, se espera mejorar la eficiencia en la operación diaria de la empresa, y aumentar la satisfacción del cliente, al garantizar la calidad en la gestión de la información que maneja la BVQ. La implementación de estas medidas no solo beneficiará

a la empresa, sino que también tendrá un impacto positivo en todo el mercado de valores de Quito, al aumentar la confianza en la gestión de información en el ámbito financiero.

4.1.2. Diseño de la mejora

La propuesta de mejora de la gestión de respaldos de información de la BVQ, tiene como objetivo mejorar la gestión de los respaldos de información crítica de la organización, de manera que se puedan minimizar los riesgos y asegurar la continuidad del negocio en caso de alguna contingencia. La propuesta sugiere implementar un sistema de respaldo de información que garantice la integridad, confidencialidad y disponibilidad de la información almacenada, y que permita su recuperación en caso de un desastre. También, se propone la realización de pruebas periódicas para asegurar que el sistema de respaldo funcione correctamente y se puedan corregir posibles fallos antes de una contingencia real.

En este sentido, se presenta en la Tabla 38 donde se establece la propuesta en base a las debilidades encontradas en la BVQ.

Tabla 38*Propuesta de mejora*

Problemas encontrados	Acciones a llevar a cabo	Actividades	Presupuesto	Responsable	Objetivos
Insuficiencia en la gestión de respaldos de información crítica, lo que puede generar riesgos e interrupciones en la operación diaria de la empresa.	Implementar una política de gestión de respaldos de información.	<ol style="list-style-type: none"> 1. Diseñar una propuesta de mejora que contemple la implementación de procesos y procedimientos estandarizados para el manejo, administración y gestión de los respaldos de información. <ol style="list-style-type: none"> A. Procesos de gestión de respaldos de información. B. Definir los procesos de gestión de respaldo de información. C. Establecer los tipos, periodicidad y permanencia de backup. D. Definir la política de clasificación de los activos de información en la BVQ. E. Establecer el inventario de activos en la BVQ. 	\$25.000	Gerente de TI	Garantizar la continuidad del negocio de la BVQ.
Falta de coordinación efectiva entre gerencias y colaboradores.	Establecer un proceso de coordinación efectivo entre las gerencias y colaboradores para asegurar una gestión	<ol style="list-style-type: none"> 1. Desarrollar e implementar un plan de coordinación efectiva entre gerencias y colaboradores, a través de la creación de mecanismos de comunicación y coordinación claros y eficientes, con el objetivo de mejorar la gestión de la información crítica y evitar interrupciones en la operación diaria de la empresa. 	\$8.000	Gerente de TI	Establecer una comunicación efectiva y coordinación entre las gerencias y colaboradores de la empresa en relación a la gestión de

	adecuada de la información.	<p>A. Establecer una propuesta de coordinación entre las gerencias y colaboradores.</p> <p>B. Definir los roles y responsabilidades de cada persona involucrada en el proceso de respaldo de información.</p>			información y respaldos.
Falta de mecanismos de control que puede generar riesgos e interrupciones en la operación diaria de la BVQ.	Diseñar y establecer controles periódicos para garantizar que los respaldos de información se estén realizando correctamente y en los plazos establecidos.	<ol style="list-style-type: none"> 1. Establecer controles adecuados para el proceso de respaldo de información 2. Definir indicadores de crecimiento y gestión de espacio de almacenamiento de los respaldos de información de la BVQ 	\$6.000	Gerente de TI	Mejorar la eficacia del proceso y asegurar que se estén cumpliendo los objetivos y metas establecidos en la propuesta de mejora.
Limitada capacidad para invertir en nuevas tecnologías y servicios debido a restricciones financieras.	Optimizar la infraestructura tecnológica existente.	<ol style="list-style-type: none"> 1. Realizar un diagnóstico de la infraestructura tecnológica actual. 2. Establecimiento de una propuesta de actualización de tecnología para mejorar la eficiencia del proceso de respaldo de información. 	\$5.000	Gerente de TI	Mejorar la eficiencia y eficacia de los procesos de la empresa.
Establecimiento del plan de acción	Establecer un equipo de proyecto para el análisis de costo-benéfico.	<ol style="list-style-type: none"> 1. Realizar un análisis de costo beneficio y costo efectividad sobre la propuesta de mejora 	\$5.000	Equipo de proyecto	Evaluar la viabilidad económica y la efectividad de la propuesta de mejora.

Nota: Esta tabla presenta la propuesta de mejora.

La propuesta de mejora presentada en la tabla anterior contempla acciones concretas que abordan las debilidades identificadas en la empresa. En particular, se plantean soluciones para mejorar la gestión de los respaldos de información crítica. Estas iniciativas, además, se llevan a cabo con un presupuesto razonable y con un enfoque claro en la responsabilidad de cada uno de los miembros del equipo de trabajo.

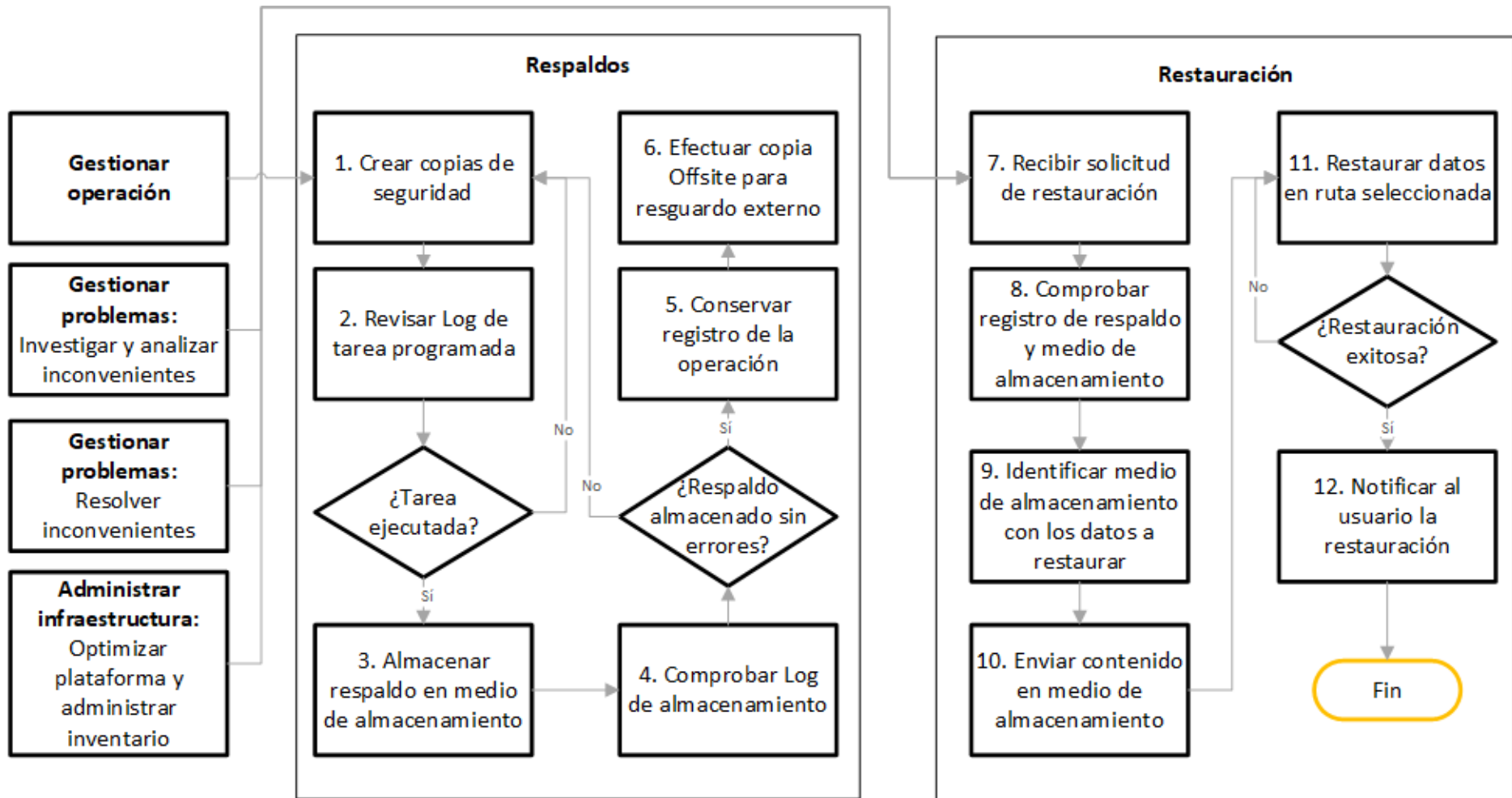
4.1.2.1. Definir el proceso de gestión de respaldos de información.

