

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DEFINICIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RESPALDOS DE INFORMACIÓN CENTRALIZADO EN LA EMPRESA YAKINDU CIA. LTDA. EMPLEANDO HERRAMIENTAS DE SOFTWARE LIBRE

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

SORIA DE LA CRUZ PAUL ORLANDO

ospaul.cruz@hotmail.com

DIRECTOR: Ing. ENRIQUE ANDRES LARCO AMPUDIA, MSc.

andres.larco@epn.edu.ec

Quito, Enero 2016

DECLARACIÓN

Yo, Soria De la Cruz Paul Orlando, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Soria De la Cruz Paul Orlando

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por: Paúl Orlando Soria De la Cruz, bajo mi supervisión.

Ing. ENRIQUE ANDRES LARCO AMPUDIA, MSc.

DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios por ayudarme a perseverar para lograr cumplir un objetivo trazado hace mucho tiempo junto con la ayuda de mis padres, hermanos y amigos que forman parte en mi vida.

A mis Padres: Luis Soria y Rosa De la Cruz por su infinito amor y constante lucha para que no nos falte nada a mí y mis hermanos, por inculcarnos buenos valores éticos y morales para hacerme un hombre de bien.

A mis hermanos, Fredy, Luis y Daniel por estar siempre preocupados y pendientes, por brindarme su ayuda y apoyo constante.

DEDICATORIA

A Dios por su inmenso amor, A mi Mami, a mi Papi, a mis Hermanos que nunca han dejado de apoyarme.

Y a todos mis amigos.

PAÚL

CONTENIDO

1.	CAPÍTULO 1: DESCRIPCIÓN DEL PROBLEMA	1
1.1.	PLANTEAMIENTO DEL PROBLEMA	1
1.1.1.	SITUACIÓN ACTUAL DEL PROBLEMA	1
1.1.2.	DESCRIPCIÓN DEL PROBLEMA	1
1.1.3.	JUSTIFICACIÓN DEL PROBLEMA.....	2
1.2.	ANÁLISIS Y SELECCIÓN DE LA HERRAMIENTA A UTILIZAR	3
1.2.1.	FACTORES.....	3
1.2.2.	NECESIDADES.....	3
1.2.3.	CUADRO COMPARATIVO.....	4
1.2.4.	ANÁLISIS DE LA HERRAMIENTA:	11
1.3.	ANÁLISIS Y SELECCIÓN DE LA METODOLOGÍA DE TRABAJO	21
1.3.1.	MARCOS DE TRABAJO Y NORMAS MÁS USADAS	22
1.3.2.	METODOLOGIA DE TRABAJO	40
2.	CAPÍTULO 2: PLANIFICACIÓN Y ANÁLISIS DE REQUERIMIENTOS.....	43
2.1.	DEFINICIÓN DE UN MODELO DE RESPALDO DE DATOS	43
2.1.1.	IMPORTANCIA DE LA INFORMACIÓN	43
2.1.2.	PLAN DE RESPALDOS	43
2.1.3.	SELECCIÓN DE LA HERRAMIENTA DE AUTOMATIZACIÓN.....	45
2.1.4.	TIPOS DE RESPALDOS	45
2.1.5.	MEDIOS DE ALMACENAMIENTO A UTILIZAR.....	47
2.1.6.	PLANIFICACION DE RESPALDOS	48
2.1.7.	RESTAURACIÓN DE DATOS.....	49
2.1.8.	POLÍTICAS DE RESPALDOS	50
2.1.9.	PLAN DE CONTINGENCIA.....	52
2.2.	DEFINICIÓN DE UN MODELO DE ARQUITECTURA DE INFORMACIÓN	53
2.2.1.	RECOPIACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN	53
2.2.2.	PROCESAMIENTO DE INFORMACIÓN.....	54

2.2.3.	ANÁLISIS DE LA INFORMACIÓN.....	55
2.2.4.	PRESENTACIÓN Y UTILIZACIÓN DE LA INFORMACIÓN.....	55
2.2.5.	RIESGOS EN SISTEMAS DE INFORMACIÓN.....	55
3.	CAPITULO 3: IMPLEMENTACIÓN DEL PROTOTIPO EN EL CASO DE ESTUDIO	58
3.1.	DESCRIPCIÓN DEL CASO DE ESTUDIO.....	58
3.1.1.	DESCRIPCIÓN DE LA COMPAÑÍA “YAKINDU CIA. LTDA”.....	58
3.1.2.	ESTRUCTURA ORGANIZATIVA.....	58
3.1.3.	SERVICIOS.....	59
3.1.4.	TOPOLOGÍA DEL SISTEMA.....	60
3.1.5.	SITUACIÓN ACTUAL DE TI DEL CASO DE ESTUDIO.....	60
3.2.	POLÍTICAS DE RESPALDO DE INFORMACIÓN	62
3.2.1.	OBJETIVOS GENERALES.....	62
3.2.2.	OBJETIVOS ESPECÍFICOS	62
3.2.3.	DESARROLLO DEL MODELO DE PLAN DE RESPALDOS.....	62
3.2.4.	POLITICAS DE RESPALDOS.....	81
3.2.5.	PLAN DE CONTINGENCIA.....	83
3.3.	INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR.....	88
3.3.1.	PASO 1: INSTALACIÓN DEL SISTEMA OPERATIVO	88
3.3.2.	PASO 2: INSTALACIÓN DEL SERVIDOR BACULA.....	88
3.3.3.	PASO 3: CONFIGURACIÓN BACULA.....	90
3.3.4.	PASO 4: INSTALACIÓN Y CONFIGURACIÓN DE BACULA WEBMIN	91
3.4.	INSTALACIÓN Y CONFIGURACIÓN DE LOS CLIENTES	94
3.4.1.	INSTALACIÓN Y CONFIGURACIÓN DE UN CLIENTE LINUX	94
3.4.2.	INSTALACIÓN Y CONFIGURACIÓN DE UN CLIENTE WINDOWS.....	96
3.5.	CONFIGURACIÓN DE TAREAS PROGRAMADAS	98
3.6.	PRUEBAS	98
3.7.	ANÁLISIS DE RESULTADOS.....	104
3.7.1.	SITUACIÓN SIN LA APLICACIÓN DEL MODELO.....	104
3.7.2.	SITUACIÓN CON LA APLICACIÓN DEL MODELO.....	104

3.7.3.	EVALUACIÓN	106
4.	CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES	
	116	
4.1.	CONCLUSIONES	116
4.2.	RECOMENDACIONES.....	118
5.	Bibliografía	119

ÍNDICE DE FIGURAS

Figura 1-1 Arquitectura de Bacula.....	12
Figura 1-2 Principios de COBIT 5.....	24
Figura 1-3 Habilitadores de COBIT 5	25
Figura 1-4 Tres dimensiones críticas para el negocio	28
Figura 1-5 Modelo PDCA aplicado a los procesos SGSI	34
Figura 1-6 Ciclo de Vida ITIL.....	37
Figura 1-7 Ciclo Deming.....	40
Figura 3-1 Estructura Organizativa.....	58
Figura 3-2 Topología del Sistema.....	60
Figura 3-3 Lineamiento COBIT 5 para gestión de respaldos	76
Figura 3-4 Matriz RACI del Catalizador DSS04 Entregar, dar Servicio y Soporte	76
Figura 3-5 Directorio de Restauración de Archivos	81
Figura 3-6 Instalación servidor Bacula	88
Figura 3-7 Configuración Mysql.....	88
Figura 3-8 Contraseña Mysql	89
Figura 3-9 Instalación de herramientas Bacula	89
Figura 3-10 Privilegios Mysql	89
Figura 3-11 Creación Base de datos.....	90
Figura 3-12 Creación de tablas en Base de datos	90
Figura 3-13 Privilegios elementos de Bacula	90
Figura 3-14 Archivos configuración de Bacula	91
Figura 3-15 Descarga paquete Webmin.....	91
Figura 3-16 Instalación paquete Webmin.....	92
Figura 3-17 Iniciar servicio Webmin	92
Figura 3-18 Activar servicio Webmin.....	92
Figura 3-19 Portal Webmin Ingreso.....	93
Figura 3-20 Portal Webmin.....	93
Figura 3-21 Inicio Portal Webmin	93
Figura 3-22 Configuración Base de datos	94
Figura 3-23 Elementos Bacula	94

Figura 3-24 Instalación Cliente Bacula	95
Figura 3-25 Configuración Cliente Bacula	95
Figura 3-26 Configuración de consola Cliente Bacula	95
Figura 3-27 Instalación Cliente Bacula Windows	96
Figura 3-28 Escoge Elementos Cliente Bacula Windows	96
Figura 3-29 Configura datos servidor Bacula	97
Figura 3-30 Configura nombre del cliente Bacula	97
Figura 3-31 Respaldo de servidores	98
Figura 3-32 Solicitud de restauración httpdold	99
Figura 3-33 Solicitud de restauración svn	100
Figura 3-34 Tipo de restauración	101
Figura 3-35 Cliente a restaurar	101
Figura 3-36 Restauración de cliente httpdold	102
Figura 3-37 Restauración de cliente svn	103
Figura 3-38 Archivos restaurados	103

ÍNDICE DE TABLAS

Tabla 1-1 Soluciones de respaldos modificado por el Autor	9
Tabla 1-2 Áreas de proceso, categorías y niveles de madurez CMMI Model Foundation	31
Tabla 1-3 Áreas de proceso, categorías y niveles de madurez CMMI-DEV.....	32
Tabla 3-1 Tamaño de Servidor de Base de Datos	64
Tabla 3-2 Tamaño de Servidor de Aplicaciones.....	64
Tabla 3-3 Tamaño de Servidor de SVN	65
Tabla 3-4 Datos de Servidor de Base de Datos	65
Tabla 3-5 Datos de Servidor de Aplicaciones.....	65
Tabla 3-6 Datos de Servidor SVN	65
Tabla 3-7 Crecimiento de la Información de Servidores.....	66
Tabla 3-8 Presentación y utilización de la información.....	68
Tabla 3-9 Mapeo de los objetivos del negocio con las metas corporativas de COBIT 5	69
Tabla 3-10 Mapeo de las metas corporativas de COBIT 5 y las metas relacionadas con las TI.....	70
Tabla 3-11 Mapeo entre las metas relacionadas con las TI con los procesos de COBIT 5	72
Tabla 3-12 Mapeo de Procesos de COBIT 5 con riesgos identificados	73
Tabla 3-13 Roles del proceso DSS04	77
Tabla 3-14 Carga operacional del servidor de virtualización	79
Tabla 3-15 Planificación de Respaldos	80
Tabla 3-16 Cumplimiento de los objetivos de TI.....	105
Tabla 3-17 Evaluación del proceso sin la implementación del modelo	107
Tabla 3-18 Matriz de resultados de evaluación sin el modelo implementado	108
Tabla 3-19 Evaluación del proceso con la implementación del modelo	113
Tabla 3-20 Matriz de resultados de evaluación con el modelo implementado ...	114
Tabla 3-21 Eficiencia de la solución de respaldos.....	115

RESUMEN

El presente proyecto de titulación consiste en Implementar un Sistema de Gestión de Respaldos de Información para la empresa Yakindu Cia. Ltda. para la cual se respaldará información de los sistemas, aplicaciones, programas, bases de datos, directorios y archivos almacenados en los servidores, contando de esta manera con mecanismos que ayuden a garantizar la disponibilidad de la información ante un problema, desastre o pérdida de información y realizar una recuperación confiable. En el Capítulo 1 se realiza el planteamiento del problema: la situación actual del problema, la descripción y una justificación del problema. Se hace un análisis y selección de la herramienta de respaldos a utilizar. Se analizan varios marcos de trabajo para de esta manera seguir una metodología de trabajo ya que no hay una metodología formal para respaldos de información que se adapte a las necesidades de la empresa.

En el Capítulo 2 se define el modelo de arquitectura de información que determina la información a respaldarse como los riesgos de la empresa y define un modelo de respaldo de datos que permite planificar los respaldos de información en los medios establecidos así como establece las políticas de respaldos y su plan de contingencia.

En el Capítulo 3 se realiza una descripción completa del caso de estudio para conocer la situación actual de los respaldos y los procesos que manejan, se analiza la información a respaldar y planifica los respaldos luego instala y configura el servidor y los nodos determinados, que depende de los resultados dados por el desarrollo del modelo de respaldos, también se realizan pruebas de restauración de la información generada por los respaldos, para verificar que los procedimientos aplicados a la obtención de respaldos estén siendo usados de la manera correcta.

En el Capítulo 4 están las conclusiones y recomendaciones del presente proyecto de titulación.

PRESENTACIÓN

Actualmente la empresa caso de estudio no cuenta con una gestión de respaldo de datos, se realiza respaldos manuales a cargo del jefe técnico en horarios no definidos y no cuenta con una organización de sus datos que en caso de pérdidas de información compromete datos confidenciales o genera pérdidas de dinero.

Se plantea como solución implementar el modelo propuesto en este documento que consta de 2 fases:

1. Primera fase de planificación y análisis de requerimientos en la que se define el modelo de gestión de respaldos con uso de un marco de trabajo que provee un conjunto de mejores prácticas de TI.
2. Segunda fase de implementación de la solución de respaldos con el uso de la herramienta Bacula para salvaguardar la información de la empresa de una manera automatizada, centralizada y compatible con sus productos actuales de TI

Con la solución en funcionamiento se obtuvo como resultado un sistema automatizado de gestión de respaldos confiable y seguro que permite al responsable no afectar la carga operacional y disponibilidad de los recursos de la empresa mejorando así su rendimiento y tiempo de respuesta, dejando abierta una ventana de actualización para mejora ya que ningún modelo es único.

CAPÍTULO 1: DESCRIPCIÓN DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

1.1.1. SITUACIÓN ACTUAL DEL PROBLEMA

Actualmente la evolución de las empresas de Desarrollo de Software en el mercado han llevado a las organizaciones a prepararse con medios y herramientas de gran importancia para justificar y cumplir todas las demandas y necesidades de sus clientes, por lo cual la información generada día a día es cada vez más importante para sus negocios, al mismo tiempo, surgen nuevas amenazas y distintas formas de ataques que pueden ser generadas por delincuentes cibernéticos, también por causas relacionadas con el factor humano y tecnológico que no le dan la suficiente importancia a los riesgos que se pueden presentar, por lo cual la gestión de riesgos es un tema muy importante para la administración de la información. Por tanto, las empresas han venido desarrollando y planificando el manejo a priori de su información y así preparándose para enfrentar cualquier riesgo que se pueda presentar.

1.1.2. DESCRIPCIÓN DEL PROBLEMA

En la actualidad la información es el activo más importante de una empresa, de modo que la pérdida supone un alto riesgo para la continuidad del negocio.

Las empresas no cuentan con un sistema de respaldos optimizado y en el caso de tener alguno en muchas de las ocasiones no está implementado de forma correcta, puesto que para lograrlo debe existir un análisis previo que esté basado en la necesidad particular de la situación de la empresa y de esta manera poder realizar la tarea de respaldo periódico.

Las empresas han sido expuestas a varios riesgos como:

- La falta de controles de acceso a instalaciones físicas, aplicativos y equipos.

- Incumplimiento de normas y procedimientos relacionados a la seguridad de la información.
- Ausencia de respaldos de la información, códigos fuentes y bases de datos de trabajo.
- Falta de cuidado en la custodia de activos por el responsable asignado o personal a cargo de la seguridad.
- Falta de controles a nivel de equipos, tales como ubicación y protección, seguridad en cableado o mantenimiento periódico de equipos.
- Falta de Gestión de control de cambios ante la implementación de nuevas tecnologías.
- Falta de Definición de políticas de seguridad que permitan controlar la integridad, disponibilidad y confiabilidad de la información.

1.1.3. JUSTIFICACIÓN DEL PROBLEMA

El crecimiento exponencial de la información en las empresas en los tiempos actuales, permiten la llegada de nuevos sistemas de información la cual es crítica y debe estar respaldada de manera eficaz y eficiente, así como el requisito legal de mantener la información histórica por varios años lo que hace que la implementación de un modelo de respaldos de información sea imprescindible.

El presente proyecto consiste en implementar un modelo de respaldos y recuperación de la información para las empresas que manejan información sensible y delicada de sus clientes la cual necesita estar protegida y disponible en caso de algún inconveniente. Ya que la empresa no cuenta con un modelo de respaldos el proyecto propone un completo estudio de las necesidades de la empresa con el fin de plantear la correcta metodología y procedimientos del modelo de respaldos que aplican a la empresa de una manera automatizada para evitar la pérdida de información importante y que de la misma manera se encuentre protegida, para lo cual la propuesta contempla la implementación de un sistema de respaldo con tecnología de código abierto para que se realice los procesos de una

forma automatizada que garantice la disponibilidad y seguridad de la información así como la continuidad del negocio.

1.2. ANÁLISIS Y SELECCIÓN DE LA HERRAMIENTA A UTILIZAR

La implementación de una herramienta automatizada de respaldos genera beneficios de orden administrativo, operativo y económico. Con esto se busca brindar una guía básica para que los profesionales de TI puedan en su momento justificar la implementación de una herramienta de este tipo.

Para elegir una herramienta de sistema de respaldo de datos es importante identificar la más adecuada de acuerdo a las necesidades del negocio.

1.2.1. FACTORES

Los factores que impulsan la necesidad de respaldar información son:

- Aspectos del crecimiento de información y la presión resultante en los procesos de “Respaldos”.
- Tecnologías para realización de “Respaldos” actuales y su implementación.
- Beneficios de implementar “Respaldos” y su impacto positivo en el negocio.
- Factores que determinan la eficiencia de un “Respaldo”.
- Consideraciones específicas de “Respaldos” en disco.

1.2.2. NECESIDADES

Las principales necesidades organizacionales son:

1. Disponibilidad de información cuando es necesario y por los medios adecuados, suministro de información de manera selectiva.
2. Variedad en la forma de presentación de la información.
3. Grado de inteligencia incorporado al sistema.
4. Tiempo de respuesta del sistema.
5. Exactitud de la información.

6. Flexibilidad en capacidad de adaptación.
7. Fiabilidad para que el sistema opere correctamente.
8. Seguridad protección contra pérdidas.
9. Reserva nivel de repetición del sistema para evitar pérdidas.
10. Usabilidad para el usuario.
11. Costos

1.2.3. CUADRO COMPARATIVO

En la actualidad existen una gran variedad de soluciones de copias de seguridad por lo cual en la Tabla 1.1 se muestra una comparativa de las herramientas a seleccionarse de acuerdo a la conveniencia o necesidad de la empresa que la planee implementar.

	Bacula	Amanda	Tivoli (TSM)	Veritas	Legato Networker	CA ARCserve	Arkeia Network Backup	Quest NetVault: Backup	LBackup
Niveles de Respaldos	Full, Diferencial, Incremental, Consolidación	Full, Incremental	Full, Incremental	Full, Diferencial, Incremental	Full, Diferencial, Incremental, Consolidación	Full, Full Sintético, Diferencial, Incremental, Nivel Incremental de Bloque Infinito	Full, Diferencial, Incremental	Full, Diferencial, Incremental	Full, Incremental
Formato de Datos	Personalizado, Libre	Libre, Recuperable sin Amanda	Personalizado	Personalizado	Personalizado	Personalizado, Formato de Cintas Microsoft (MTF)	Personalizado, Restauración de Código Abierto	Personalizado	Personalizado, Libre
Auto-cambiadores	Soportado	Soportado	Soportado	N/A	Opcional	Soportado	Soportado	Soportado	No Soportado

De duplicación	Lado de destino	N/A	Lado de destino	Ambos lados	N/A	Variable global del bloque de duplicación, Lado de destino	Ambos lados	Lado de destino	N/A
NDMP	Si	Si	Si	Si	Si	Si	Si	Si	No
Respaldo a cinta	Si	Si	Si	Si	Si	Si	Si	Si	No
Respaldo a Disco	Si	Si	Si	Si	Opcional	Si	Si	Opcional	Si
Respaldo a DVD	Si	Si	No	N/A	No	N/A	No	No	No
Puesta en Etapas	Si	Si	Si	Si	Si	Si	Si	N/A	N/A
Catalogo SQL	Si	No	Si	No	N/A	Si	No	No	No
Puede gestionar 1 billón de objetos	Si	Si	Si	N/A	N/A	Si	Si	N/A	Depende del Sistema de Archivos

Abarca Múltiples Volúmenes de Respaldos	Si	Si	N/A	Si	Si	Si	Si	Si	Si	N/A	No
Soporte de Microsoft Exchange	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
Reporte de Respaldos	Si	Si	N/A	Si	Si	N/A	Si	Si	Si	Si	Si
Alertas de Respaldos (Notificación)	Si	Si	N/A	Si	Si	N/A	Si	Si	Si	Si	Si
Manejo incremental de archivos borrados	Si	Si	Si	N/A	N/A	N/A	Si	Si	Si	N/A	Si
Encriptación del Flujo de Datos	Si	Si	N/A	Si	Si	N/A	Si	Si	Si	N/A	Si

SopORTE MSSQL	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
SopORTE Oracle	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
SopORTE PostgreSQL	Si	N/A	N/A	N/A	N/A	N/A	N/A	No	N/A	N/A	N/A	N/A	N/A
SopORTE Almacenamiento de Máquinas Virtuales	Si	N/A	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	N/A
Certificado de Seguridad	N/A	Si	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	No

Tabla 1-1 Soluciones de respaldos modificado por el Autor¹

¹ <http://wiki.bacula.org/doku.php?id=comparisons>

En el mercado informático existen diversas soluciones para intentar resolver problemas de respaldo de información, como los mostrados en el cuadro comparativo, los cuales son los más conocidos y usados actualmente, que permitirá que el proyecto sea ejecutado de una manera adecuada y segura.

Hay que reconocer que existe una amplia gama de plataformas para realizar los respaldos y cada empresa buscando la mejora de su negocio implementan productos de alta calidad que no generen altas inversiones, para ello las herramientas de código abierto son la mejor opción que podrán solventar las necesidades de las empresas así como proyectarse para su continuo desarrollo y crecimiento, por cual motivo se excluirán las soluciones licenciadas como TSM que aunque es una excelente herramienta usada por muchas empresas y corporaciones no podría ser solventada por las pequeñas y medianas empresas por sus costos de licenciamiento.

Las soluciones de código abierto mostradas en el cuadro comparativo son: LBackup, Amanda y Bacula, las cuales cuentan con un soporte comercial en caso de requerirlo.

Entre estas herramientas que tienen características similares una de las más importantes es el soporte de almacenamiento de máquinas virtuales ya que en la actualidad la virtualización es usada en toda empresa.

El soporte a postgresSQL, postgres es un gestor de bases de datos de código abierto usado por cualquier entidad por ejemplo el sector público.

Otra característica importante a tomar en cuenta es la de duplicación para no tener datos repetidos y desperdicio de espacio.

Revisando estas características que diferencian a estas herramientas la mejor opción para este proyecto es Bacula ya que soporta las características mencionadas y el cual va a permitir automatizar las tareas de respaldo.

Esta herramienta permite la administración y efectuar respaldos, recuperación de información a través de la red, siendo este multiplataforma.

La importancia de la implementación de este proyecto radica en el ámbito administrativo, operativo y económico. En el ámbito administrativo facilita la creación de una planificación de los respaldos diarios, semanales, mensuales y anuales, así como las políticas de respaldo y tiempo de vida del mismo.

En un ámbito operativo la interacción del personal de operaciones con el sistema de respaldo será para verificar que la planificación de dichos respaldos se haya finalizado correctamente y la correspondiente toma acción en caso de existir fallas durante la ejecución.

Bacula es una alternativa popular, gratuita y de código abierto, requiere instalar programas cliente en cada máquina objeto de respaldo, todos los cuales se controlan a través de un servidor que maneja centralmente las reglas de respaldos.

1.2.4. ANÁLISIS DE LA HERRAMIENTA:

Bacula es una solución de respaldos distribuida, multiplataforma y Open Source que permite administrar los respaldos realizados así como restaurar y verificar los datos en una red heterogénea. Bacula se basa en una arquitectura Cliente-Servidor que es muy eficiente y resulta fácil de usar, a la vez que ofrece muchas funcionalidades avanzadas para la administración de los datos almacenados, lo cual facilita encontrar y recuperar archivos perdidos o dañados.

1.2.4.1. ARQUITECTURA Y COMPONENTES DE BACULA

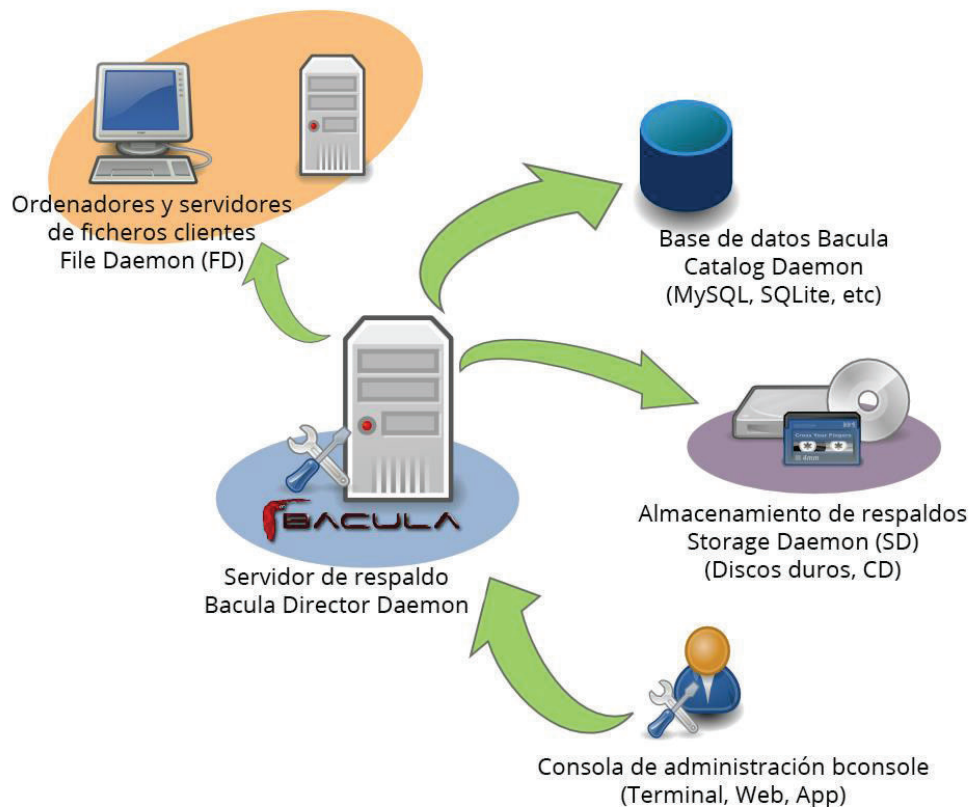


Figura 1-1 Arquitectura de Bacula²

- **Director (DIR, bacula-director):** es el programa servidor que supervisa todas las funciones necesarias para las operaciones de copia de seguridad y restauración. Es el eje central de Bacula y en él se declaran todos los parámetros necesarios. Se ejecuta como un “demonio” en el servidor.³

² <http://victorroblesweb.es/2013/11/04/backups-red-bacula-funcionamiento/>

³ <http://victorroblesweb.es/2013/11/04/backups-red-bacula-funcionamiento/>

- **Storage (SD, bacula-sd):** es el programa que gestiona las unidades de almacenamiento donde se almacenarán los datos. Es el responsable de escribir y leer en los medios que utilizaremos para nuestras copias de seguridad. Se ejecuta como un “demonio” en la máquina propietaria de los medios utilizados. En muchos casos será en el propio servidor, pero también puede ser otro equipo independiente.
- **Catalog:** es la base de datos que almacena la información necesaria para localizar donde se encuentran los datos salvaguardados de cada archivo, de cada cliente, entre otros. En muchos casos será en el propio servidor, pero también puede ser otro equipo independiente.
- **Console (bconsole):** es el programa que permite la interacción con el “Director” para todas las funciones del servidor. La versión original es una aplicación en modo texto (bconsole). Existen igualmente aplicaciones GUI para Windows y Linux (Webmin, Bacula Admin Tool, Bacuview, Webacula, Reportula, Bacula-Web).
- **File (FD):** este servicio, conocido como “cliente” o servidor de ficheros está instalado en cada máquina a salvaguardar y es específico al sistema operativo donde se ejecuta. Responsable para enviar al “Director” los datos cuando este lo requiera.⁴

1.2.4.2. ELEMENTOS DE CONFIGURACIÓN BACULA

Una vez instalados todos los demonios de Bacula se modifica los archivos de configuración necesarios para que las diferentes instancias de Bacula puedan interactuar entre sí.

Archivos de configuración necesarios para poder configurar Bacula:

⁴ <http://victorroblesweb.es/2013/11/04/backups-red-bacula-funcionamiento/>

- bacula-dir.conf, archivo de configuración de Bacula director.
- bacula-sd.conf, archivo de configuración del storage daemon.
- bacula-fd.conf, archivo de configuración de file daemon.
- bconsole.conf, consola para realizar respaldo

Elementos de bacula-dir.conf

Este es el archivo de configuración de Bacula Director. Los elementos que se deben definir son:

Director: Esta directiva sirve para definir la clave de acceso de la consola al director y sólo puede existir una instancia de este recurso.

- **Name:** Nombre que se asigna al director. Es el mismo nombre que se permitirá a los otros demonios.
- **DIRport:** Puerto de escucha para las consolas, por defecto viene configurado el puerto 9101.
- **QueryFile:** Archivo con las consultas a la base de datos.
- **WorkingDirectory:** Directorio de trabajo, esto no se debe cambiar.
- **PidDirectory:** Directorio donde crear los archivos con pid.
- **Maximum Concurrent Jobs:** Número máximo de trabajos concurrentes que acepta, establecer este valor igual a 1 implica que el director solo hará un trabajo cada vez, este es el valor por defecto, si este valor aumenta se permite que varios directores utilicen esos demonios a la vez.
- **Password:** Contraseña que se le pedirá al programa de consola. Esta contraseña no se pide por teclado, sino que se almacena en el archivo de configuración del programa de consola.
- **Messages:** Donde se enviarán los mensajes asociados a un trabajo concreto.

- **DirAddress:** Dirección donde escucha el director. Indicar 127.0.0.1 implicara que no podrán abrirse consolas Bacula en máquinas remotas, pero no causa problemas si tenemos los demás demonios en otras máquinas puesto que es el director es el que abre las conexiones con los otros demonios. En el caso que configure la dirección IP local pero puede poner la dirección IP del mismo servidor.