En lo que respecta a la insuficiente gestión de respaldos de información crítica, la propuesta sugiere una serie de actividades, tales como la definición de las estrategias de backup, y la implementación de procesos de verificación y validación de los respaldos. Estas medidas permitirán a la empresa asegurar la integridad y disponibilidad de su información crítica en caso de eventos disruptivos, minimizando el riesgo de interrupciones en su operación diaria.

Igualmente, se ha diseñado un diagrama de flujo que representa de manera gráfica el proceso de gestión de respaldos de información, con el objetivo de ilustrar de manera clara y concisa el procedimiento propuesto. La Figura 15 muestra el mencionado diagrama, que permitirá mejorar la eficiencia y eficacia en la gestión de respaldos de información en la BVQ. Cabe destacar, que este proceso de mejora es fundamental en la actualidad, en vista de la creciente importancia de la información y su papel estratégico en el desempeño de la institución.

Figura 15

Gestión de respaldos de información



Nota: La figura representa la gestión de respaldos de información.

4.1.2.2. Establecer el Tipo, periodicidad y permanencia de backup.

Una vez finalizada la etapa de análisis y diagnóstico de la situación actual en la BVQ, se solicitará al encargado de la gestión de tecnologías de la información llevar a cabo los procesos necesarios para adoptar el proceso sugerido. A tal efecto, se requerirá la instalación de los paquetes de software necesarios para garantizar que todas las aplicaciones, bases de datos y el Core del negocio estén respaldados adecuadamente. Asimismo, se definirán los nodos, clases de gestión, programaciones y tareas administrativas necesarias para una buena administración de la herramienta.

Una vez adoptados los procesos, se solicitará al encargado varios documentos y herramientas para la operación. En primer lugar, se solicitará que se defina una política de respaldo y recuperación de información. Esta política debe incluir el alcance, los objetivos generales y específicos, el tipo de información susceptible de ser respaldada por la plataforma, los deberes y responsabilidades de los administradores de la plataforma y los usuarios, así como un glosario de términos. También se debe incluir el grupo de soporte encargado de la gestión de la plataforma, su dirección o unidad del negocio, los horarios de atención del soporte, el tipo de backup, la periodicidad con que se ejecuta el respaldo y la retención.

En segundo lugar, en la Tabla 39, se presenta un cuadro resumen que expone los aspectos más significativos que se deben considerar al momento de diseñar una política de respaldo de información.

Por último, se definirá una política para la administración de medios de almacenamiento. Esta política debe incluir el alcance, los objetivos generales y específicos, los tipos de medios de almacenamiento utilizados en la administración de la plataforma de respaldos de información, el grupo responsable por la tutela de los medios al interior de la organización, el procedimiento empleado para la destrucción

de medios defectuosos, los procedimientos en materia de seguridad para la custodia y accesibilidad a los medios al interior de la organización y la empresa encargada de la custodia externa de la copia Offsite.

Tabla 39

Tipo, periodicidad y permanencia de backup

Tipo de respaldo	Periodicidad	Permanencia (Días)	
Archivos y aplicativos	Diario	30	
	Semanal	120	
	Mensual	300	
	Histórico	Permanente	
Información de funcionarios	Mensual	300	
Archivos de Correos Electrónicos	Diario	30	
Cuenta Office 365	Semanal	100	
Data Center	Diario	30	
Data Center	Histórico	Permanente	
Servidor BDT	Offsite	Semanal	100

Nota: Esta tabla presenta el tipo, periodicidad y permanencia de backup.

4.1.2.3. Definir la propuesta de política de clasificación de los activos de información en la BVQ.

Además de las acciones propuestas en la tabla de mejora, se recomienda establecer una política de clasificación de los activos de información en la BVQ. Esta política permitirá gestionar y proteger adecuadamente los activos de información crítica para el negocio, y debe ser adoptada por todas las áreas, así como departamentos de la BVQ. La política de clasificación de activos de información debe estar basada en la norma ISO/IEC 27001 (2022), la cual establece un marco de referencia para la gestión de la seguridad de la información y define los requisitos mínimos para un sistema de gestión de seguridad de la información (SGSI).

Para implementar esta política, se deben definir los activos de información crítica y establecer un proceso de clasificación que permita asignar niveles de protección y acceso a cada uno de ellos. Se recomienda realizar una evaluación de riesgos que permita identificar los activos de información crítica y sus riesgos asociados. Una vez identificados, se pueden clasificar los activos en función de su importancia para el negocio y su nivel de confidencialidad, integridad y disponibilidad.

Es importante que esta política de clasificación de activos de información sea comunicada y capacitada a todos los colaboradores involucrados en la gestión de información en la BVQ, con el fin de asegurar que todos comprendan su importancia y puedan aplicarla en su día a día. La capacitación debe ser continua y adaptada a las necesidades de cada área y departamento, con el fin de garantizar su comprensión y aplicación efectiva. A continuación, se presenta en la Tabla 40 posibles estrategias que se pueden implementar para establecer una política de clasificación de los activos de información en la BVQ.

Tabla 40

Propuesta de política de clasificación de los activos de información en la BVQ

Estrategias	Actividades	Responsable	Presupuesto	Objetivos
Identificación de los activos de información	Realizar un inventario detallado de los activos de información existentes en la BVQ, incluyendo datos de su ubicación, propietario, nivel de importancia y criticidad.	Gerente de Sistemas	\$2.000	Establecer una lista completa y actualizada de los activos de información, con el fin de identificar y priorizar los recursos de protección de información.
Clasificación de los activos de información	Definir una categorización de los activos de información según su nivel de	Gerente de Sistemas y Gerente de Seguridad	\$5.000	Establecer un esquema de clasificación de los activos de información en función de su importancia y

	<p>importancia, criticidad y de la confidencialidad.</p> <p>Asignar a cada categoría un conjunto de medidas de protección acordes.</p>	de la Información		<p>criticidad, con el fin de priorizar los recursos de protección de información, reducir los riesgos de pérdida o robo de datos críticos y mejorar la eficiencia en el manejo de la información.</p>
Definición de políticas y procedimientos	<p>Desarrollar políticas y procedimientos claros y detallados que definan cómo se deben manejar los distintos activos de información, incluyendo aspectos como la autorización de acceso, la gestión de contraseñas, la conservación y custodia de la información, la transmisión segura de datos, la realización de copias de seguridad y la recuperación de información.</p>	Gerente de Sistemas y Gerente de Seguridad de la Información	\$10.000	<p>Establecer una guía clara y detallada de cómo se deben manejar los distintos activos de información en la BVQ, con el fin de evitar la pérdida de información valiosa y mejorar la eficiencia en el manejo de la información.</p>
Capacitación y comunicación	<p>Capacitar y comunicar a todos los colaboradores involucrados en la gestión de información en la BVQ sobre la importancia y los procedimientos de la política de clasificación de activos de información.</p>	Gerente de Sistemas y Gerente de Seguridad de la Información	\$3.000	<p>Garantizar que todos los colaboradores involucrados en la gestión de información en la BVQ tengan conocimiento de la política de clasificación de activos de información y cómo aplicarla, reduciendo los riesgos de pérdida o robo de datos críticos.</p>

Nota: Esta tabla presenta la propuesta de política de clasificación de los activos de información en la BVQ.