JobDefs: En este recurso se define la tarea, directorios, para un cliente, planificación de copias, conjunto de discos, un determinado dispositivo.

- **Name:** definición del nombre del trabajo, es lo que se visualiza en la consola.
- **Type:** tipo de trabajo puede ser: respaldos o restauraciones.
- **Level:** tipo de respaldos: Full, Incremental, Diferencial.
- **Client:** definimos el recurso del cliente, del que queremos hacer respaldos.
- **FileSet:** definimos el recurso FileSet, de los ficheros que queremos guardar.
- **Schedule:** programación asignada al respaldos.
- **Storage:** donde guardaremos los ficheros.
- **Messages:** donde se enviaran los mensajes asociados a un trabajo concreto.
- **Pool:** que conjunto de volumen se usara.

Job: se definen los jobs que se van a correr. Bacula corre los jobs automáticamente solo si tiene un Schedule asociado y si no lo tiene, el job se puede correr manualmente.

- **Name:** se le asigna un nombre al job.
- **JobDefs:** define el nombre del recurso JobDefs que voy a utilizar.

En este caso también se indica el Job para la restauración de archivos:

- **Name:** definición del nombre del trabajo, es lo que se visualiza en la consola
- **Type:** tipo de trabajo puede ser: respaldos o restauración.
- **Client:** definimos el recurso del cliente.
- **FileSet:** FileSet a usar.
- **Storage:** donde guardaremos los ficheros.
- **Pool:** que conjunto de volumen se usara.
- **Message:** donde se enviaran los mensajes asociados a un trabajo concreto
- **Where:** directorio donde se guardara los archives restaurados.

FileSet: Define los directorios y archivos que se van a respaldar y cuales se van a excluir.

- **Name:** nombre del recurso
- **File:** indica los directorios que se van a respaldar.

Schedule: Define cuando se va a ejecutar un trabajo y el tipo de copia que se va a hacer.

- **Name:** nombre que se le asigna al recurso.
- **Run:** configuración de la programación de la tarea que puede ser incremental, full o diferencial.

Client: Aquí se especifica los datos del bacula file daemon con el que se debe establecer conexión para leer los ficheros necesarios, aquí se define la referencia hacia el equipo que queremos hacer respaldos.

- **Name:** Nombre del file daemon, debe coincidir con el nombre del cliente a respaldar.
- **Address:** IP o hostname de la máquina que tiene nuestro file daemon.
- **FDPort:** puerto donde escucha el file daemon.
- **Catalog:** el catálogo que usa nuestro file daemon.
- **Password:** Contraseña que enviará el director al file daemon para autenticarse.
- **File Retention:** Este parámetro indica cuanto tiempo deben permanecer los archivos en el catálogo.
- **Job Retention:** Indica cuanto tiempo como máximo estará un trabajo esperando.
- **AutoPrune:** una vez pasados los periodos File Retention y/o Job Retention se eliminan del catálogo y/o cola los ficheros/trabajos.

Storage: especifica los dispositivos encargados que podrá emplear Bacula para albergar las copias de respaldo.

- **Name:** nombre del medio de respaldo.
- **Address:** indica donde está el storage daemon que maneja el medio de almacenamiento.
- **SDPort:** Puerto de escucha.
- **Password:** Contraseña que enviará el director para autenticarse contra el storage daemon.
- **Device:** Nombre del medio configurado en el storage daemon que se debe usar.

- **Media Type:** Cuando se configura el medio se especifica qué tipo de medio, aquí también se muestra y debe coincidir con el que indica en el storage daemon.

Catalog: fija la información sobre qué base de datos se está utilizando y sólo puede existir una instancia de este recurso.

- **Name:** Nombre del catálogo.
- **dbname:** Nombre de la base de datos.
- **DB Address:** ip o host donde tenemos nuestro servidor MySQL.
- **user:** Usuario con privilegios en la base de datos.
- **password:** clave de usuario en esa base de datos.

Messages: se decide cómo y cuándo se va a comunicar Bacula con el administrador de respaldos.

- **Name:** nombre del recurso Messages.

Pool: Define una colección de cintas o discos sobre las que se hacen las copias de seguridad. Se pueden definir un pool por cada cliente que se tenga.

- **Name:** nombre del pool
- **Pool Type:** define el tipo de pool, que corresponde con el tipo de trabajo que se está ejecutando.
- **Recycle:** especifica que cada volumen se va a utilizar sólo una vez.
- **Autoprune:** aplica automáticamente el período de retención de volumen.
- **Volumen Retention:** define el período del tiempo que Bacula mantendrá registros de empleo asociados al volumen en la base de datos de catálogo.

- **Maximum Volume Bytes:** especifica el número máximo de bytes que se pueden escribir en el volumen.
- **Maximum Volume:** especifica el número máximo de volúmenes (cintas o archivos) que figuran en el pool.
- **Label Format:** etiqueta del archivo de respaldos.

Elementos del bacula-sd.conf

Configuración del archivo Bacula Storage. Se configura el storage y los dispositivos, que son los medios donde se van a almacenar físicamente los respaldos.

- **Storage:** donde se define el storage daemon.
- **Director:** donde se especifican los directores que pueden conectarse a ese storage.
- **Device:** se especifica el dispositivo donde se guardarán los datos.
- **Messages:** se decide cómo y cuándo se va a comunicar Bacula con el administrador de respaldos.

Elementos del bacula-fd.conf

Archivo donde se configura el cliente. Hay un archivo por cada cliente y reside en el cliente, no en el director.

Elementos del bconsole.conf

Este archivo configura la bconsole. Pueden existir varias bconsoles en distintos hosts, cada una con su archivo de configuración.

1.2.4.3. REQUERIMIENTOS DEL SISTEMA

SOFTWARE

Bacula se ha compilado y probado en los sistemas OpenSuSE Linux, FreeBSD y Solaris.

Para su compilación, requiere GNU C++ versión 2.95 o superior.

Dependiendo del gestor de base de datos elegido, necesita como mínimo la versión: MySQL 4.1, PostgreSQL 7.4, SQLite 3.

La consola para GNOME ha sido desarrollada y probada sobre GNOME 2.x. No hay ya soporte para GNOME 1.4.

HAREWARE

Procesador: Dual-Core AMD Opteron 1218

Memoria: 2 GB de RAM

Tarjeta Gráfica: nVidia Quadro FX 1500

Consumo de memoria

El rendimiento de una aplicación cliente-servidor como Bacula depende de varios factores que hacen difícil hacer un análisis de consumo. Hay diversos factores a tener en cuenta como el tipo de servidor del Director, la carga de trabajo, el volumen de las copias y el tráfico, y el tipo de clientes así como sus dispositivos.

Velocidad de ejecución

En cuanto a velocidad hay que limitarse a unas condiciones similares a las anteriores, ya que dependerá de la carga del servidor, del tráfico y volumen de datos.

1.2.4.4. VENTAJAS DE BACULA

- Bacula reduce el riesgo de pérdida de datos a un bajo costo y cumpliendo con los estándares de la industria.
- No requiere de un nivel alto de mantenimiento, liberando a su equipo de IT para realizar otras tareas.
- Bacula es un sistema escalable y mantenible, que lleva estabilidad y seguridad a su organización a un costo más bajo que el de cualquier herramienta pagada.

1.3. ANÁLISIS Y SELECCIÓN DE LA METODOLOGÍA DE TRABAJO

Las metodologías de trabajo son un conjunto de procedimientos, técnicas y ayudas a la documentación para el desarrollo de productos, facilitando la planificación, gestión, control y evaluación de los proyectos; consiguiendo un mejor proceso de desarrollo y un proceso estándar en su planificación.

Usando una metodología se pueden alcanzar los siguientes atributos en el producto final:

1. **Eficacia:** El sistema satisface los requisitos del usuario.
2. **Mantenibilidad:** Facilidad para realizar cambios una vez que el sistema está funcionando en la empresa del cliente.
3. **Usabilidad:** Facilidad de aprender a manejar el sistema por parte de un usuario que no tiene por qué ser informático. (La resistencia de los usuarios a aceptar un sistema nuevo será mayor cuanto peor sea la usabilidad).
4. **Fiabilidad:** Probabilidad de que no ocurra un error durante un intervalo de tiempo dado. La diferencia con la corrección es que en este atributo interesa

el tiempo, es decir, no se trata del número absoluto de defectos en el sistema sino de los que se manifiestan en un intervalo de tiempo.

- 5. Disponibilidad:** Probabilidad de que el sistema esté funcionando en un instante dado.
- 6. Corrección:** Baja densidad de defectos.
- 7. Eficiencia:** Capacidad del sistema de realizar su tarea con el mínimo consumo de recursos necesario.

Este proyecto servirá como una guía para la justificación del uso de una herramienta automatizada de respaldos, poniendo énfasis en las pérdidas por no contar con la información en el momento de un plan de contingencia o necesidad específica.

Para conseguir este objetivo y lograr que el presente proyecto tenga un desarrollo continuo y controlado se aplicarán técnicas de control de proyectos. Actualmente existen varias técnicas, normas o mejores prácticas que se encuentran documentadas en varias fuentes, de las cuales se escogerá la más conveniente.

1.3.1. MARCOS DE TRABAJO Y NORMAS MÁS USADAS

Las infraestructuras de las TI son el cimiento de los servicios del negocio, soportando los procesos de las organizaciones.

Los marcos de trabajo y buenas prácticas más usadas actualmente son:

1.3.1.1. COBIT 5

Conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI). COBIT 5 provee un Framework de Gobierno y Gestión de TI para las empresas.

COBIT es un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT.

La última versión de COBIT fue liberada en abril de 2012, esta última versión consolida e integra los marcos de trabajo COBIT 4.1, Val IT 2.0 y Risk IT, y también se basa significativamente en el marco de trabajo de aseguramiento de TI de ISACA (ITAF) y el Modelo de Negocio para la Información de Seguridad (BMIS). Sigue en línea con los marcos de trabajo y estándares como ITIL, ISO, PMBOK, PRINCE2 y FFIEC7⁵.

Beneficios de COBIT 5:

- Mantiene información de alta calidad para soportar las decisiones de negocio.
- Alcanzar los objetivos estratégicos y obtener los beneficios de negocio a través del uso efectivo e innovador de TI.
- Lograr la excelencia operativa a través de una aplicación fiable y eficiente de la tecnología.
- Mantener los riesgos relacionados con TI a un nivel aceptable.
- Optimizar el costo de servicios de TI y tecnología.

⁵ **ISACA**. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. [En línea] 2012. [Citado el: 18 de Julio de 2012.] <http://www.isaca.org/COBIT/Pages/default.aspx>.

- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas⁶.

Principios de COBIT 5

El marco de COBIT 5 se basa en 5 principios clave que incluyen una amplia guía para los facilitadores de gobierno y gestión de TI en la empresa. En la Figura 1.2 se muestran estos 5 principios.



Figura 1-2 Principios de COBIT 5

⁶ ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. [En línea] 2012. [Citado el: 18 de Julio de 2012.] <http://www.isaca.org/COBIT/Pages/default.aspx>.

COBIT 5 define 7 categorías de habilitadores que se pueden ver en la Figura 1.3:



Figura 1-3 Habilitadores de COBIT 5⁷

Principios, Políticas y Marcos: Son el vehículo para trasladar el comportamiento deseado en guías prácticas para la gestión diaria.

Procesos: Describen un conjunto de prácticas y actividades organizadas para cumplir con ciertos objetivos y producir un conjunto de salidas para alcanzar los objetivos generales relacionados con TI.

Estructuras Organizacionales: Son las entidades claves en la toma de decisiones de la empresa.

Cultura, Ética y Comportamiento: La cultura, ética y comportamiento de los individuos y de la empresa muchas veces son sobrestimados como un factor de éxito en las actividades de gobierno y gestión.

Información: Requerida para mantener la empresa en ejecución y bien gobernada. En el nivel operacional, la información es un producto clave de la empresa.

Servicios, Infraestructura y Aplicaciones: Incluye la infraestructura, la tecnología y las aplicaciones para proveer a la empresa los servicios y procesamiento de Tecnología de la Información.

⁷ COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

Personas, Habilidades y Competencias: Requeridas para completar con éxito las actividades y para tomar las decisiones correctas y acciones correctivas.

COBIT 5 hace una clara distinción entre gobierno y gestión. Estas dos disciplinas abarcan diferentes tipos de actividades, requieren de estructuras organizativas diferentes y tienen objetivos diferentes⁸.

Para este marco la diferencia clave entre gobierno y gestión es:

Gobierno: asegura que las necesidades de los Stakeholders, condiciones y opciones son evaluadas para determinar un balance entre el logro de los objetivos estratégicos de la organización; establecer dirección de la organización a través de priorización y toma de decisiones; y monitorear el desempeño y cumplimiento contra la dirección y los objetivos acordados. En la mayoría de las empresas, el gobierno es responsabilidad de la junta directiva bajo el mando del presidente.

Gestión: planea, construye, ejecuta y monitorea actividades en alineamiento con la dirección establecida por gobierno, para alcanzar los objetivos estratégicos de la organización. En la mayoría de las organizaciones, gestión es responsabilidad de la dirección ejecutiva bajo el mando del CEO.

FRAMEWORK – Mapeos incluidos en COBIT 5

Estos mapeos son de suma utilidad a la hora de poder enlazar los distintos elementos que vinculan la capa más alta del Negocio con las actividades relacionadas con TI de los distintos Procesos de COBIT 5 los cuales son detallados en el Apéndice D del Framework.

La cascada de metas de COBIT 5 apoya el Principio #1:

Satisfacer las necesidades de los interesados, que es fundamental para COBIT y que por lo tanto se ha hecho prominente en las guías.

⁸ **ISACA.** COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows: ISACA, 2012. ISBN 978-1-60420-237-3.p.31.

Las metas en cascada de COBIT 5 traducen las necesidades de las partes interesadas en metas específicas, accionables y personalizadas dentro del contexto de la Organización, de las metas relacionadas con la TI y de las metas habilitadoras.

Los beneficios de las Metas en Cascada de COBIT 5:

- Permite definir las prioridades para implementar, mejorar y asegurar el gobierno corporativo de la TI, en base de los objetivos (estratégicos) de la Organización y los riesgos relacionados:
- En la práctica, las metas en cascada:
 - Definen los objetivos y las metas tangibles y relevantes, en diferentes niveles de responsabilidad.
 - Filtran la base de conocimiento de COBIT 5, en base de las metas corporativas para extraer una orientación relevante para la inclusión en los proyectos específicos de implementación, mejora o aseguramiento.
 - Claramente identifican y comunican qué importancia tienen los habilitadores (algunas veces muy operacionales) para lograr las metas corporativas.

1.3.1.2. Capability Maturity Model Integration (CMMI)

CMMI (Capability Maturity Model Integration) es un modelo de madurez de mejora de los procesos para el desarrollo de productos y de servicios. Consiste en las mejores prácticas que tratan las actividades de desarrollo y de mantenimiento que cubren el ciclo de vida del producto, desde la concepción a la entrega y el mantenimiento. Inicialmente fue desarrollado para los procesos relacionados con desarrollo e implementación de software por la Universidad Carnegie-Mellon para el Software Engineering Institute (SEI).

Las mejores prácticas CMMI se publican en los documentos llamados modelos. La versión actual de CMMI es la versión 1.3 y sus modelos cubren tres áreas de interés: Desarrollo, Adquisición y Servicios⁹.

El SEI ha identificado varias dimensiones para ayudar a las organizaciones en el desarrollo y mantenimiento de productos y servicios de calidad. En estas dimensiones la organización puede enfocarse para mejorar su negocio. En la Figura 1.4 se muestran las tres dimensiones críticas en que las organizaciones se enfocan: personas, procedimientos y métodos, herramientas y equipos.

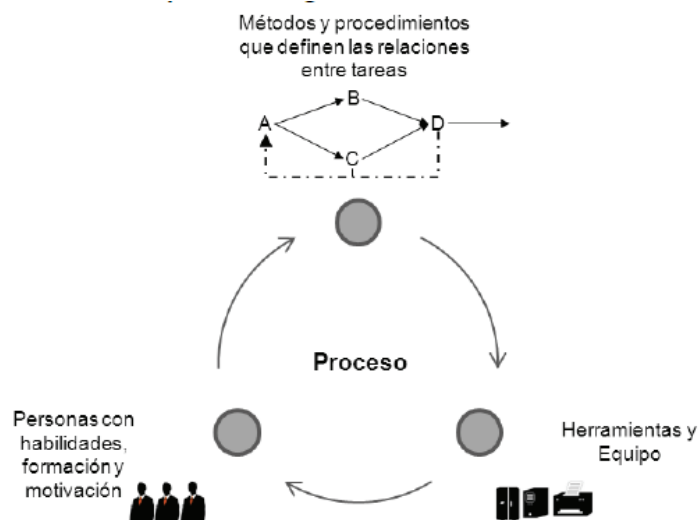


Figura 1-4 Tres dimensiones críticas para el negocio¹⁰

CMMI Framework

⁹ SOFTWARE ENGINEERING INSTITUTE. *Introduction to the Architecture of the*

CMMI® Framework. Hanscom AFB : Carnegie Mellon, 2007. CMU/SEI-2007-TN-009. p.1

¹⁰ Fuente: CMMI® for Development, Version 1.3 Introduction

Para la construcción de los modelos de CMMI, al igual que para los materiales de entrenamiento y evaluación, se utilizó el Framework de CMMI que consta de una colección de componentes para este fin, tales como áreas de proceso, metas, prácticas, material informativo acerca del uso de los modelos y sus componentes, guías de implementación de los modelos y componentes que describen el proceso de evaluación de los procesos en las organizaciones en la metas y prácticas del modelo.

La arquitectura del marco CMMI tiene por objeto controlar la selección y el uso de los componentes del modelo para la construcción de modelos de CMMI para distintas áreas de interés. Cuando se crea un nuevo modelo CMMI, los desarrolladores usan componentes ya probados que se ajusten a las necesidades de la nueva área de interés. De esta manera reducen el entrenamiento necesario y el alineamiento para procesos existentes.

CMMI Model Foundation

En el framework CMMI también se encuentra el CMMI Model Foundation (CMF), que es un esqueleto o base que contiene los componentes que debe incluir cada modelo de CMMI. De esta forma cada modelo de CMMI se construye complementando el CMF con componentes adicionales.

- El CMF está compuesto de las secciones:
- Parte introductoria del modelo
- Metas genéricas y prácticas genéricas
- Áreas de proceso
- Glosario

Un área de proceso es un grupo de prácticas referentes a un área determinada, que cuando se implementan, satisfacen un conjunto de metas consideradas importantes para el mejoramiento de esa área¹¹.

¹¹ **SOFTWARE ENGINEERING INSTITUTE.** *Introduction to the Architecture of the CMMI® Framework.* Hanscom AFB : Carnegie Mellon, 2007. CMU/SEI-2007-TN-009. p.9

Niveles de madurez CMMI

CMMI clasifica a las empresas en niveles de madurez. Estos niveles sirven para conocer la madurez de los procesos de ingeniería de software.

- **Inicial o Nivel 1 CMM:** Este es el nivel en donde están todas las empresas que no tienen procesos.
- **Repetible o Nivel 2 CMM:** Quiere decir que el éxito de los resultados obtenidos se pueden repetir. La principal diferencia entre este nivel y el anterior es que el proyecto es gestionado y controlado durante el desarrollo del mismo.
- **Definido o Nivel 3 CMM:** alcanzar este nivel significa que la forma de desarrollar proyectos está definida, esto quiere decir que está establecida, documentada y que existen métricas para la consecución de objetivos concretos.
- **Cuantitativamente Gestionado o Nivel 4 CMM:** Los proyectos usan objetivos medibles para alcanzar las necesidades de los clientes y la organización. Se usan métricas para gestionar la organización.
- **Optimizado o Nivel 5 CMM:** Los procesos de los proyectos y de la organización están orientados a la mejora de las actividades. Mejoras incrementales e innovadoras de los procesos que mediante métricas son identificadas, evaluadas y puestas en práctica.

La Tabla 1.2 muestra las áreas de proceso core de CMMI y su asociación con los niveles de madurez.

Área de Proceso	Categoría	Nivel de Madurez
Análisis Causal y Resolución (CAR)	Soporte	5
Gestión de Configuración (CM)	Soporte	2
Análisis de Decisiones y Resolución (DAR)	Soporte	3
Gestión Integrada del Proyecto (IPM)	Gestión de Trabajo y Proyectos	3
Medición y Análisis (MA)	Soporte	2

Definición de Procesos de la Organización (OPD)	Gestión de Procesos	3
Enfoque en Procesos de la Organización (OPF)	Gestión de Procesos	3
Gestión del Rendimiento de la Organización (OPM)	Gestión de Procesos	5
Rendimiento de Procesos de la Organización (OPP)	Gestión de Procesos	4
Formación en la Organización (OT)	Gestión de Procesos	3
Monitorización y Control del Proyecto (PMC)	Gestión de Trabajo y Proyectos	2
Planificación de Proyecto (PP)	Gestión de Trabajo y Proyectos	2
Aseguramiento de la Calidad del Proceso y del Producto (PPQA)	Soporte	2
Gestión Cuantitativa del Proyecto (QPM)	Gestión de Trabajo y Proyectos	4
Gestión de Requisitos (REQM)	Gestión de Trabajo y Proyectos	2
Gestión de Riesgos (RSKM)	Gestión de Trabajo y Proyectos	3

Tabla 1-2 Áreas de proceso, categorías y niveles de madurez CMMI Model Foundation¹²

CMMI for Development (CMMI-DEV)

Este modelo identificado como CMMI-DEV provee una guía para la aplicación de mejores prácticas de CMMI para procesos de desarrollo de software en las organizaciones. La idea de CMMI no es crear ni establecer los procesos para el desarrollo de software, solo plantea lineamientos que deberían tener estos procesos. Estos lineamientos cubren todo el ciclo de vida del producto desde concepción hasta implementación y mantenimiento. CMMI-DEV contiene 22 áreas

¹² CMMI® for Development, Version 1.3 Process Areas

de proceso. De estas áreas de proceso 16 son core, una es un área de proceso compartida y 5 son áreas de proceso específicas de desarrollo de software¹³.

Áreas de proceso

Dado que todos los modelos de CMMI son construidos con el CMMI framework, CMMI DEV contiene 16 áreas core de proceso que cubren los aspectos básicos para la mejora de procesos en esta área de interés. Parte del contenido en algunas áreas core de proceso es similar en los demás modelos y otra parte puede estar ajustada para trabajar con un área de interés específica, en este caso Development.

Todos los modelos de CMMI representan niveles de madurez en su diseño y contenido. Un nivel de madurez es un escalamiento definido de la evolución en la mejora de procesos de la organización. Cada nivel de madurez forma y mejora un importante grupo de procesos en la organización, preparándola para alcanzar el siguiente nivel de madurez.

La Tabla 1.3 muestra los procesos de CMMI-DEV y su asociación con los niveles de madurez.

Área de Proceso	Categoría	Nivel de Madurez
Integración del Producto (PI)	Ingeniería	3
Desarrollo de Requisitos (RD)	Ingeniería	3
Gestión de Acuerdos con Proveedores (SAM)	Gestión de Proyectos	2
Solución Técnica (TS)	Ingeniería	3
Validación (VAL)	Ingeniería	3
Verificación (VER)	Ingeniería	3

Tabla 1-3 Áreas de proceso, categorías y niveles de madurez CMMI-DEV¹⁴

¹³ **SOFTWARE ENGINEERING INSTITUTE.** *CMMI® for Development, Version 1.3.* Hanscom AFB : Carnegie Mellon, 2010. ESC-TR-2010-033. p.3

¹⁴ CMMI® for Development, Version 1.3 Process Areas

1.3.1.3. ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. La mayoría de estos estándares se encuentran en preparación. Dentro de los más importantes de esta serie están: ISO 27000, ISO 27001, ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27006.

Para el propósito de este trabajo se toman como enfoque de análisis de la serie ISO 27000, las normas ISO 27001 e ISO 27002.

1.3.1.3.1. Norma ISO 27001

Tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI). Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. Esta norma abarca todos los tipos de organizaciones ya sean empresas comerciales, entes del gobierno u organizaciones sin fines de lucro y ha sido preparada con el fin de proporcionar a estas organizaciones un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). En Colombia la norma NTC-ISO/IEC 27001 fue ratificada por ICONTEC en el Consejo Directivo del 22 de Marzo de 2006.

La adopción de un SGSI debería ser una decisión estratégica para una organización, ya que el diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización.

Este enfoque basado en procesos para SGSI, estimula a los usuarios a hacer énfasis en:

- Comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información.
- Implementar y operar controles para mejorar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización.
- El seguimiento y revisión del desempeño y eficacia del SGSI.
- La mejora continua basada en la medición de objetivos¹⁵.

En la Figura 1.5 se encuentra el origen de la referencia se muestra cómo funciona el modelo Planear-Hacer-Chequear-Actuar (PDCA) adoptado por la norma 27001 y que puede ser aplicado a todos los procesos del SGSI. Muestra como el SGSI toma requerimientos y expectativas de seguridad de los Stakeholders, y por medio de acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen esos requerimientos y expectativas.

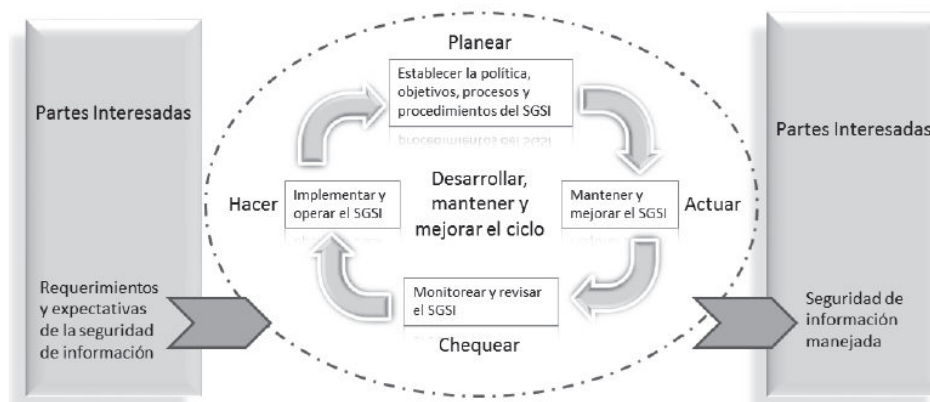


Figura 1-5 Modelo PDCA aplicado a los procesos SGSI¹⁶

¹⁵ Caracterización de Procesos de Gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria Editorial Colombiana, apoyando el proceso de transformación digital.

¹⁶ INTERNATIONAL STANDARD ISO/IEC 27001. PCDA Model

Establecer el SGSI: En este punto la organización debe establecer una política de SGSI de acuerdo a las características del negocio, su ubicación y sus activos, al igual que definir objetivos de control, controles, procesos y procedimientos de seguridad necesarios para gestionar el riesgo, y mejorar la seguridad de la información.

Implementar y operar el SGSI: La organización debe formular e implementar un plan para el tratamiento de los riesgos para cumplir con los objetivos de control identificados, este plan debe considerar la financiación y asignación de funciones y responsables. En este punto también se debe definir cómo medir la eficacia de los controles seleccionados para el tratamiento de riesgos además de gestionar la operación de SGSI, sus recursos, e implementar procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

Monitorear y revisar el SGSI: La organización debe ejecutar procedimientos de monitoreo y revisión para detectar fácilmente errores en procesamiento, identificar rápidamente incidentes de seguridad y determinar si las acciones tomadas para solucionar un problema de seguridad fueron eficaces. Otro aspecto importante en este punto es actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

Mantener y mejorar el SGSI: En este punto, la organización regularmente debe emprender acciones correctivas y preventivas para mitigar las causas de no conformidades asociadas a los requisitos del SGSI, comunicar estas acciones y mejoras a todas las partes interesadas de la organización y asegurar que las mejoras cumplan con los objetivos previstos.

1.3.1.3.2. Norma ISO 27002

Un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 y renombrado sin modificar su contenido en 2007 a ISO/IEC 27002:2005. Tiene su origen en el British Standard BS 7799-1 que fue desarrollado y publicado por el BSI. Esta norma es una guía de buenas prácticas de seguridad

de la información, contiene los objetivos de control y controles recomendables para seguridad de la información¹⁷.

Este estándar está compuesto por 39 objetivos de control y 133 controles, agrupados en 11 dominios o cláusulas de control de seguridad.

Cláusulas de control de seguridad

Cada cláusula contiene un número de categorías de seguridad principales. Cada categoría está compuesta de un objetivo de control que establece lo que se debería lograr y uno o más controles que se pueden aplicar para lograr el objetivo de control.

- Política de Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes de Seguridad de la Información
- Gestión de la Continuidad Comercial
- Cumplimiento

¹⁷ **ISO/IEC**. *INTERNATIONAL STANDARD ISO/IEC 17799*. Switzerland : ISO copyright office, 2005.
ISO/IEC 17799:2005.p.vii

1.3.1.4. Information Technology Infrastructure Library (ITIL)

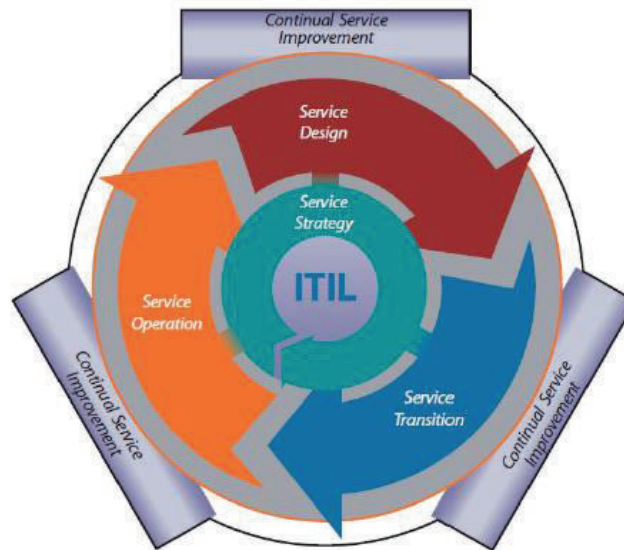


Figura 1-6 Ciclo de Vida ITIL¹⁸

Estrategia del servicio

Guía de cómo diseñar, desarrollar e implementar una Gestión de Servicios como un activo estratégico. Modela y planea servicios que tengan Utilidad y Garantía. Fase donde se integra la visión y objetivos del negocio con TI. En esta fase se establecen Políticas y objetivos. Se determinan objetivos estratégicos, se definen prioridades de Inversión, se definen patrones de actividad del negocio y se desarrollan planes para predominar sobre competidores¹⁹.