4.1.2.4. Establecer la propuesta de inventario de activos en la BVQ.

Seguidamente, se puede indicar que, en un entorno empresarial cada vez más digitalizado, la gestión de la información es fundamental para garantizar la continuidad del negocio. En este contexto, el primer paso para una gestión efectiva de la información es tener un inventario completo de los activos de información de la organización. Esto permite conocer en detalle el tipo de información que se maneja, su ubicación, grado de confidencialidad, accesibilidad y los controles de seguridad necesarios para protegerla adecuadamente.

La BVQ no es ajena a esta necesidad, ya que maneja información crítica y confidencial sobre las operaciones bursátiles, por lo que es necesario contar con un inventario completo de sus activos de información. Esto permitirá a la BVQ conocer en detalle su infraestructura de información y tomar las medidas necesarias para protegerla de manera efectiva. Por tanto, establecer un inventario completo de los activos de información en la BVQ es una estrategia clave en la propuesta de mejora de la gestión de respaldos de información como se indica en la Tabla 41.

Tabla 41

Propuesta de inventario de activos en la BVQ

Estrategias	Descripción
Realizar una auditoría de activos de información	Realizar un análisis exhaustivo de la información de la BVQ, incluyendo la identificación de los activos de información, su ubicación, grado de confidencialidad, accesibilidad y controles de seguridad requeridos.
Asignar un responsable de activos de información	Asignar un custodio o responsable para cada uno de los activos de información identificados en la auditoría, con el fin de garantizar la protección y seguridad de la información, así como establecer claramente los roles y

	responsabilidades de cada persona involucrada en la gestión de la información.
Establecer una política de control de acceso	Establecer una política clara de control de acceso para todos los activos de información de la BVQ, definiendo quiénes tienen acceso a ellos y en qué circunstancias, con el fin de evitar posibles vulnerabilidades y reducir el riesgo de incidentes de seguridad.
Implementar controles de seguridad adecuados	Implementar los controles de seguridad adecuados para cada uno de los activos de información, según su grado de confidencialidad y accesibilidad, como la encriptación, la identificación y autenticación de usuarios, entre otros.
Realizar capacitación al personal involucrado	Capacitar al personal involucrado en la gestión de los activos de información, con el fin de asegurar que entiendan la importancia de su rol en la protección y seguridad de la información y que estén familiarizados con los procesos y procedimientos establecidos para su gestión.

Nota: Esta tabla presenta la propuesta de inventario de activos en la BVQ.

4.1.2.5. Propuesta de coordinación entre las gerencias y colaboradores.

Siguiendo con la propuesta de mejoras, se puede indicar que la gestión de la información es un proceso crítico en cualquier organización, y su importancia es aún mayor en la BVQ, donde se maneja información financiera sensible y confidencial. Para garantizar la seguridad y disponibilidad de esta información, es necesario establecer un sistema de coordinación entre las gerencias y colaboradores, con el fin de adoptar las mejores prácticas propuestas y asegurarse de que se implementen de manera adecuada en la gestión y administración de la información en la BVQ.

Este sistema de coordinación debe incluir la definición de roles y responsabilidades claras para cada área y colaborador involucrado en la gestión de la información, así como la implementación de herramientas tecnológicas y la capacitación del personal encargado de la gestión de la información. En este sentido, se hace necesario establecer un plan de acción que permita la implementación efectiva de las prácticas propuestas como se observa en la Tabla 42, asegurando la adecuada gestión y protección de la información crítica de la BVQ.

Tabla 42

Propuesta de coordinación entre las gerencias y colaboradores

Estrategias	Actividades	Responsable	Objetivos
Realizar reuniones periódicas.	Establecer una agenda y un cronograma para las reuniones periódicas de coordinación entre las gerencias y colaboradores.	Coordinador de la gestión de información.	Garantizar la alineación de los objetivos y metas en cuanto a la gestión y administración de la información.
Implementar un sistema de seguimiento y monitoreo.	Diseñar un sistema que permita realizar seguimiento y monitoreo al proceso de implementación de las mejores prácticas propuestas.	Coordinador de la gestión de información.	Garantizar la efectividad de la implementación de las mejores prácticas propuestas.
Establecer un equipo de trabajo multidisciplinario.	Seleccionar a los miembros del equipo de trabajo y asignar las responsabilidades correspondientes.	Coordinador de la gestión de información.	Asegurar la participación de todas las áreas y departamentos de la BVQ en la implementación de las mejores prácticas propuestas.

Realizar capacitaciones.	Diseñar un plan de capacitación para los colaboradores de todas las áreas y departamentos de la BVQ.	Responsable de capacitaciones.	Asegurar que todos los colaboradores estén capacitados en cuanto a la gestión y administración de la información.
Definir métricas de seguimiento	Establecer las métricas de seguimiento para evaluar el éxito de la implementación de las mejores prácticas propuestas.	Coordinador de la gestión de información	Evaluar el éxito de la implementación de las mejores prácticas propuestas y tomar acciones de mejora en caso de ser necesario.

Nota: Esta tabla presenta la propuesta de coordinación entre las gerencias y colaboradores.

Es importante mencionar que estas estrategias deberán ser adaptadas a las necesidades y particularidades de la BVQ. Además, es importante que todas las estrategias estén integradas y trabajen de manera conjunta para asegurar una adecuada coordinación entre las gerencias y colaboradores en la implementación de las mejores prácticas propuestas.

4.1.2.6. Optimización de la infraestructura tecnológica existente.

Una infraestructura tecnológica adecuada es fundamental para garantizar la eficacia de los procesos de gestión de respaldos de información. Para lograr una optimización en la infraestructura existente, se debe llevar a cabo una evaluación detallada de las tecnologías utilizadas para la realización de los respaldos. La evaluación permitirá identificar oportunidades de mejora y definir estrategias que aseguren la calidad y eficacia del proceso de respaldo de información. A continuación, se presenta en la Tabla 43 la propuesta de evaluación de las tecnologías existentes para realizar los respaldos de información.

Tabla 43

Evaluación de las tecnologías existentes para la realización de los respaldos de información

Estrategia	Actividades	Responsable	Objetivos
1	Identificación de las tecnologías existentes para el respaldo de información.	Equipo de TI	Identificar todas las tecnologías y herramientas utilizadas para el respaldo de información.
2	Análisis de las funcionalidades y características de las tecnologías existentes.	Equipo de TI	Evaluar las funcionalidades y características de cada una de las tecnologías identificadas, con el fin de determinar su capacidad y limitaciones en cuanto al respaldo de información.
3	Evaluación de la compatibilidad de las tecnologías existentes con los sistemas y aplicaciones utilizados en la organización.	Equipo de TI	Verificar la compatibilidad de las tecnologías existentes con los sistemas y aplicaciones utilizados en la organización, para garantizar una

		integración adecuada y evitar problemas en el proceso de respaldo de información.
4	Análisis de la eficacia y eficiencia de las tecnologías existentes en la realización de los respaldos de información.	Equipo de TI Evaluar la eficacia y eficiencia de las tecnologías existentes en el proceso de respaldo de información, con el fin de identificar oportunidades de mejora y definir estrategias para optimizar el proceso.
5	Definición de un plan de mejora para la infraestructura tecnológica existente.	Equipo de TI Identificar las oportunidades de mejora y definir un plan de acción para optimizar la infraestructura tecnológica existente y garantizar la calidad y eficacia del proceso de respaldo de información.

Nota: Esta tabla presenta la evaluación de las tecnologías existentes para la realización de los respaldos de información.

4.1.2.7. Establecimiento de una propuesta de actualización de tecnología para mejorar la eficiencia del proceso de respaldo de información.

En un entorno empresarial en constante evolución, el uso de tecnologías obsoletas puede afectar negativamente la eficiencia y efectividad de los procesos. En el caso de la gestión de respaldo de información de la BVQ, el uso de tecnologías obsoletas puede ser una barrera para la optimización del proceso. Por lo tanto, es necesario establecer una propuesta de actualización de tecnología que permita mejorar la eficiencia del proceso de respaldo de información que se presenta en la Tabla 44.

Tabla 44

Propuesta de actualización de tecnología

Estrategia	Actividades	Responsable	Objetivos
Pruebas de concepto	Realizar pruebas de concepto de las tecnologías seleccionadas para evaluar su eficiencia y efectividad en el proceso de respaldo de información.	Equipo de TI	Evaluar la eficiencia y efectividad de las tecnologías seleccionadas.
Selección de tecnología	Seleccionar la tecnología más	Equipo de TI	Identificar la tecnología más

		adecuada para mejorar el proceso de respaldo de información.		adecuada para mejorar la eficiencia del proceso de respaldo de información.
Plan de implementación	de	Elaborar un plan de implementación para la nueva tecnología seleccionada.	Equipo de TI	Garantizar una implementación exitosa de la nueva tecnología.
Capacitación y entrenamiento	y	Capacitar y entrenar a los usuarios y administradores del nuevo sistema.	Equipo de TI	Garantizar el correcto uso y administración del nuevo sistema.
Monitoreo y Evaluación	y	Realizar monitoreo y evaluación constante del nuevo sistema para garantizar su eficiencia y efectividad en el proceso de respaldo de información.	Equipo de TI	Asegurar que el nuevo sistema cumpla con los objetivos establecidos y que el proceso de respaldo de información sea más eficiente y efectivo.

Nota: Esta tabla presenta la propuesta de actualización de tecnología.

4.1.3. Mecanismos de control

4.1.3.1. Propuestas de definición de roles y responsabilidades

En la BVQ, es fundamental garantizar la protección y gestión adecuada de la información. Para lograrlo, es necesario establecer mecanismos de control que permitan garantizar el cumplimiento de los procesos y procedimientos establecidos en la propuesta de mejora. Esta estrategia involucra la definición de roles y responsabilidades claros, la implementación de herramientas tecnológicas adecuadas y la capacitación del personal encargado de la gestión de la información. En la siguiente Tabla 45 se presentan algunas de las mejores prácticas que se pueden implementar en la BVQ para asegurar el cumplimiento de estos objetivos.

Tabla 45

Propuestas de definición de roles y responsabilidades

Estrategias	Descripción
Definición de roles y responsabilidades.	Es fundamental definir claramente los roles y responsabilidades de cada persona involucrada en la gestión de la información en la BVQ, desde los altos directivos hasta los empleados encargados de la implementación de los procesos y procedimientos. Esto permitirá una asignación clara de responsabilidades y una mayor eficiencia en la gestión de la información.
Implementación de herramientas tecnológicas.	Es importante contar con herramientas tecnológicas adecuadas para la gestión y administración de la información en la BVQ. Estas herramientas deben permitir la clasificación, almacenamiento y protección adecuada de la información crítica de la organización.
Capacitación del personal encargado	El personal encargado de la gestión y administración de la información debe recibir capacitación adecuada, sobre los procesos y procedimientos establecidos en la propuesta de

de la gestión de la información.	mejora, así como en el uso de las herramientas tecnológicas para la gestión de la información. Esto permitirá una mejor implementación de los procesos y procedimientos y una mayor eficiencia en la gestión de la información.
Auditorías internas.	Es importante realizar auditorías internas periódicas para evaluar el cumplimiento de los procesos y procedimientos establecidos en la propuesta de mejora. Esto permitirá detectar posibles desviaciones y tomar medidas correctivas oportunamente.
Evaluación de proveedores.	Es importante evaluar regularmente a los proveedores de servicios y herramientas tecnológicas utilizados en la gestión y administración de la información en la BVQ. Esto permitirá asegurarse de que cumplen con los estándares de seguridad y calidad necesarios para proteger la información crítica de la organización.

Nota: Esta tabla presenta la propuestas de definición de roles y responsabilidades.

4.1.3.2. Propuestas de controles.

Adicionalmente, es fundamental establecer mecanismos de control que garanticen la integridad y disponibilidad de la información. En el caso específico de la BVQ, resulta indispensable contar con mecanismos que permitan controlar los respaldos de información, garantizando su recuperación en caso de pérdida o daño de la información original. Para tal fin, se pueden utilizar diversas estrategias y herramientas de control que permitan asegurar la efectividad de los procesos de gestión de respaldos. En la siguiente Tabla 46 se presentan algunas de las principales estrategias de control que se pueden implementar, así como los responsables, objetivos y tiempo estimado para su implementación.

Tabla 46*Propuestas de controles*

Mecanismo de control	Tiempo estimado	Responsable	Objetivo
Realizar pruebas de recuperación ante desastres de forma periódica.	Anualmente.	Equipo de Seguridad Informática.	Verificar la efectividad de los procedimientos de recuperación de la información en caso de eventos catastróficos.
Mantener registros detallados de las copias de seguridad realizadas.	Diariamente.	Equipo de Gestión de Respaldos.	Garantizar la disponibilidad y localización de las copias de seguridad.
Establecer políticas de retención de respaldos y eliminación de datos obsoletos.	Trimestralmente.	Equipo de Gestión de Respaldos.	Reducir el riesgo de pérdida de información por exceso de almacenamiento o eliminación inadecuada.
Utilizar técnicas de encriptación para la protección de los datos de respaldo.	Continuamente.	Equipo de Seguridad Informática.	Proteger la información sensible contenida en los respaldos de información.
Realizar auditorías internas y externas para evaluar la eficacia de los controles implementados.	Anualmente.	Equipo de Auditoría Interna / Externa.	Evaluar la eficacia de los controles implementados y detectar posibles deficiencias en la gestión de respaldos.
Establecer procedimientos de autorización para la restauración de	Continuamente.	Equipo de Gestión de Respaldos.	Garantizar la integridad de los datos y evitar la restauración no autorizada de información.

información a partir de respaldos.

Nota: Esta tabla presenta la propuestas de controles.

4.1.3.3. Indicadores de crecimiento y gestión de espacio de almacenamiento de los respaldos de información de la BVQ.

En el marco de la gestión de tecnologías de la información, resulta fundamental contar con herramientas que permitan monitorear el desempeño de los sistemas y aplicaciones críticas. En este sentido, la herramienta PRTG Network Monitor se presenta como una alternativa viable para mejorar la gestión de respaldos de información en la BVQ, ya que la implementación de esta herramienta permitirá monitorear de manera efectiva el estado de los respaldos, lo que facilitará detectar y resolver cualquier incidencia de manera oportuna.

Asimismo, PRTG Network Monitor proporcionará un conjunto completo de informes y estadísticas, lo que permitirá a los responsables de la gestión de información obtener una visión clara y detallada de la situación de los respaldos en tiempo real. En el ANEXOS

Anexo 1, se presenta un ejemplo de cómo se puede monitorear el crecimiento de la base de datos a través de sensores de monitoreo de almacenamiento utilizando esta herramienta.

Asimismo, la gestión adecuada de la información es fundamental para la continuidad de cualquier organización. En el caso de la BVQ, es esencial tener un control riguroso sobre el crecimiento y estadísticas de la información almacenada en sus sistemas. Para esto, se han establecido indicadores de crecimiento y estadísticas que permitirán conocer la cantidad de información almacenada y su evolución a lo largo del tiempo. Además, se han definido alertas de control respecto al espacio y la

frecuencia de los respaldos de información. Es importante que estos indicadores y alertas sean monitoreados por un equipo de IT especializado, encargado de gestionar la información y asegurar su continuidad. A continuación, se presenta en la **Tabla 47** los indicadores propuestos.