Procesos

- Gestión de Portafolio
- Gestión Financiera
- Gestión de la Demanda

¹⁸ Libro ITIL – The Official Introduction to the ITIL Service Lifecycle.

¹⁹ OGC. Service Strategy. *ITIL Version 3*.

Diseño del servicio

La principal característica de esta fase es la de diseñar, o modificar servicios para su incorporación en el catálogo de servicios. Debe tener en cuenta los requerimientos del negocio como los recursos y capacidades disponibles. Tiene 4 áreas principales a ser consideradas (4P) Personas, Procesos, Productos, Proveedores²⁰.

Procesos

- Gestión de Niveles de Servicio
- Gestión de Catalogo de Servicio
- Gestión de la Disponibilidad
- Gestión de la Seguridad de la información
- Gestión de Proveedores
- Gestión de la Capacidad
- Gestión de la Continuidad del servicio de TI

Transición del servicio

En esta fase se establecen expectativas del cliente de cómo debe ser prestado el servicio y su uso, integra los productos y servicios definidos en la fase de Diseño, además de garantizar que sean accesibles a los usuarios autorizados. También se evalúan los riesgos y errores durante la transición. Se incrementan las recomendaciones sobre el uso del servicio, se reducen las variaciones entre las expectativas y lo que realmente se presta²¹.

Procesos

- Gestión de Cambios
- Gestión de la Configuración y Activos del Servicio
- Gestión de Entregas y Despliegues

²⁰ OCG. Service Design. *ITIL Version 3*.

²¹ OCG. Service Transition. *ITIL Version 3*.

- Validación y pruebas
- Evaluación
- Gestión del Conocimiento

Operación del Servicio

En esta fase se tiene la etapa crítica de todo el ciclo de vida del servicio. La calidad de los servicios prestados es evaluada constantemente por la satisfacción y la percepción que tengan los clientes y usuarios en la prestación del servicio, todo depende de una sincronía entre la coordinación de los recursos y los servicios en una correcta organización. Se gestionan la infraestructura tecnológica utilizada en la prestación de los servicios y se da soporte a los usuarios del servicio²².

Procesos

- Gestión de Eventos
- Gestión de Incidencias
- Gestión de Peticiones
- Gestión de Problemas
- Gestión de Acceso a los Servicios TI

Mejoramiento Continuo:

El objetivo de esta Gestión es hacer seguimiento y medición a todas las actividades y procesos involucrados en la prestación de los servicios de TI. Todo hace énfasis en mejorar la calidad de los servicios actuales, identificar e incorporar servicios que cumplan de una mejor forma los requerimientos del cliente, hacer procesos más eficientes²³.

²² **OCG.** Service Operation. *ITIL Version 3.*

²³ **OCG.** Continual Service Improvement. *ITIL Version 3.*



Figura 1-7 Ciclo Deming²⁴

1.3.2. METODOLOGIA DE TRABAJO

El presente trabajo tiene como propósito formular un marco de trabajo para la definición e implementación de una gestión de respaldos de información que proporcione una gran variedad de funciones de gestión de almacenamiento desde un único punto de control, que permite a la empresa aprovechar la gran cantidad de información de la que dispone, así como proteger los datos de la organización de fallas y otros errores mediante copias de respaldo, archivado, administración del espacio de almacenamiento, así mismo, cumplir con regulaciones y planes de recuperación de desastres.

Para el desarrollo de la metodología de trabajo se emplea un método analítico que estudia los hechos partiendo de la descomposición del objeto de estudio, para analizarlo en forma individual y luego de una forma integral.

Adaptando esta metodología al objeto de estudio se parte de los criterios de información establecidos en COBIT 5, hasta llegar a un mapeo integral de los

²⁴ Libro ITIL – The Official Introduction to the ITIL Service Lifecycle.

procesos y gestiones que intervienen en la definición de un plan de contingencia mediante la fusión de marcos de referencia y buenas prácticas como es ITIL v3 2011.

Para la definición e implementación de un sistema de gestión de respaldos de información centralizado, así como las políticas de seguridad de respaldos y plan de contingencia se realizará en las siguientes fases:

FASE1.- PLANIFICACION Y ANALISIS DE REQUERIMIENTOS

Esta fase proporciona un marco de trabajo que permita gestionar y proteger los datos de las empresas mediante la automatización de respaldos de información.

PASO 1.- DEFINICIÓN DE UN MODELO DE RESPALDO DE DATOS:

En esta fase el objetivo es conocer la situación actual del sistema de respaldos del caso de estudio y analizar los esquemas que maneja, luego se determina que bacula nos permite realizar el proceso a través de la red, permitiendo así planificar por los diferentes métodos (Incremental, Diferencial, Full) disponibles, así como el desarrollo de las políticas de respaldos y plan de contingencia. Dicho proceso de respaldo se lo va a realizar en los servidores que se consideren prioritarios, y de esta manera se optimizará y automatizará la forma actual de realizarlo, la cual puede estar sujeta a errores.

PASO 2.- DEFINICIÓN DE UN MODELO DE ARQUITECTURA DE INFORMACIÓN :

En esta fase se realiza la recopilación y análisis de los datos para determinar la información a respaldarse, para el cumplimiento de esta tarea se realizaran encuestas o entrevistas con los encargados o responsables de los datos en el caso de estudio tanto para recopilar información para el desarrollo de políticas de respaldo y plan de contingencia.

FASE 2.- IMPLEMENTACIÓN DEL PROTOTIPO

En la actualidad la automatización de procesos es un tema de gran importancia por tal motivo la implementación de este prototipo inicia con un análisis del caso de

estudio que permita identificar sus necesidades y poder desarrollar el modelo de respaldos.

PASO 1.- DESCRIPCIÓN DEL CASO DE ESTUDIO

Realizar un análisis completo del caso de estudio y determinar los procesos y tipos de respaldos que realiza.

PASO 2.- POLITICAS DE RESPALDO DE INFORMACIÓN

Esta fase es la determinada para el desarrollo del modelo de arquitectura de información y el modelo de plan de respaldos ya identificados los problemas del caso de estudio se puede automatizar los respaldos y definir las políticas de respaldo y plan de contingencia.

PASO 3.- INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR

Se inicia la instalación y configuración del servidor con la información definida en la fase anterior.

PASO 4.- INSTALACIÓN Y CONFIGURACIÓN DE LOS CLIENTES

Se realiza la instalación y configuración de cada nodo ya identificado a respaldarse.

PASO 5.- CONFIGURACIÓN DE LAS TAREAS PROGRAMADAS

Muestra la configuración de la planificación ya definida en el modelo de respaldos.

PASO 6.- PRUEBAS

Se realizan las pruebas de ejecución del sistema automatizado, tomando en cuenta que la parte primordial de un sistema de respaldos es la restauración en el modelo realizado.

PASO 7.- ANALISIS DE RESULTADOS

Realiza un breve análisis del funcionamiento del sistema automatizado de respaldos y los beneficios generados al caso de estudio desde su implementación.

CAPÍTULO 2: PLANIFICACIÓN Y ANÁLISIS DE REQUERIMIENTOS

2.1. DEFINICIÓN DE UN MODELO DE RESPALDO DE DATOS

La definición de un modelo de respaldo de datos tiene que ver con salvaguardar, defender y proteger la información, para ello es muy importante realizar una copia de seguridad de la información sensible que será tomada de la empresa.

El concepto de proteger con el uso de herramientas automatizadas intenta defender la información almacenada en los servidores de la organización, tales como Servidores de Archivos, Servidores de Correo, Servidores de Aplicaciones, de pérdidas de información, desastres naturales, error humano, entre otros.

2.1.1. IMPORTANCIA DE LA INFORMACIÓN

Es importante conocer el estado actual del sistema de respaldos de la empresa, sus actividades, procesos, procedimientos y personas que lo ejecutan hasta la actualidad, para a partir de ello planificar el nuevo modelo de respaldos.

Cada aplicación maneja un conjunto muy variado de datos, algunos estáticos, otros dinámicos. Hay datos base, a partir de los cuales se generan datos resultantes (información). Al definir el respaldo se establece si se copian todos los archivos o parte de ellos. También se puede tomar en consideración si la copia incluye la aplicación o a su vez el sistema informático. La decisión final se tomará sobre un análisis de la información basándose en la criticidad de los datos y el valor que estos tengan para la empresa, para ello se hará un análisis completo en el [Capítulo 2.2](#).

2.1.2. PLAN DE RESPALDOS

Los procedimientos de respaldo y recuperación que se realicen dentro de la empresa deben formar parte de un elaborado plan de respaldo y recuperación, el cual debe ser documentado y comunicado a todas las personas involucradas. El

plan debe ser revisado y de ser necesario modificado de manera periódica dado que, con el pasar del tiempo, varias características que se consideran para elaborar este plan sufren cambios o actualizaciones (software o hardware utilizado, soporte, entre otros).

Respaldo o copia de seguridad: Es el proceso mediante el cual se generan copias controladas y seguras de la información, estas copias se guardan por tiempos definidos y se pueden utilizar para restaurar información en caso de pérdida, degradación o para consulta histórica.

El objetivo principal de realizar estas copias de seguridad es tener la capacidad de asegurar la recuperación de los datos ante posibles pérdidas o catástrofes. Esta capacidad para la mayoría de empresas se convierte en algo de suma importancia, incluso algo crítico para las empresas debido a la creciente cantidad de información con que se trabaja hoy en día.

Las copias de seguridad se pueden clasificar en 2 grandes grupos:

Copias de seguridad del sistema: cuyo objetivo es la recuperación y arranque de un sistema informático tras un desastre en el cual se almacenaran copias de los ficheros de software de base y software de aplicación.

Copias de seguridad de datos: cuyo objetivo es la recuperación de los datos ante eventuales pérdidas ocurridas por alguna pérdida de información.

Realizar una copia de seguridad resulta un proceso fácil, sin embargo, la dificultad se presenta al realizar la planificación de una copia de seguridad. Hay que discernir qué es lo que se ha de guardar en ella, cómo guardarlo, dónde hacerlo y cómo recuperar la información. Estas dificultades se hacen cada vez mayores según aumenta el volumen de datos a manejar.

El plan debe contener todos los ítems detallados a continuación y cualquier otro que mejore la realización del trabajo o clarifique la tarea.

2.1.3. SELECCIÓN DE LA HERRAMIENTA DE AUTOMATIZACIÓN

En este proyecto se definió el uso de Bacula una herramienta de código abierto especificado en el [capítulo 1.2.4](#), pero las empresas están libres de escoger la herramienta para automatizar sus respaldos.

En esta fase se determinará el tipo de hardware y software mínimo indispensable para cumplir con los requerimientos de la solución de respaldos a usarse. Es importante indicar que la decisión es comprar una herramienta especializada en lugar de desarrollarla, debido a que factores como tiempo, costo, y conocimientos específicos para desarrollo siempre serán mayores en este tipo de proyectos.

2.1.4. TIPOS DE RESPALDOS

Existen diferentes tipos de respaldos en función de la cantidad de datos que se desean respaldar, cuando se copian la totalidad de los datos existentes se considera dicha copia como respaldo completo y cuando se respalda sólo una parte de la información, a éstos se los denomina respaldos parciales.

Existen ocasiones en las que por cantidad, capacidad de los medios o tiempo disponible, no es posible copiar todos los datos existentes. Para solucionar este tipo de problemas existen varias maneras de realizarlas:

2.1.4.1. RESPALDOS COMPLETOS

Los respaldos completos copian todo lo que se encuentra en el origen y lo almacenan en el destino programado. Algo que hay que tener en cuenta cuando realizamos este tipo de respaldos es que suelen ocupar mucho espacio en los servidores asignados para esta acción y normalmente es necesario invertir bastante tiempo de los recursos técnicos y humanos para realizarlas.

Por otro lado, este tipo de copias permiten restaurar un sistema fácilmente ante una catástrofe.

Las copias completas guardan desde el sistema operativo de la máquina o la estructura de directorios, log, perfiles de usuario, estructuras de datos y toda

aquella información necesaria; si restauramos la copia en una máquina que no sea la de origen, podrá funcionar exactamente de la misma manera que en el momento en que se hizo la copia de seguridad.

Cuando se realiza una copia de este tipo, se borra todo lo que tenían los soportes de almacenamiento antes, es decir, se vacía el catálogo. Para realizar la copia podremos estar usando o bien un software de copias de seguridad o bien algún mandato u opción proporcionada por el propio sistema operativo. En función de la alternativa empleada, podrá ser necesario inicializar los soportes antes de empezar la copia.

2.1.4.2. RESPALDOS DE TODO LO MODIFICADO

Dentro de las copias de todo lo modificado, podemos distinguir 2 tipos:

2.1.4.2.1. RESPALDOS INCREMENTALES

Los respaldos incrementales, también llamadas copias de archivos modificados o copias evolutivas, son las copias que se realizan partiendo de un respaldo total y en la que en los siguientes procesos de copia solamente tomarán los datos que hayan cambiado desde el respaldo anterior. Tiene la ventaja de que reduce en buena parte la cantidad de datos a copiar en cada operación, pero la restauración de los mismos es complicada, puesto que requiere que los datos se recuperen en el mismo orden que se realizaron si se desea disponer de los datos correctamente actualizados y evitar incongruencias.

La principal desventaja es el recuperar un archivo cuando un respaldo incremental ha fallado, puesto que será imposible recuperar su información.

2.1.4.2.2. RESPALDOS DIFERENCIALES

Al igual que en los respaldos incrementales, en las diferenciales no se guardan todos los archivos, sino sólo aquellos que han sido modificados, la copia diferencial únicamente copia los archivos y directorios que han sido creados y/o modificados desde la última copia completa. Esto viene a suponer que si el lunes se realiza una

copia completa y el martes se ejecuta una copia diferencial, únicamente se copiaran los ficheros creados o modificados durante el martes. Este mismo comportamiento se efectuará si la lanzamos el miércoles, tomando la copia completa del lunes como base.

Los respaldos diferenciales requieren más espacio en disco y más tiempo que los respaldos incrementales, más datos deben ser copiados a la cinta diferencial y la cantidad de datos que se guardan en las cintas cada día después de un respaldo total es mayor.

2.1.5. MEDIOS DE ALMACENAMIENTO A UTILIZAR

Existen numerosos medios de almacenamiento en el mercado. La decisión de elegir unos u otros depende principalmente del volumen de información que maneje la empresa.

Los medios a utilizar dependerán del tipo de sistema (micro, Main frame, entre otros), cantidad de información a almacenar, tiempo disponible para realizar el respaldo, costos y obviamente de la tecnología disponible al momento.

Actualmente se cuenta con una variedad muy amplia de equipos disponibles y a costos muy bajos, sobre todo al nivel de micro computadoras. A nivel mainframe las posibilidades se limitan. Las características principales a considerar de cada opción serán la capacidad de almacenamiento, medida en MB, GB o TB con velocidad de transferencia de datos medida desde KB/s hasta GB/s. Los medios magnéticos son los más difundidos; también los hay ópticos.