Tabla 47

Indicadores de crecimiento y gestión de espacio de almacenamiento de los respaldos de información de la BVQ

Indicador	Descripción	Fórmula/Definición	Meta/Alerta
Crecimiento anual del volumen de datos.	Porcentaje de crecimiento anual del volumen de datos almacenados en la BVQ.	$\frac{(\text{Volumen actual} - \text{Volumen anterior})}{\text{Volumen anterior}} \times 100.$	Menor o igual al 20% de crecimiento anual.
Capacidad de almacenamiento disponible.	Porcentaje de capacidad de almacenamiento disponible en la BVQ.	$\frac{\text{Espacio disponible}}{\text{Espacio total}} \times 100.$	Mayor o igual al 20% de espacio disponible.
Frecuencia de backup.	Frecuencia con la que se realiza el backup de la información.	Días transcurridos entre dos backups consecutivos.	Realizar backups diarios.
Porcentaje de éxito en la recuperación de datos.	Porcentaje de éxito en la recuperación de datos en caso de incidentes.	$\frac{\text{Número de recuperaciones exitosas}}{\text{Número total de recuperaciones}} \times 100.$	Mayor o igual al 95% de éxito en recuperaciones.
Tiempo de recuperación de datos.	Tiempo promedio para recuperar datos en caso de incidentes.	Tiempo transcurrido desde la detección del incidente hasta la recuperación de los datos.	Menor o igual a 24 horas de tiempo de recuperación
Espacio ocupado por los backups.	Porcentaje de espacio ocupado por los backups en relación al	$\frac{\text{Espacio ocupado por backups}}{\text{Espacio total}} \times 100.$	Menor o igual al 50% de espacio

	espacio total de almacenamiento.	de de almacenamiento) x ocupado por backups.	100.	
Alerta de espacio disponible para backups.	Alerta de espacio disponible para backups en la BVQ.	Cuando el espacio disponible para backups es menor al 20% del espacio total de almacenamiento.	Realizar backup inmediato y aumentar el espacio de almacenamiento.	
Alerta de frecuencia de backup no cumplida.	Alerta de frecuencia de backup no cumplida en la BVQ.	Cuando la frecuencia de backup es mayor a 24 horas.	Realizar backup inmediato.	
Alerta de fallas en recuperación de datos.	Alerta de fallas en recuperación de datos en la BVQ.	Cuando el porcentaje de éxito en la recuperación de datos es menor al 95%.	Revisar procedimientos de backup y recuperación de datos.	
Alerta de tiempo de recuperación de datos excedido.	Alerta de tiempo de recuperación de datos excedido en la BVQ.	Cuando el tiempo de recuperación de datos es mayor a 24 horas.	Revisar procedimientos de backup y recuperación de datos.	
Alerta de espacio ocupado por los backups excedido.	Alerta de espacio ocupado por los backups excedido en relación al espacio total de almacenamiento.	Cuando el porcentaje de espacio ocupado por los backups es mayor al 50%.	Aumentar el espacio de almacenamiento.	

Nota: Esta tabla presenta los indicadores de crecimiento y gestión de espacio de almacenamiento de los respaldos de información de la BVQ.

En general, con la implementación de los mecanismos de control propuestos se puede generar una serie de valores esperados en la gestión de respaldos de información en la BVQ. Entre ellos, se puede destacar una mejora en la eficiencia y efectividad de la gestión de respaldos, lo que permitiría una mayor seguridad y

confidencialidad de la información, así como una reducción en el riesgo de pérdida de datos y tiempos de inactividad. Además, la aplicación de estos mecanismos puede proporcionar una mayor transparencia y responsabilidad en la gestión de la información, y una mejor capacidad para cumplir con los requisitos reglamentarios y normativos relacionados con la gestión de la información. En definitiva, se espera que la implementación de estos mecanismos de control pueda contribuir significativamente a la mejora continua de la gestión de respaldos de información en la BVQ.

4.1.3.4. Establecimiento del plan de acción

Para asegurar el éxito de la propuesta de mejora en la gestión de respaldo de información propuesta, es necesario establecer un equipo de proyecto encargado de determinar la relación beneficio-costos y costo-efectividad de la propuesta. Este equipo deberá contar con la participación de expertos en tecnología, finanzas y gestión de proyectos.

Las responsabilidades de este equipo de proyecto incluirán la evaluación de los costos y beneficios de la propuesta, la comparación de los indicadores de la situación antes y después de la implementación de la mejora, y la identificación de posibles desviaciones. Además, deberán proponer medidas correctivas y actualizar regularmente el plan de acción para garantizar el éxito del proyecto.

Es fundamental que el equipo de proyecto cuente con los recursos necesarios para llevar a cabo sus tareas de manera efectiva, así como con el apoyo de la alta dirección y la colaboración de todas las áreas involucradas en la gestión de respaldo de información.

A continuación, para establecer un plan de acción para determinar la relación beneficio-costos y costo-efectividad de la propuesta de mejora se presentan las siguientes estrategias de la Tabla 48.

Tabla 48

Propuesta de estrategias de análisis de costo beneficios.

Estrategia	Actividades	Responsable	Objetivos
Análisis de costos	Identificar los costos asociados a la implementación de la actualización de tecnología propuesta.	Equipo de proyecto	Determinar el costo total de la propuesta y su impacto en la estructura presupuestaria de la organización.
Análisis de beneficios	Identificar los beneficios que se lograrían con la implementación de la propuesta.	Equipo de proyecto	Establecer el valor monetario de los beneficios que se lograrían con la propuesta, así como su impacto en el proceso de respaldo de información.
Análisis costo-efectividad	Comparar el impacto de la propuesta con su costo en unidades distintas a las monetarias.	Equipo de proyecto	Determinar el impacto de la propuesta en unidades distintas a las monetarias, como por ejemplo en el tiempo de respuesta, calidad del servicio, entre otros.

Análisis de resultados	de Comparar los indicadores de la situación antes y después de la implementación de la propuesta.	Equipo de proyecto	Evaluar la efectividad de la propuesta y su impacto en la gestión de respaldo de información, a partir de los indicadores de la situación antes y después de la implementación.
------------------------	---	--------------------	---

Nota: Esta tabla presenta la propuesta de estrategias de análisis de costo beneficios.

Finalmente, las estrategias de análisis de costos, beneficios, costo-efectividad y resultados son fundamentales para determinar el valor monetario y no monetario de la propuesta, así como su impacto en el proceso de respaldo de información. Además, permiten comparar la situación antes y después de la implementación de la propuesta, lo que facilita la evaluación de la efectividad de la propuesta.

Es importante destacar que la implementación de la propuesta de mejora en la gestión de respaldo de información debe ser llevada a cabo de manera cuidadosa y planificada, con la participación de un equipo de proyecto y los asignados para esta tarea en particular y que además cuenten con los recursos necesarios para llevar a cabo las tareas de manera efectiva. Asimismo, es esencial que se cuente con el apoyo de la alta dirección y la colaboración de todas las áreas involucradas en la gestión de respaldo de información.

Conclusiones

Luego de realizar un diagnóstico detallado del estado actual de los procesos de manejo, administración y gestión de los respaldos de información en la BVQ, se identificaron diversos riesgos y vulnerabilidades en la gestión de la información crítica de la organización. Estos riesgos ponen en peligro la continuidad del negocio y pueden generar graves pérdidas financieras.

En respuesta a estos riesgos, se diseñó una propuesta de mejora que contempla la implementación de procesos y procedimientos estandarizados para el manejo, administración y gestión de los respaldos de información en la BVQ. La implementación de esta propuesta permitirá garantizar la seguridad y disponibilidad de la información crítica, así como reducir significativamente los riesgos y vulnerabilidades identificados.