Las opciones más comunes son (en orden descendente por capacidad de almacenamiento promedio):

- ✓ Discos duros
- ✓ Cintas
- ✓ Cartuchos (alta densidad, micro)

- ✓ DVD ROM
- ✓ Zip drive
- ✓ Tarjetas PCM-CIA

Existe la posibilidad de realizar respaldo en medios pertenecientes a terceras partes. Actualmente, varias empresas ofrecen a través de Internet un servicio de respaldo, el mismo que se realiza en los equipos de estas empresas transfiriendo los datos a través de la Internet, servicio conocido como almacenamiento en la Nube. Notar que este servicio es útil si tenemos una conexión con un buen ancho de banda y una cantidad de datos pequeña o mediana.

2.1.6. PLANIFICACION DE RESPALDOS

Para determinar cuándo se realizara el respaldo es necesario conocer los tiempos incurridos en desarrollar la tarea y las ventanas de tiempo disponibles en producción (tiempo disponible para realizar tareas que no afecte a los procesos habituales de procesamiento de datos). Los tiempos incurridos en desarrollar la tarea varían dependiendo del soporte utilizado (a mayor velocidad de transferencia menor tiempo incurrido), el tipo de respaldo utilizado (el respaldo completo es el que lleva mayor cantidad de tiempo) y la cantidad de datos a respaldar (a mayor cantidad mayor tiempo de respaldo).

Generalmente en las empresas, las ventanas de tiempo disponibles durante la semana son cortos, por lo que se combinan los tipos de respaldo dependiendo del día de la semana. Así, el fin de semana se realiza un respaldo global y durante la semana se realizan respaldos incrementales.

Periodicidad: es cada cuánto realizar los respaldos, lo cual dependerá de la cantidad de operaciones realizadas y las ventanas de tiempo disponibles.

Usualmente y como recomendable, los mismos deben realizarse diariamente.

Por ejemplo, día a día se hacen respaldos incrementales o diferenciales y una vez por semana se hacen respaldos completos parciales y una al mes respaldos completos totales.

Siempre estas decisiones dependen del volumen de los datos, del soporte de almacenamiento disponible, de la velocidad del respaldo, de la importancia de los datos, etc.

2.1.7. RESTAURACIÓN DE DATOS

La restauración de los datos es el fin a cumplir al momento de realizar una buena planificación de copias de seguridad. Como se expone anteriormente el realizar respaldos tiene como objetivo hacer frente a cualquier pérdida de información y garantizar la continuidad del negocio. Por tanto, una correcta planificación de copias de seguridad, permitirá a la empresa restaurar los datos y volver a la situación previa al desastre o la interrupción para continuar con sus actividades con total normalidad.

Llegados a este punto y después del planteamiento realizado a lo largo del trabajo, la empresa podrá enfrentar algún problema y llevar a cabo una restauración.

Los casos más típicos son dos: restaurar ficheros o carpetas sueltas, o poner en marcha un sistema desde cero.

Para hacer frente al primer caso debemos saber si el fichero, carpeta o biblioteca ha sido creado o modificado desde la última copia completa. En caso afirmativo se debe usar la copia incremental o diferencial más reciente. Si por el contrario es información que no ha sido modificada desde la última copia completa o si es necesario restaurar información de un día concreto, se hará uso de la última copia completa o bien de la copia completa más cercana a la fecha solicitada.

Para resolver el segundo caso se deberá utilizar la última copia completa que se disponga y después de las copias incrementales o diferenciales realizadas desde entonces.

Restaurando la copia completa se genera un mismo sistema con la misma estructura de directorios y con las copias de archivos modificados estaremos dejando los datos lo más actualizados posible.

El ubicarse en la primera situación se genera por errores humanos, como puede ser un borrado accidental de información o al fallo de algún proceso, por su parte la segunda opción suele ser debido a caídas de sistema, cortes inesperados de suministro eléctrico y diferentes imprevistos normalmente fuera del alcance de la organización.

Finalmente, es meritorio citar algunos aspectos a tener en cuenta antes de llevar a cabo una restauración, como por ejemplo:

- Tener una debida autorización por escrito mediante una solicitud de restauración, Ver Anexo 1 SOLICITUD DE RESTAURACIÓN por parte del responsable de la información, principalmente cuando lo que se va a restaurar es algún fichero suelto a petición de cualquier usuario.
- Versión del sistema operativo en la que fue guardada la información y versión de la máquina que recibe los datos ya que puede darse el caso de que no sea la misma.
- Comprobar que la información que vamos a restaurar corresponde realmente a lo que queremos.
- Inmediatamente después de la restauración se debe verificar el correcto funcionamiento de los procesos de negocio. Si se ha traído de sede remota, se volverá a trasladar y si estaba en las propias instalaciones se volverá a guardar bajo las medidas de seguridad adecuadas.

2.1.8. POLÍTICAS DE RESPALDOS

Las políticas de respaldos tienen como objetivo mitigar los impactos de pérdida de información para mantener la continuidad del negocio por ello cuando se hacen respaldos la seguridad es esencial ya que la información de las empresas es

sensible y no se quiere que otras personas sin autorización tengan acceso a la misma.

Para definir las políticas se deben tomar en cuenta los siguientes puntos:

1. El respaldo de información, debe realizarse exclusivamente en un servidor destinado para todas las actividades de respaldos.
2. El Área de Informática es la responsable de realizar un respaldo diario de las carpetas que contiene el Servidor de Archivos respaldo Incremental y guardar mensualmente en disco compacto la correspondiente a los tres últimos días de cada mes.
3. El Área Administrativa es la responsable de custodiar la copia del disco de respaldos.
4. El Área de Informática es la responsable de custodiar el respaldo mensual.
5. En caso de presentarse alguna falla al guardar la información del día, es responsabilidad del operador reportarla al Área de Informática. De no hacerlo, la pérdida de información será su responsabilidad.
6. Cuando un integrante de la Coordinación solicite disponer de información respaldada anteriormente, debe justificar por escrito al Coordinador las causas y la fecha del respaldo requerido.
7. Llevar un registro o bitácora de los respaldos que se realizan, así como también las eventuales recuperaciones.
8. El encargado de los respaldos (operador o administrador) es el encargado de documentar todas las actividades relacionadas con los respaldos de información.
9. El responsable debe mantener un control semanal de los respaldos realizados.
10. Las claves de usuario NO serán respaldadas.

11. El administrador del sistema de respaldos deberá comprobar la confiabilidad del sistema de respaldo y recuperación de la información.
12. Verificar por lo menos una vez mes la integridad física del medio de respaldos.
13. Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la base de datos para así asegurar la integridad de la información respaldada.
14. Mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad y otros.
15. El estándar de etiquetas para los archivos de respaldo obtenidos por la herramienta de automatización debe indicar: tipo de respaldo, nombre del servidor, fecha del respaldo.
16. Cuando el espacio en el disco duro supere 1 TB es responsabilidad del Jefe técnico obtener el respaldo físico en discos y ubicarlos en un lugar fuera de la empresa y tenga un custodio.

2.1.9. PLAN DE CONTINGENCIA

En último lugar se menciona un aspecto muy importante, precisamente por su importancia, es que, en toda instalación informática deberían existir planes de contingencia que especifican claramente qué hacer frente a una situación crítica (desastres naturales, atentados, entre otros).

Gracias a estos planes, las personas saben qué deben hacer, y logran superar las situaciones. Los procedimientos de respaldo y recuperación que son la base de este documento, solamente son una parte del plan de contingencia. El plan se complementa con todos los procedimientos necesarios para volver a la empresa operativa ante cualquier desastre.

Estos planes incluyen alternativas para continuar funcionando el negocio, el organismo o la institución de que se trate. Puede incluir lugares alternativos de procesamiento, en otra empresa, dentro o fuera del país, rutinas iguales o diferentes de procesamiento o subsistemas básicos.

Es frecuente que no existan planes de contingencia y entonces ante una falla no prevista, los funcionarios no saben qué hacer, desconocen los procedimientos que deben ejecutar y la situación problemática se vuelve más grave, ya que a la tensión existente se agregan errores de operación, por falta de especificaciones.

Es fundamental que exista para todo sistema informático un plan de contingencia que especifica qué hacer en caso de ocurrir un desastre.

2.2. DEFINICIÓN DE UN MODELO DE ARQUITECTURA DE INFORMACIÓN

En esta fase se realizará un análisis de los datos de manera que se defina la información de mayor importancia manejada por la empresa, que sea la más sensible y afecte en caso de fallo y pérdida.

2.2.1. RECOPIACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

Se puede recopilar información mediante entrevistas y encuestas para conocer los datos más importantes manejados dentro del negocio.

La recolección de la información involucra algún tipo de monitoreo, donde el objetivo de la misma es averiguar qué datos son los más importantes así como su ubicación para la realización de una buena planificación, como un correcto plan de respaldos para prevenir futuros incidentes que puedan afectar la calidad del servicio del negocio.

Los administradores de sistemas deben tener un buen entendimiento de sus sistemas, usuarios y aplicaciones los cuales deben ser capaces de clasificar y agrupar rápidamente su información en diferentes categorías.

Sin embargo, de no tener esa facilidad de entendimiento se clasificará la información en las siguientes categorías:

1. Sistema operativo

Estos datos cambian durante las actualizaciones, las instalaciones de reparaciones de errores y cualquier modificación específica.

2. Software de aplicaciones

Los datos cambian cuando se instalan, actualizan o eliminan aplicaciones.

3. Datos de aplicaciones

Los datos de aplicaciones (Directorio de datos de aplicaciones), dependiendo de la aplicación y su organización los cambios pueden ser frecuentes.

4. Datos de usuarios

Estos datos (Directorios de datos) cambian de acuerdo al uso de sus usuarios.

Basándose en estas categorías se debe tener una buena idea relacionada a la naturaleza de los respaldos que se necesitan para proteger sus datos.

2.2.2. PROCESAMIENTO DE INFORMACIÓN

Una vez que la información ha sido recolectada el siguiente paso es procesarla y generara un reporte con los datos precisos y necesarios con el cual se desarrollara el plan de respaldos así como la planificación.

Las preguntas claves que deben ser respondidas son:

- ✓ ¿Cuál son los datos más críticos dentro del negocio?
- ✓ ¿Cuál es el tamaño en disco de los datos?
- ✓ ¿Cuál es la ubicación de los datos más críticos?
- ✓ ¿Cuál es el tamaño de crecimiento de información?

2.2.3. ANÁLISIS DE LA INFORMACIÓN

Habilidades y experiencia son requeridas para llevar a cabo el análisis de la información que la recolección y el procesamiento. Lo esperado durante esta actividad es una validación, contra las metas y objetivos, donde es importante buscar respuestas a las siguientes preguntas.

- ✓ ¿Las operaciones se encuentran acorde al plan de respaldos?
- ✓ ¿Los objetivos están definidos dentro de los SLAs?
- ✓ ¿Existen acciones correctivas requeridas?
- ✓ ¿Existen tendencias?

Las tendencias deben ser periódicas y no solamente en un punto en el tiempo.

2.2.4. PRESENTACIÓN Y UTILIZACIÓN DE LA INFORMACIÓN

Esta etapa involucra la presentación de la información en un formato que sea entendible, al nivel adecuado, entregando valor de manera que permita a aquellos que la reciban tomar decisiones estratégicas, tácticas y operativas que se describen en el Anexo 2 PRESENTACIÓN Y UTILIZACIÓN DE LA INFORMACIÓN.

2.2.5. RIESGOS EN SISTEMAS DE INFORMACIÓN

Como la información y los datos son de vital importancia para los negocios muchas empresas se preocupan únicamente en las ganancias obtenidas por sus actividades y dejan que el almacenamiento y respaldo de su información sea administrado por un computador pobremente armado en hardware y software.

Principalmente por esta razón es necesario respaldar la información importante.

La pérdida de información provoca un daño de fondo como pérdida de oportunidades de negocio, clientes decepcionados, prestigio, entre otros.

La tecnología no está libre de errores y los respaldos son utilizados como un procedimiento de contingencia en caso de que una falla o error se presente. Las interrupciones informáticas se presentan de diferentes formas tales como: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones y muchas más. Y aunque no se pueda prevenir cada una de estas situaciones, la empresa sí puede prepararse para evitar las consecuencias que éstas puedan tener sobre su negocio y del tiempo que tarde en reaccionar y volver a su estado operativo normal.

El presente caso se plantea para la aplicación de COBIT 5 tomando en cuenta la descripción, objetivos y datos de la empresa.

La cascada de metas es importante, porque permite definir prioridades para la implementación, mejora y aseguramiento del gobierno de TI corporativa basada en metas (estratégicas) de la empresa y el riesgo relacionado. En este documento obtendremos una guía de referencia detallada de los procesos que están definidos en el modelo de procesos de referencia y guías de catalizadores de COBIT 5, estas incluyen un mapeo entre metas TI y procesos COBIT 5 como se muestra a continuación:

2.2.5.1. MAPEAR LOS OBJETIVOS DEL NEGOCIO CON LAS METAS CORPORATIVAS DE COBIT 5

Define metas y objetivos pertinentes y tangibles a varios niveles de responsabilidad de la empresa.

2.2.5.2. MAPEAR LAS METAS CORPORATIVAS DE COBIT 5 Y LAS METAS RELACIONADAS CON LAS TI

Filtra la base de conocimiento de COBIT 5, basada en metas corporativas, para extraer orientación pertinente a incluir en proyectos específicos de implementación, mejora o aseguramiento.

2.2.5.3. MAPEAR LAS METAS RELACIONADAS CON LAS TI CON LOS PROCESOS DE COBIT 5

Para cada catalizador se puede definir un conjunto de metas específicas y relevantes en apoyo a las metas TI. Se proporcionan metas en las descripciones detalladas del proceso.

2.2.5.4. MAPEAR PROCESOS DE COBIT 5 CON RIESGOS IDENTIFICADOS

Aquí se proporciona una referencia de proceso que representa todos los objetivos encontrados en la empresa, respecto a las actividades de TI, ofreciendo un modelo de referencia común entendible para gerentes de la parte operativa de TI y de negocio. El modelo de procesos propuesto es completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica.

Este esquema basado en mapeos y tablas provistas por COBIT 5, es aplicable a toda organización y puede ser un excelente lineamiento y guía orientadora para poder establecer un vínculo coherente y consistente para traducir las Necesidades de los Stakeholders del Negocio y los Procesos propios de TI.

Como la información es el activo más importante junto con el uso de las tecnologías relacionadas para las empresas, se debe garantizar la seguridad en todos los niveles para fomentar la confianza de los dueños y clientes de la empresa. Por tanto, mediante COBIT 5 se puede identificar, analizar, reducir o mitigar los riesgos a través de la adecuada administración de la seguridad.

Si bien se ha descrito de los beneficios que COBIT 5 puede traer a la empresa, esta vez el enfoque está dirigido a una apropiada gestión de respaldos de información. La esencia de COBIT 5 para seguridad de la información reside en ayudar a la empresa a reducir sus perfiles de riesgo a través de la adecuada administración. Esta última guía enriquece la familia del reconocido marco de trabajo y ofrece una orientación adicional, permitiendo a los operadores de la empresa contar con conocimientos calificados en gestión de respaldos de información y principalmente asegurar la continuidad del negocio.

La gestión de la información y la tecnología son temas amplios y complejos, de modo que el presente trabajo se enfoca en una parte de la gestión de respaldos mediante COBIT 5.

CAPITULO 3: IMPLEMENTACIÓN DEL PROTOTIPO EN EL CASO DE ESTUDIO

3.1. DESCRIPCIÓN DEL CASO DE ESTUDIO

3.1.1. DESCRIPCIÓN DE LA COMPAÑÍA “YAKINDU CIA. LTDA”

Yakindu Cia. Ltda.: Es una empresa consultora ecuatoriana que cuenta con un equipo profesional de amplia experiencia a nivel mundial. Especializado en el desarrollo de herramientas tecnológicas de última generación. Su equipo de trabajo crea soluciones de la más alta calidad y tiene un alto conocimiento en el manejo de las tecnologías de vanguardia en las plataformas: HTML, PHP, DRUPAL, WORDPRESS, ZICULA, JAVA, JOOMLA, PENTAHO.

3.1.2. ESTRUCTURA ORGANIZATIVA

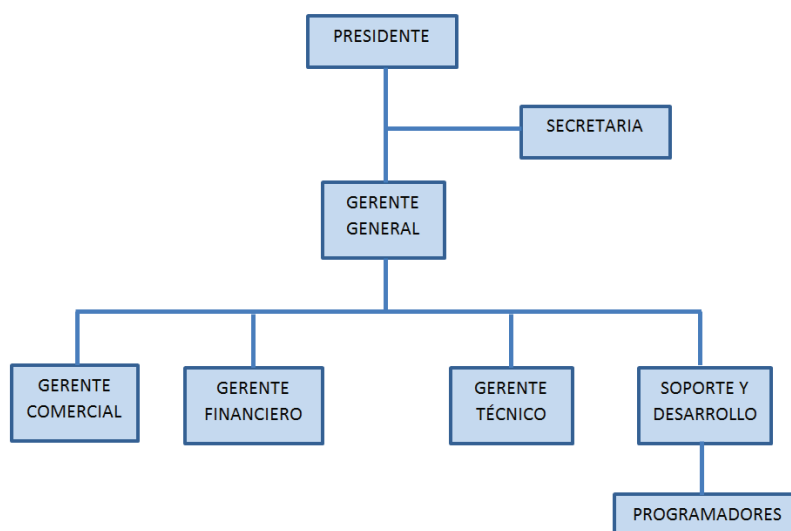


Figura 3-1 Estructura Organizativa

3.1.3. SERVICIOS

- **Desarrollo de aplicaciones de Software**

Yakindu Cia. Ltda. desarrolla aplicaciones que se adaptan perfectamente a la manera de entender el negocio de sus clientes. Se trata de soluciones y herramientas útiles que ayudarán a realizar la actividad profesional.

El Software se realiza a medida, por lo tanto siempre atenderá las necesidades reales del trabajo ya que automatiza un proceso o procesos del negocio ayudando a mejorar su función. Todo el potencial de las aplicaciones de se lo puede realizar tanto en aplicaciones de escritorio como en desarrollos sobre plataforma web.

El desarrollo de software presenta numerosos beneficios, ya que sustituyen el trabajo manual en los trabajos operacionales. Por otra parte fomentar el uso de una aplicación amplia ha respaldado el camino de las empresas hacia un mejor futuro donde se crean nuevas oportunidades de desarrollo nacional e internacional sosteniendo el uso del mismo de la mejor manera posible.

- **Soporte de aplicaciones de software**

Yakindu Cia. Ltda. cuenta con servicios de implementación y soporte de aplicaciones, que van desde la Consultoría de Procesos hasta el soporte funcional y la mejora continua de aplicaciones, pasando por la implementación y soporte técnico de todas las aplicaciones que sirve para ayudar a resolver los problemas que puedan presentarse a los usuarios, mientras hacen uso de servicios o aplicaciones.

3.1.4. TOPOLOGÍA DEL SISTEMA

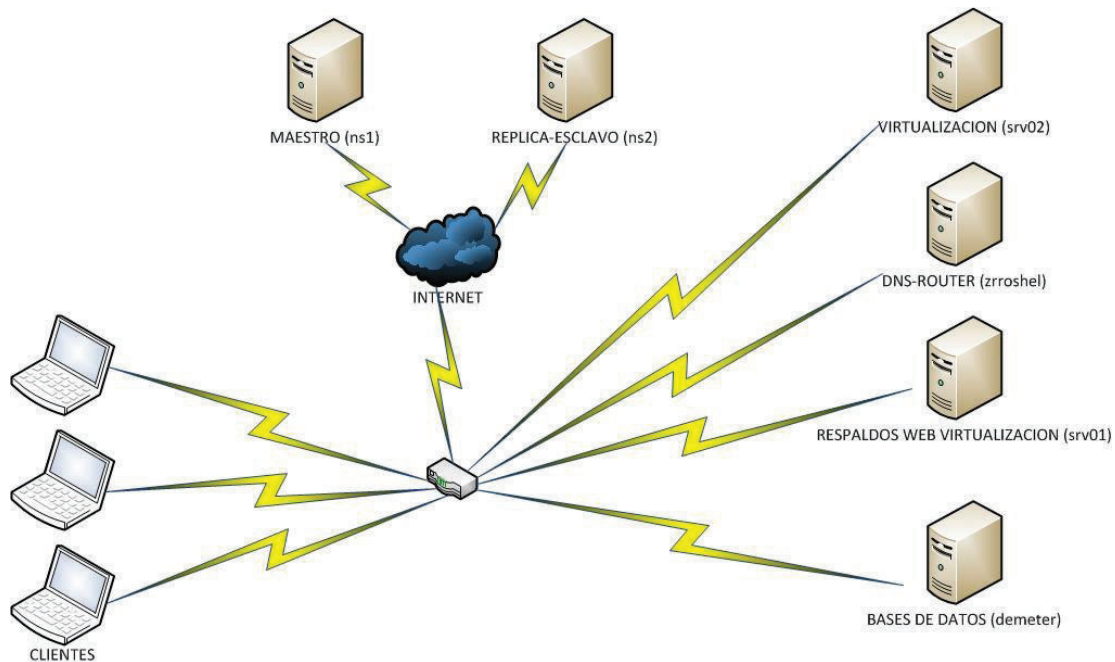


Figura 3-2 Topología del Sistema

3.1.5. SITUACIÓN ACTUAL DE TI DEL CASO DE ESTUDIO

La Gerencia de Tecnología e Información se encuentra compuesta por los siguientes departamentos:

La Gerencia de Tecnología con Desarrollo y Soporte abarca las siguientes funciones:

- ✓ Soporte Tecnológico.
- ✓ Desarrollo Tecnológico.
- ✓ Administrador de Base de Datos.
- ✓ Jefatura de Redes e Infraestructura.

Estos departamentos manejan la información más sensible de la empresa así como de sus clientes, los cuales no manejan una gestión segura ni algún tipo de proceso que ayude con sus funciones.

3.1.5.1. SITUACIÓN ACTUAL DE LOS RESPALDOS DEL CASO DE ESTUDIO

El procedimiento de respaldos actual de la empresa Yakindu. Cia. Ltda. consiste en efectuar respaldos cada semana de los servidores más importantes del interés de su negocio como base de datos y desarrollo de aplicaciones, cabe mencionar que los respaldos los realiza el jefe técnico manualmente a disco, los cuales son realizados por seguridad en horas que no afecte la productividad de la empresa.

Es necesario mencionar que la empresa no sigue ningún proceso o alguna metodología de respaldos para su protección, por lo que se ve en la necesidad de desarrollar una planificación de respaldos así como un plan de contingencia en caso de pérdida de información.

3.1.5.2. PROBLEMAS E INCIDENTES

- ✓ Falta de administración de red que deriva en problemas estructurales, de configuración, monitoreo, centro de cómputo, infraestructura y seguridad de la red.
- ✓ Falta de un plan de respaldos.
- ✓ Falta de metodologías y herramientas adecuadas para la realización y manejo de respaldos.
- ✓ Falta de políticas de manejo de la criticidad de la información.

3.1.5.3. TIPOS DE SEGURIDAD DE ACCESO

1. Gestión de accesos de usuario.
2. Existen equipos firewall con reglas de protección básicas.
3. Control de cambios en las aplicaciones internas.

3.1.5.4. PROCESOS Y PROCEDIMIENTOS

Los procesos no se encuentran documentados, como manuales, descriptivo de funciones, histórico de incidentes, base de conocimientos dentro del área de TI.

El procedimiento de control de cambios dentro del área de desarrollo se encuentra desarrollado por el jefe de departamento técnico.

3.2. POLÍTICAS DE RESPALDO DE INFORMACIÓN

El presente documento tiene como finalidad dar a conocer las políticas o estándares de respaldos de información que deberán ser observados por los usuarios y responsables de los servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información del caso de estudio para determinarlo aplicamos el modelo desarrollado en el [CAPÍTULO 2](#).

3.2.1. OBJETIVOS GENERALES

Definir e implementar un modelo de respaldos de información en la empresa Yakindu. Cia. Ltda. empleando herramientas de software libre.

3.2.2. OBJETIVOS ESPECÍFICOS

- ✓ Analizar la situación actual de la empresa Yakindu Cia. Ltda.
- ✓ Definir los requerimientos necesarios en cuanto a la planificación e implementación de respaldos de información.
- ✓ Proponer un modelo de respaldos de información para la empresa Yakindu Cia. Ltda. basado en las mejores prácticas.
- ✓ Implementar el modelo de respaldos de información propuesto empleando herramientas de software libre.
- ✓ Evaluar el modelo implementado.

3.2.3. DESARROLLO DEL MODELO DE PLAN DE RESPALDOS

EL Plan de Respaldos de Datos se desarrollara de acuerdo a las necesidades del caso de estudio para salvaguardar, defender y proteger la información, siguiendo los pasos puestos a continuación:

3.2.3.1. IMPORTANCIA DE LA INFORMACIÓN

Existen datos muy sensibles para la continuidad del negocio de la empresa los cuales serán indicados a continuación:

3.2.3.1.1. DESARROLLO DEL MODELO DE ARQUITECTURA DE INFORMACIÓN

TIPO DE INFORMACIÓN QUE SE RESPALDA

De acuerdo al respectivo análisis y dependiendo de las características de cada fragmento de información se determinará los datos más importantes y críticos además el mecanismo, periodicidad y tecnología de respaldo utilizada para resguardarla en el tiempo.

RECOPIACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

La recopilación de información se la realizó con entrevistas al jefe técnico, los integrantes del área de soporte, desarrollo y el administrador de base de datos quienes dieron a conocer los datos más importantes que maneja la empresa los cuales por motivos de seguridad y solicitud del jefe técnico no se detallara en el documento como direcciones IPs o clientes.

PROCESAMIENTO DE INFORMACIÓN

En primer lugar se puede ver que los datos se encuentran muy bien organizados dentro de su servidor específico tanto en bases de datos, aplicaciones, servidor SVN, entre otros, varios de los cuales se encuentran virtualizados como se puede visualizar en la topología de red que la empresa posee.

Con la información ya recolectada precedemos a procesarla:

✓ ¿Cuál son los datos más críticos dentro del negocio?

La información más crítica contemplada en la empresa son las aplicaciones web y base de datos de sus clientes ya que no podrían funcionar si se produjera algún inconveniente, también es importante el servidor SVN.

Tomando en cuenta la clasificación de la información y el conocimiento de los administradores de los sistemas, los datos están tomados en cuenta a nivel de aplicación ya que todos los sistemas operativos son Linux.

1. Base de datos: se manejan base de datos de los clientes así como información propia de la empresa, se utiliza MySQL y Postgress.
2. Aplicaciones: existen varios servidores de aplicaciones los cuales constan de servidores web como Apache, en los cuales se debe hacer énfasis ya que es importante su correcto funcionamiento para sus clientes.
3. Servidor Svn: este servidor guarda el desarrollo de aplicaciones diario que se realiza en la empresa por lo que es muy necesario su respaldo diario en caso de negligencias o por una mala realización del proceso.

✓ **¿Cuál es el tamaño en disco de los datos?**

Detallaremos el tamaño en disco de los datos más críticos en cada servidor:

1. Bases de datos:

SERVIDOR	TAMAÑO
MySql	11 GB
Postgress	16 GB

Tabla 3-1 Tamaño de Servidor de Base de Datos

2. Aplicaciones

SERVIDOR	TAMAÑO
Server52	96 GB
Server57	20 GB
Httpdold	5 GB

Tabla 3-2 Tamaño de Servidor de Aplicaciones

3. Servidor SVN

SERVIDOR	TAMAÑO
SVN	46 GB

Tabla 3-3 Tamaño de Servidor de SVN

✓ ¿Cuál es la dirección y fileserver de los datos más críticos?

1. Bases de datos:

SERVIDOR	IP	FILESERVER
MySql	192.168.X.X	/var/lib/mysql
Postgress	192.168.X.X	/var/lib/postgress

Tabla 3-4 Datos de Servidor de Base de Datos

2. Aplicaciones:

SERVIDOR	IP	FILESERVER
Server52	192.168.X.X	/var/www/sitio1
		/var/www/sitio2
		/var/www/sitio3
Server57	192.168.X.X	/var/www/sitio1
		/var/www/sitio2
Httpdold	192.168.X.X	/var/www

Tabla 3-5 Datos de Servidor de Aplicaciones

3. Servidor SVN:

SERVIDOR	IP	FILESERVER
SVN	192.168.X.X	/var/www/svn

Tabla 3-6 Datos de Servidor SVN

✓ **¿Cuál es el tamaño de crecimiento de información?**

De acuerdo a la información brindada se puede determinar que el crecimiento de los datos es aproximadamente de 1 GB mensual.

SERVIDOR	TAMAÑO	TAMAÑO	TAMAÑO
MySql	9.45 GB	10.24 GB	11 GB
Postgress	14.12 GB	15 GB	16 GB
Server52	94 GB	95 GB	96 GB
Server57	18.38 GB	19.23 GB	20 GB
Httpdold	4.23 GB	4.61 GB	5 GB
SVN	43.80 GB	45 GB	46 GB

Tabla 3-7 Crecimiento de la Información de Servidores

ANÁLISIS DE LA INFORMACIÓN

Habilidades y experiencia son requeridas para llevar a cabo el análisis de la información obtenida con la recolección y el procesamiento. Lo esperado durante esta actividad es una verificación, contra las metas y objetivos, donde es importante buscar respuestas a las siguientes preguntas.

✓ **¿Las operaciones se encuentran acorde al plan de respaldos?**

La empresa no posee ninguna planificación de respaldos para salvaguardar su información, únicamente realizan operaciones manuales de respaldos considerados por el jefe técnico importantes, estas son las bases de datos.

✓ **¿Los objetivos están definidos dentro de los SLAs?**

Los objetivos necesarios de nuestro proyecto deben estar cubiertos por el punto de las provisiones de seguridad y datos. Basándose en la información recopilada se entiende que no cumplen con los objetivos establecidos ya que

es muy necesario contar con el plan de respaldos y un plan de contingencia en caso de desastre.

✓ **¿Existen acciones correctivas requeridas?**

Se requiere varias acciones dentro del caso de estudio, el más importante, el tema tratado dentro del proyecto para salvaguardar la información crítica que maneja la empresa, así como definir los procesos necesarios para un mejor manejo de los recursos.

✓ **¿Existen tendencias?**

Las tendencias del caso de estudio es lo contenido con la información, ya que el trabajo diario realizado por los empleados debe ser respaldado así como la información de los clientes que es muy necesario como también que sus aplicaciones se encuentren en funcionamiento.