Para garantizar el éxito de esta propuesta, se establecieron mecanismos de control que permitirán asegurar el cumplimiento de los procesos y procedimientos establecidos, incluyendo la definición de roles y responsabilidades, la implementación de herramientas tecnológicas y la capacitación del personal encargado de la gestión de la información.

Concluyendo, que la propuesta de mejora diseñada permitirá a la BVQ mejorar sustancialmente el manejo, administración y gestión de los respaldos de información, lo que garantizará la continuidad del negocio ante posibles incidentes o desastres. Esta propuesta está basada en las mejores prácticas y normas que representa un paso importante en la consolidación de la BVQ como una organización segura y confiable en el manejo de la información crítica.

Recomendaciones

Tras haber realizado un diagnóstico detallado del estado actual de la gestión de respaldos de información en la BVQ, y haber diseñado una propuesta de mejora con sus respectivos mecanismos de control, se presentan a continuación una serie de recomendaciones que tienen como objetivo contribuir a una gestión más eficiente y efectiva de la información en esta institución. Estas recomendaciones se basan en las mejores prácticas y están dirigidas, tanto a aspectos que se pueden seguir investigando sobre el tema, como a otras áreas en las que se puede seguir trabajando para garantizar la continuidad del negocio de la BVQ.

Se recomienda continuar mejorando la gestión de los respaldos de información, ya que la propuesta de mejora planteada en este trabajo puede ser objeto de seguimiento y evaluación continua para asegurar su efectividad y eficiencia en el tiempo. Es importante establecer un plan de acción concreto para implementar las directrices y procedimientos definidos en la propuesta de mejora, y realizar monitoreos periódicos para asegurar que se están cumpliendo. Asimismo, se sugiere realizar auditorías periódicas a la gestión de respaldos de información para verificar que se están cumpliendo con los procesos y procedimientos establecidos.

Se recomienda realizar una evaluación periódica de los riesgos y vulnerabilidades que pueden afectar a la gestión de los respaldos de información. Es importante actualizar y revisar regularmente las políticas y procedimientos establecidos en la propuesta de mejora para estar preparados ante posibles incidentes o desastres. La evaluación de riesgos y vulnerabilidades puede incluir la identificación de posibles escenarios de pérdida de información y la definición de planes de contingencia para minimizar los impactos en caso de que se materialicen.

Se sugiere implementar sistemas de gestión de la calidad y seguridad de la información, como ISO 27001, para asegurar que la gestión de los respaldos de información cumpla con los estándares y buenas prácticas internacionales. La implementación de estos sistemas permitirá establecer una cultura de seguridad de la información en la organización, garantizar la continuidad del negocio y mejorar la imagen y reputación de la BVQ.

Es importante fomentar la capacitación y conciencia en seguridad de la información en todos los colaboradores de la BVQ, para que comprendan la importancia de la gestión adecuada de los respaldos de información y conozcan los riesgos y vulnerabilidades asociados. La capacitación debe ser continua y adaptada a las necesidades específicas de cada área y colaborador.

Se sugiere establecer alianzas y colaboraciones con otras instituciones del sector financiero y bursátil, para compartir buenas prácticas y experiencias en la gestión de respaldos de información. Además, se pueden establecer mecanismos de colaboración para la gestión de incidentes de seguridad de la información y para la realización de evaluaciones conjuntas de riesgos y vulnerabilidades.

BIBLIOGRAFÍA

- Ahituv, N., Munro, M. C., & Wand, Y. (1981). The value of information in information analysis. *Information and Management*, 4(3), 143–150.
[https://doi.org/10.1016/0378-7206\(81\)90041-0](https://doi.org/10.1016/0378-7206(81)90041-0)
- Alnahari, W. (2021). Information Security Protection and Planning for: Continuity and Security. *Research Aquare*, 1–12.
https://www.researchgate.net/publication/349353081_Information_Security_Protection_and_Planning_for_Continuity_and_Security
- Arabnia, H., Jandieri, G., Solo, A., & Tinetti, F. (2019). *Foundations of Computer Science* (1st ed.). C. S. R. E. A.
- Blair, A. (2021). *Information: A Historical Companion* (P. Duguid, A.-S. Goeing, & A. Grafton (eds.)). Princeton University Press.
<https://doi.org/10.2307/J.CTV1PDRRBS>
- BVQ. (2023). *¿Tienes alguna pregunta?* Bolsa de Valores de Quito.
<https://www.bolsadequito.com/index.php/component/sppagebuilder/76-transformation-s-a>
- California Consumer Privacy Act. (2018). *California Privacy Protection Agency - California Consumer Privacy Act*.
https://cppa.ca.gov/regulations/pdf/cppa_act.pdf
- Chiavenato, I. (2006). *Introducción a la teoría general de la administración* (6th ed.). McGraw-Hill Interamericana.
[https://frrq.cvg.utn.edu.ar/pluginfile.php/15525/mod_resource/content/0/Chiavenato Idalberto. Introducción a la teoría general de la Administración.pdf](https://frrq.cvg.utn.edu.ar/pluginfile.php/15525/mod_resource/content/0/Chiavenato%20Idalberto.%20Introducci3n%20a%20la%20teor3a%20general%20de%20la%20Administraci3n.pdf)
- Czinkota, M. R., & Kotabe, M. (2001). *Administración de la mercadotecnia* (2nd ed.).

International Thomson Editores.

Elder, S., & Elder, J. (2019). *Faster Disaster Recovery: The Business Owner's Guide to Developing a Business Continuity Plan* (Samuel F. Elder & Jennifer H. Elder (eds.); Aicpa Series, Vol. 1). John Wiley & Sons, Incorporated.

Ferrell, O. C., Hirt, G., Ferrell, L., Ramos, L., Rodríguez, M., & Flores, M. (2010). *Introducción a los negocios en un mundo cambiante*. McGraw-Hill Interamericana.

García, M. (2019). *Información y tipos de información*.
http://ri.uaemex.mx/bitstream/handle/20.500.11799/108236/secme-16870_1.pdf?sequence=1

Gaspar, J. (2010). *El Plan De Continuidad De Negocio* (Vol. 66).
https://www.google.com.ec/books/edition/El_plan_de_continuidad_de_negocio/um1V2jADP78C?hl=es-419&gbpv=1&dq=El+plan+de+continuidad+de+negocio:+guía+práctica+para+su+elaboración&printsec=frontcover

Gupta, C., & Goyal K. (2020). *Computer Concepts and Management Information Systems* (1st ed.). Mercury Learning & Information.

Hayes, B., & Kotwica, K. (2018). Chapter 12 Backup and Recovery. In *Business Continuity* (Vol. 1, pp. 1–32).
[https://nscpolteksby.ac.id/ebook/files/Ebook/Computer_Engineering/EMC_Information_Storage_and_Management_\(2009\)/18_Chapter_12_-_Backup_and_Recovery.pdf](https://nscpolteksby.ac.id/ebook/files/Ebook/Computer_Engineering/EMC_Information_Storage_and_Management_(2009)/18_Chapter_12_-_Backup_and_Recovery.pdf)

Henao, M. (2021). *Estandarización de procesos en la gestión de proyectos del departamento de planta física de la universidad EAFIT basados en la metodología Prince 2, PMI e integrada a los procesos BIM* [tesis de maestría, Universidad EAFIT]. <https://repository.eafit.edu.co/xmlui/bitstream/handle/10784/30875/TG->

Sabrina Molina-ESTANDARIZACIÓN DE PROCESOS EN LA GESTIÓN DE PROYECTOS DEF.pdf?sequence=2&isAllowed=y

IBM. (2023a). *Data Lifecycle Management*. <https://www.ibm.com/topics/data-lifecycle-management>

IBM. (2023b). *What Is Enterprise Content Management*. <https://www.ibm.com/topics/enterprise-content-management>

IBM. (2023c). *What is IT Management? | IBM*. <https://www.ibm.com/topics/it-management>

International Organization for Standardization. (2022). *ISO - ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. <https://www.iso.org/standard/82875.html>

ISACA. (2022). *COBIT | Control Objectives for Information Technologies*. <https://www.isaca.org/resources/cobit>

ITIL. (2022). *ITIL 4: Las mejores prácticas en Gestión de Servicios de TI*. <https://www.itil.com.mx/>

Kliem, R. L., & Richie, G. D. (2015). *Business continuity planning: a project management approach* (1st ed.). CRC Press. https://books.google.com/books/about/Business_Continuity_Planning.html?hl=es&id=fRVCrgEACAAJ

Ley 24. (2004). *Ley Orgánica de Transparencia y Acceso a la Información Pública*. https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cpccs_22_ley_org_tran_acc_inf_pub.pdf

Ley BOE-A-1968-444. (1968). *BOE-A-1968-444 Ley 9/1968, de 5 de abril, sobre secretos oficiales*. <https://www.boe.es/buscar/act.php?id=BOE-A-1968-444>

Lovatt, M. (2021). *Solution Architecture Foundations* (1st ed.). BCS Learning &

Development Limited.

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, 25(2), 419–441. <https://doi.org/10.1007/S11948-017-9992-1>

Moulos, V., Chatzikyriakos, G., Kassouras, V., Doulamis, A., Doulamis, N., Leventakis, G., Florakis, T., Varvarigou, T., Mitsokapas, E., Kioumourtzis, G., Klirodetis, P., Psychas, A., Marinakis, A., Sfetsos, T., Koniaris, A., Liapis, D., & Gatzoura, A. (2018). A robust information life cycle management framework for securing and governing critical infrastructure systems. *Inventions*, 3(4). <https://doi.org/10.3390/INVENTIONS3040071>

NIST. (2008). *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*. <https://doi.org/10.6028/NIST.SP.800-60v2r1>

Nyemba, C. (2018). *Right to Data Privacy in the Digital Era Critical Assessment of Malawi's Data Privacy Protection Regime HRDA, The Master's Programme in Human Rights and Democratisation in Africa* [Tesis de maestría, The LLM/MPhil in Human Rights and Democratisation in Africa (HRDA)]. <https://repository.gchumanrights.org/server/api/core/bitstreams/b81ef078-848d-4468-9f3d-076c88e1ed30/content>

Petrenko, S. (2021). *Developing an Enterprise Continuity Program* (1st ed.). River Publishers.

RAE. (2023). *información | Definición | Diccionario de la lengua española | RAE - ASALE*. <https://dle.rae.es/informaci%25C3%25B3n>

Romero, J. (2019). *Diseño del proyecto de digitalización del archivo histórico de la antigua academia de San Carlos* [Tesis de maestría, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC)].

https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/342/1/INFOTEC_MDETIC_JLRG_11102019.pdf

Room, S., Davis, S., Room, S., Niall O'Brien, M., Panagiotopoulos, A., Nahid, S., Hall, R., Thuraisingam, T., & Drury, J. (2021). *Data Protection and Compliance : Second edition* (2nd ed.). BCS Learning & Development Limited.

SAP. (2023). *SAP Information Lifecycle Management | Data Archiving and Retention*. <https://www.sap.com/products/technology-platform/information-lifecycle-management.html>

Smallwood, R. (2019). *Information Governance : Concepts, Strategies and Best Practices: Vol. Wiley CIO Series* (2nd ed.). John Wiley & Sons, Incorporated.

Toffler, A., & Toffler, H. (2006). *La revolución de la riqueza*. Descate.

Vega, E. (2021, March 9). Seguridad de la información. *Seguridad de La Información*, 1–113. <https://doi.org/10.17993/TICS.2021.4>

Villasana, L., Hernández, P., Ramírez, É., Villasana, L., Hernández, P., & Ramírez, É. (2021). La gestión del conocimiento, pasado, presente y futuro. Una revisión de la literatura. *Trascender, Contabilidad y Gestión*, 6(18), 53–78. <https://doi.org/10.36791/TCG.V0I18.128>

ANEXOS

Anexo 1

PRTG Network Monitor es una solución para monitorizar toda la infraestructura TI de una compañía, permitiendo tener una visión global del rendimiento y estado de tu red, asegurando que todos los componentes críticos de tu infraestructura IT que puedan afectar a tu negocio, estén disponibles 100%. Por ello, a través de esta herramienta se pueden implementar sensores (alertas) que indicaran el crecimiento de información en cada uno de los dispositivos de almacenamiento.



Sensores de monitoreo de almacenamiento

Procedimiento de verificación de crecimiento de BD y notificación para resolver las novedades presentadas.

Activo BD	Tamaño (KB) Nov 2022	Tamaño (KB) Dic 2022	Incremento (KB)	Incremento (%)	Estado
BW_Compliance	273,692	274,720	1,028	0.38%	Satisfactorio
dbcentral	15,719,452	15,938,716	219,264	1.39%	Alerta
Documentación	513,704	523,824	10,120	1.97%	Satisfactorio
efacturaonline	16,227,884	17,279,900	1,052,016	6.48%	Alerta
master	4,348	4,348	0	0.00%	Satisfactorio
Nomina	235,164	245,924	10,760	4.58%	Satisfactorio
ServiciosBVQ	1,364,904	1,370,792	5,888	0.43%	Satisfactorio
SICAV_BVQ	10,526,608	10,552,208	25,600	0.24%	Satisfactorio
SicavFG	6,733,528	6,761,244	27,716	0.41%	Satisfactorio
SicavSA	10,715,900	10,814,076	98,176	0.92%	Satisfactorio
sicavVGR	863,388	897,888	34,500	4.00%	Satisfactorio
slc	3,020,268	3,046,956	26,688	0.88%	Satisfactorio
TraderBVQ	1,730,960	1,873,748	142,788	8.25%	Satisfactorio

Verificación de crecimiento de BD

Anexo 2 Recopilación de información generada en la BVQ

Recopilación de Información Generada en la BVQ

La presente encuesta tiene por objetivo recopilar a detalle toda la información que es generada por cada uno de los funcionarios de acuerdo con las funciones y tareas que tiene asignadas, con el fin de dar recomendaciones específicas sobre el manejo, administración y gestión de los respaldos de información en la BVQ.

* Obligatoria

* Este formulario registrará su nombre, escriba su nombre.

1. Nombres y Apellidos

2. Departamento

3. ¿Usted conoce los medios de almacenamiento que se encuentran disponibles como son: OneDrive personal o SharePoint? *

SI

NO

4. ¿Qué tipos de archivos genera en función de sus actividades que realiza o le han asignado? *

Correo Electrónico

Excel

PDF

Word

XML

TXT

Imágenes

PowerPoint

5. ¿A qué sistemas tiene acceso para desempeñar sus funciones y tareas que le han asignado? *

- SLC
- SLC_BVG
- Documex
- SicavSA
- Insoft - Contabilidad
- Insoft - NIIF
- Insoft - Nómina
- GFondosNIIF
- Sicav VGR
- Sicav Fondo Garantía

6. ¿Con que frecuencia piensa que es necesaria respaldar su información generada? *

- Diaria
- Mensual
- Anual
- Bajo Demanda

7. ¿La información que usted genera en su área, es información confidencial? *

SI

NO

8. La información que usted genera en su área, es de tipo? *

Pública

Clasificada

9. ¿La información que usted genera de acuerdo con sus funciones y tareas asignadas la almacena en su equipo de trabajo? *

SI

NO

10. ¿La información que usted genera en su área la guarda con un formato establecido y nombres claros? *

SI

NO

11. ¿La información que usted genera en su área la guarda de una manera ordenada? *

SI

NO

12. ¿Usted conoce si se tiene establecida una política de respaldos, o recomendaciones para una gestión correcta de almacenamiento de información? *

SI

NO

Este contenido no está creado ni respaldado por Microsoft. Los datos que envíe se enviarán al propietario del formulario.

 Microsoft Forms

Anexo 3 Resultados de la información generada en la BVQ

Recopilación de Información Generada en la BVQ

28

Respuestas

02:50

Tiempo medio para finalizar

Activo

Estado

1. Nombres y Apellidos

28

Respuestas

Respuestas más recientes

"JOFFRE SEBASTIAN HERRERA YANEZ"

"JENNY EDITH RUIZ VINUEZA"

"PATRICIO JOSE VILLACIS GUILLEN"

2. Departamento

28

Respuestas

Respuestas más recientes

"OPERACIONES"

"SERVICIOS"

"TECNOLOGÍA"

7 encuestados (25%) respondieron **TECNOLOGÍA** para esta pregunta.

ESTADÍSTICAS AUDITORÍA MARK
ADMINISTRACIÓN **TECNOLOGÍA** LEG
HUMANO
FINANCIERO OPERACIONES COMERCIO

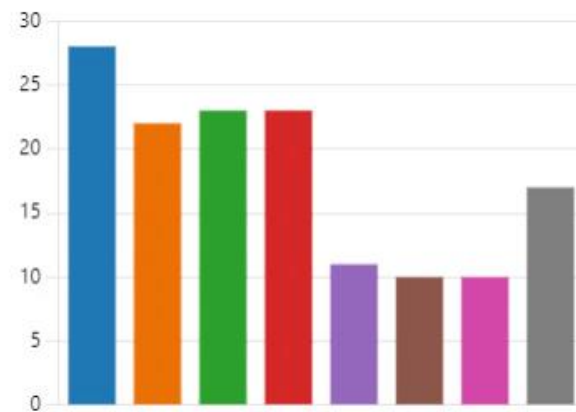
3. ¿Usted conoce los medios de almacenamiento que se encuentran disponibles como son: OneDrive personal o SharePoint?

● SI	17
● NO	11



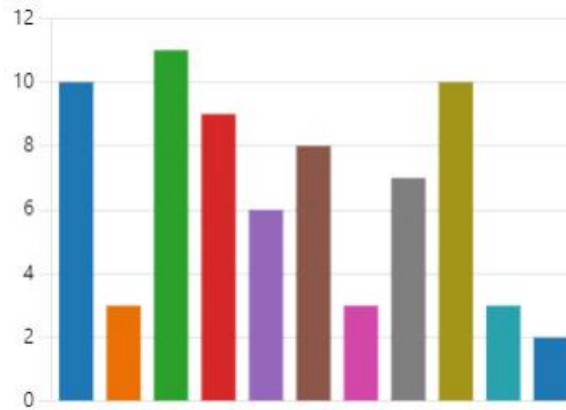
4. ¿Qué tipos de archivos genera en función de sus actividades que realiza o le han asignado?

● Correo Electrónico	28
● Excel	22
● PDF	23
● Word	23
● XML	11
● TXT	10
● Imágenes	10
● PowerPoint	17



5. ¿A qué sistemas tiene acceso para desempeñar sus funciones y tareas que le han asignado?

● SLC	10
● SLC_BVG	3
● Documex	11
● SicavSA	9
● Insoft - Contabilidad	6
● Insoft - NIIF	8
● Insoft - Nómina	3
● GFondosNIIF	7
● Sicav VGR	10
● Sicav Fondo Garantía	3
● N/A	2



6. ¿Con qué frecuencia piensa que es necesaria respaldar su información generada?

● Diaria	7
● Mensual	12
● Anual	14
● Bajo Demanda	0



7. ¿La información que usted genera en su área, es información confidencial?

● Si	9
● NO	19



8. La información que usted genera en su área, es de tipo?

● Pública	20
● Clasificada	8



9. ¿La información que usted genera de acuerdo con sus funciones y tareas asignadas la almacena en su equipo de trabajo?

● SI, la guardo en mi equipo	16
● NO, la almaceno sólo en la nube	10
● Otras	2



10. ¿La información que usted genera en su área la guarda con un formato establecido y nombres claros?

● SI	9
● NO	19



11. ¿La información que usted genera en su área la guarda de una manera ordenada?

● SI	11
● NO	17



12. ¿Usted conoce si se tiene establecida una política de respaldos, o recomendaciones para una gestión correcta de almacenamiento de información?

● SI	7
● NO	21



Encuesta Técnica (Analista Senior de Soporte y Seguridades TI)

La presente encuesta tiene el objetivo de conocer la realidad actual del manejo de respaldos de la institución, con el fin de analizar dicha información en este estudio y poder plantear recomendaciones sobre el manejo, administración y gestión de los respaldos de información en la BVQ.

* Este formulario registrará su nombre, escriba su nombre.



1. ¿Se realizan copias de seguridad de la información de la institución?

Si

No

2. ¿Identifique en que dispositivos se realizan las copias de seguridades?

3. ¿Guardamos toda la información crítica de nuestro negocio, así como información de apoyo de cada funcionario?

Si

No

4. ¿Qué información se almacena?

5. ¿Hasta cuánto tiempo atrás podemos recuperar datos?

6. ¿Cuánto tiempo tardamos en recuperar nuestros datos?

7. ¿Se Tiene documentado el proceso de respaldo y restauración?

8. ¿Se hacen test de recuperación de datos de las copias?

9. ¿Están cifradas las copias fuera de la empresa?

10. ¿Cuenta con dispositivos de redundancia para almacenamiento?

Este contenido no está creado ni respaldado por Microsoft. Los datos que envíe se enviarán al propietario del formulario.

 Microsoft Forms

Anexo 5 Resultados de la Encuesta técnica (Análisis Senior de Soporte y Seguridad TI)

Encuesta Técnica (Analista Senior de Soporte y Seguridades TI)

1

Respuestas

14:43

Tiempo medio para finalizar

Activo

Estado

1. ¿Se realizan copias de seguridad de la información de la institución?

- Si
- No

1

0



2. ¿Identifique en que dispositivos se realizan las copias de seguridades?

1

Respuestas

Respuestas más recientes

"Nube (OneDrive), Nube (SharePoint), Servidor (File Server), Discos Externos, PC Personales"

3. ¿Guardamos toda la información crítica de nuestro negocio, así como información de apoyo de cada funcionario?



4. ¿Qué información se almacena?

1
Respuestas

Respuestas más recientes

"Bases de Datos, Respaldos Bases de Datos, Aplicaciones, Información de funcionarios, Archivos de Correos Electrónicos"

5. ¿Hasta cuánto tiempo atrás podemos recuperar datos?

1
Respuestas

Respuestas más recientes

"Dependiendo del tipo del respaldo se puede recuperar Información hasta de 3 años atrás."

6. ¿Cuánto tiempo tardamos en recuperar nuestros datos?

0
Respuestas

Respuestas más recientes

7. ¿Se Tiene documentado el proceso de respaldo y restauración?

1
Respuestas

Respuestas más recientes

"Depende del tipo del respaldo, por ejemplo en el caso de archivos aproximadamente uno 15 minutos, al tratarse de bases de datos y dependiendo del tamaño aproximadamente 1 hora."

8. ¿Se hacen test de recuperación de datos de las copias?

1

Respuestas

Respuestas más recientes

"Si, pero únicamente de las bases de datos de forma mensual."

9. ¿Están cifradas las copias fuera de la empresa?

1

Respuestas

Respuestas más recientes

"En el caso de bases de datos, los respaldos se generan con una contraseña de seguridad."

10. ¿Cuenta con dispositivos de redundancia para almacenamiento?

1

Respuestas

Respuestas más recientes

"Se tiene considerado Implementarlos más adelante, por el momento solo los detallados en la pregunta 2."