PRESENTACIÓN Y UTILIZACIÓN DE LA INFORMACIÓN

PREGUNTAS	SI	NO	N/A
¿La empresa posee datos críticos dentro del negocio?		x	
¿Cuenta con inventarios de Hardware y Software?	x		
¿Cuenta la empresa con un plan de respaldos?		x	
¿Cuenta la empresa con un plan de contingencia?		x	
¿La empresa cuenta con un sistema automatizado de respaldos?		x	
¿Tiene un responsable la gestión de respaldos?		x	
¿Actualmente hay algún manual o instructivo de los procesos manejados para la realización de respaldos?		x	
¿Están preparados para una eventualidad, catástrofe o error?		x	

¿Cuentan con una bitácora para mantener registros de los respaldos realizados?		x	
¿Existe una revisión periódica de los activos de la empresa?	x		
¿Se verifica el crecimiento de los datos en los servidores?	x		
En caso de resguardo de información, ¿Se custodian en algún lugar seguro?		x	
¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?		x	
¿Existe un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software?		x	

Tabla 3-8 Presentación y utilización de la información

La empresa no presentó ninguna evidencia documentada de registro de información de sus procedimientos, únicamente se levantó la información y se dio a conocer que el Jefe técnico realiza los respaldos manualmente de las bases de datos semanalmente sin un horario definido.

RIESGOS EN SISTEMAS DE INFORMACIÓN

Los riesgos en sistemas de información comúnmente se ve como una función técnica encomendada a expertos en tecnologías de la información, en el caso de estudio la función se encuentra ejercida por el Jefe técnico, quien muestra el sistema de actividad humana de la dirección estratégica de tecnologías de información, descripción de las actividades y métodos propuestos.

La empresa cuenta con una infraestructura muy bien planificada con los niveles de seguridad requeridos para la protección física de su información, pero no cuenta con un sistema automatizado de respaldos ni planes de contingencia en caso de desastres, lo cual es un riesgo vital a la continuidad del negocio.

MAPEAR LOS OBJETIVOS DEL NEGOCIO CON LAS METAS CORPORATIVAS DE COBIT 5

Se escogen las metas corporativas de COBIT 5 de acuerdo al objetivo del negocio determinado por la empresa, en este caso Implementar un modelo de respaldos de información en la empresa Yakindu Cia. Ltda.

Mapeo de los Objetivos del Negocio con las Metas Corporativas de COBIT 5		OBJETIVOS DE NEGOCIOS
METAS CORPORATIVAS DE COBIT 5		Implementar un modelo de respaldos de información en la empresa Yakindu Cia. Ltda.
1.	Valor para las partes interesadas de las inversiones de negocio	
2.	Cartera de productos y servicios competitivos	
3.	Riesgos de negocio gestionados (salvaguarda de activo)	X
4.	Cumplimiento de leyes y regulaciones externas	X
5.	Transparencia financiera	
6.	Cultura de servicio orientada al cliente	
7.	Continuidad y disponibilidad del servicio de negocio	X
8.	Respuestas ágiles a un entorno de negocio cambiante	
9.	Toma estratégica de Decisiones basadas en información	
10.	Optimización de costes de entrega del servicio	
11.	Optimización de la funcionalidad de los procesos de negocio	
12.	Optimización de los costes de los procesos de negocio	
13.	Programas gestionados de cambio en el negocio	
14.	Productividad operacional y de los empleados	
15.	Cumplimiento con las políticas internas	X
16.	Personal entrenado y motivado	
17.	Cultura de innovación del producto y del negocio	

Tabla 3-9 Mapeo de los objetivos del negocio con las metas corporativas de COBIT 5

MAPEAR LAS METAS CORPORATIVAS DE COBIT 5 Y LAS METAS RELACIONADAS CON LAS TI

Con las metas corporativas ya determinadas las mapeamos con las metas relacionadas con las TI.

Mapeo de las Metas Corporativas de COBIT 5 y las metas relacionadas con las TI						
		Metas Corporativas				
		Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Continuidad y disponibilidad del servicio de negocio	Cumplimiento con las políticas internas	
		3.	4.	7.	15.	
Meta relacionada con las TI		Financiera	Cliente	Interna		
Financiera	4	Riesgos de negocio relacionados con las TI Gestionados	P	S	P	S
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	P	P	P	P

Tabla 3-10 Mapeo de las metas corporativas de COBIT 5 y las metas relacionadas con las TI

MAPEAR LAS METAS RELACIONADAS CON LAS TI CON LOS PROCESOS DE COBIT 5

Definimos los procesos de COBIT 5 identificados con las metas relacionadas con las TI.

Mapeo entre metas relacionados con las TI en COBIT 5 con procesos de COBIT 5					
			Meta relacionado con las TI		
			Riesgos de negocio relacionados con las TI gestionados	Disponibilidad de información útil y relevante para la toma de decisiones.	
			4	14	
Procesos de COBIT 5			Financiera	Interna	
Evaluar, Orientar y Monitorizar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S	S	
	EDM02	Asegurar la Entrega de Beneficios		S	
	EDM03	Asegurar la Optimización del Riesgo	P	S	
	EDM04	Asegurar la Optimización de los Recursos	S		
	EDM05	Asegurar la Transparencia hacia las partes interesadas		S	
Organizar Alinear, Planificar y	APO01	Gestionar el Marco de Gestión de TI	S	S	
	APO02	Gestionar la Estrategia	S	S	
	APO03	Gestionar la Arquitectura Empresarial	S	S	
	APO04	Gestionar la Innovación	S	S	
	APO05	Gestionar el Portafolio	S		

	APO06	Gestionar el Presupuesto			
		y los Costes	S		
	APO07	Gestionar los Recursos			
		Humanos	S		
	APO08	Gestionar las Relaciones	S		
	APO09	Gestionar los Acuerdos de Servicio	S	P	
	APO10	Gestionar los Proveedores	P	S	
	APO11	Gestionar la Calidad	S	S	
APO12	Gestionar el Riesgo	P	S	X	
APO13	Gestionar la Seguridad	P	P		
Implementación e Construcción, Adquisición e	BAI01	Gestionar los Programas y Proyectos	P		
	BAI02	Gestionar la Definición de Requisitos	S	S	
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S	S	
	BAI04	Gestionar la Disponibilidad y la Capacidad	S	P	
	BAI05	Gestionar la introducción de Cambios Organizativos			
	BAI06	Gestionar los Cambios	P	S	
	BAI07	Gestionar la Aceptación del Cambio y de la Transición	S	S	
	BAI08	Gestionar el Conocimiento		S	
	BAI09	Gestionar los Activos	S	S	
	BAI10	Gestionar la Configuración	S	P	
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones	P	S	
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio	P	S	
	DSS03	Gestionar los Problemas	P	P	
	DSS04	Gestionar la Continuidad	P	P	X
	DSS05	Gestionar los Servicios de Seguridad			
			S	S	
DSS06	Gestionar los Controles de los Procesos del Negocio		S		

Tabla 3-11 Mapeo entre las metas relacionadas con las TI con los procesos de COBIT 5

MAPEAR PROCESOS DE COBIT 5 CON RIESGOS IDENTIFICADOS

Mapear Procesos COBIT 5 con Riesgos Identificados				
			Procesos	
			Alinear, Planificar y Organizar	Entrega, dar servicio y Soporte
			Gestionar el Riesgo	Gestionar la Continuidad
			APO12	DSS04
Seguridad de la información	Falta de un individuo (Ejemplo: Director u Oficial de Seguridad de la Información) o función dedicada al manejo de la seguridad.	R1		
Protección de Privacidad y Datos	La falta de un programa global de privacidad aumenta el riesgo de incumplimiento con las disposiciones de privacidad específicas que deben ser establecidas por el Gobierno de TI.	R2		
Continuidad del Negocio	Existe un riesgo al no contar con un Plan de Continuidad de Negocios (PCN) establecido ya probado por el gobierno de TI y la junta directiva no se pueda garantizar la disponibilidad de los servicios de tecnología que mantienen el negocio.	R3	X	
Plan de recuperación de desastres.	Si no existe un Plan de Recuperación de Desastres la compañía se encuentra en el riesgo de perder información y no poder permitir la continuidad del negocio cuando se presente algún tipo de evento que ponga en riesgo los dispositivos de Hardware y software de la compañía.	R4		X
Gestionar Acuerdos de respaldo	Mantener la disponibilidad de la información crítica del negocio.	R5		X

Tabla 3-12 Mapeo de Procesos de COBIT 5 con riesgos identificados

CONTROLES

APO12 GESTIONAR EL RIESGO

Descripción del Proceso: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

Declaración del Propósito del Proceso: Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.²⁵

DSS04 GESTIONAR LA CONTINUIDAD

Descripción del Proceso: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

Declaración del Propósito del Proceso: Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.²⁶

Tomando en cuenta el objetivo del negocio de la empresa y la necesidad de mantener la continuidad del negocio, una de estas prácticas se relaciona con la Gestión de acuerdos de respaldos (DSS04.07) que tiene como propósito mantener la disponibilidad de la información crítica para el negocio, la cual se permitirá verificar los lineamientos del modelo a implementar cumple con las necesidades del negocio.

²⁵ COBIT5. AN ISACA Framework. Enabling.Processes.Español, Página 107

²⁶ COBIT5 AN ISACA Framework. Enabling.Processes.Español, Página 185

El control APO12 se lo menciona como una recomendación para la mejora de la empresa ya que se pueda garantizar la disponibilidad de los servicios de tecnología que mantienen el negocio.

DSS04.07 GESTIONAR ACUERDOS DE RESPALDO

1. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida, considerando:
 - Frecuencia (mensual, semanal, diaria, etc.)
 - Modo de copias de seguridad (por ejemplo, discos espejo para copias de seguridad en tiempo real frente a DVD-ROM para retenciones de larga duración)
 - Tipo de copias de seguridad (por ejemplo, completa frente a incremental)
 - Tipo de soporte
 - Copias de seguridad automatizadas en línea
 - Tipos de datos (por ejemplo, voz, óptica)
 - Creación de registros
 - Datos de cálculos críticos de usuario final (por ejemplo, hojas de cálculo)
 - Localización física y lógica de las fuentes de los datos
 - Seguridad y derechos de acceso
 - Cifrado
2. Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes. Considerar acuerdos de depósito (escrow).
3. Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.

4. Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP).
5. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente²⁷.

La figura 3.3 muestra el Lineamiento para la gestión de respaldos.

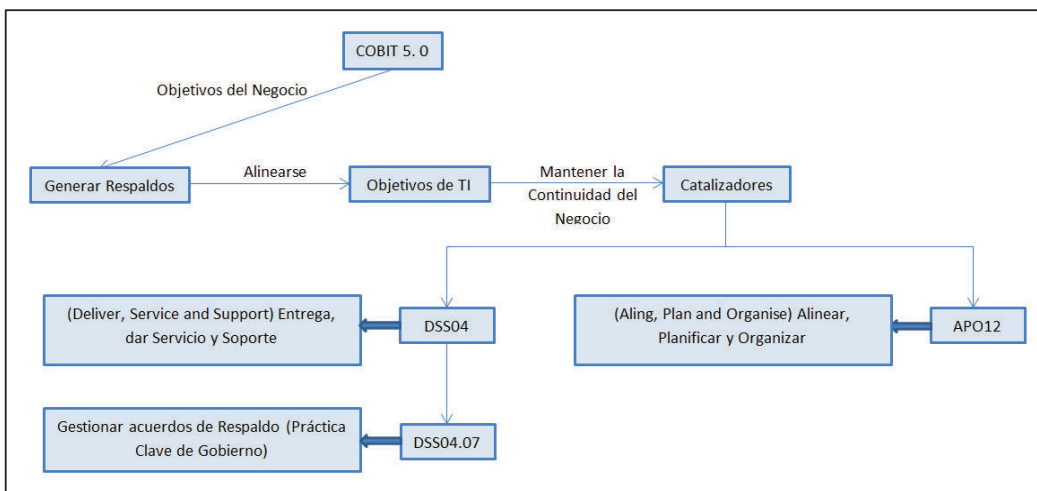


Figura 3-3 Lineamiento COBIT 5 para gestión de respaldos

Matriz RACI del Catalizador DSS04

En esta matriz se asigna el rol que el recurso debe desempeñar para cada actividad dada. No es necesario que en cada actividad se asignen los cuatro roles, pero sí por lo menos el de responsable (A) y el de encargado (R).

Matriz RACI DSS04																											
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Proprietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CSO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información	
DSS04.07																											
Gestionar acuerdos de respaldo.																											

Figura 3-4 Matriz RACI del Catalizador DSS04 Entregar, dar Servicio y Soporte

²⁷ COBIT5 AN ISACA Framework. Enabling.Processes.Español, Página 189

Roles asignados en el Catalizador DSS04.

ROL		DESCRIPCIÓN
C	Consultado	Este rol posee alguna información o capacidad necesaria para realizar la tarea.
A	Alta Responsabilidad	Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su responsable (R).
R	Responsable	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea; si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI.

Tabla 3-13 Roles del proceso DSS04

3.2.3.2. PLAN DE RESPALDOS

La importancia del plan de respaldos radica en que todos los dispositivos de almacenamiento masivo de información tienen la posibilidad de fallar, por lo tanto es necesario que se cuente con una copia de seguridad de la información importante, ya que la probabilidad de que 2 dispositivos fallen de manera simultánea es muy difícil.

De acuerdo a las necesidades de la empresa los respaldos deben ser automatizados con una herramienta de software libre en los cuales la información a respaldar será a nivel de archivos o datos.

El plan debe contener todos los ítems detallados a continuación con:

3.2.3.3. SELECCIÓN DE LA HERRAMIENTA DE AUTOMATIZACION Y SUS NECESIDADES

En esta fase se determinará el tipo de hardware y software indispensable para cumplir con los requerimientos de la solución de respaldos a usarse. Es importante indicar que la decisión es usar una herramienta especializada en lugar de desarrollarla, debido a que factores como tiempo, costo, y conocimientos específicos para desarrollo siempre serán mayores en este tipo de proyectos.

En el primer capítulo de este documento se determinó que la mejor herramienta puede ser Bacula, la cual cumple las necesidades del caso de estudio.

Yakindu Cia. Ltda. teniendo en cuenta la necesidad de implementar un sistema automatizado asignado a un servidor con grandes características de hardware y el uso de software libre, las cuales son:

Sistema Operativo: Centos 6.6

Tamaño en Disco: 8 TB

Tamaño en memoria: 8 GB

Procesador: Intel Core i5

Estas características son superiores al mínimo que necesita la herramienta para su uso, así que se realizara la implementación sin ningún inconveniente.

3.2.3.4. TIPOS DE RESPALDOS

Teniendo en cuenta la importancia de la información manejada por la empresa y capacidad de crecimiento se plantea realizar respaldos completos semanales y respaldos incrementales diarios los cuales se realizaran en horas no laborables para un mejor rendimiento.

El tiempo disponible para efectuar las copias de seguridad es importante, ya que la infraestructura manejada por la empresa, la grabación en disco y volumen de datos a almacenar, puede hacer que el proceso de grabación de los datos dure horas y teniendo en cuenta que mientras se efectúa el proceso es conveniente no realizar

accesos o modificaciones sobre los datos objeto de la copia, este proceso es muy necesario realizarlo en las noches y horas no laborables.

3.2.3.5. MEDIOS DE ALMACENAMIENTO A UTILIZAR

El jefe técnico asignó 8 TB en disco para la realización de respaldos, esta unidad será fija.

3.2.3.6. PLANIFICACIÓN DE RESPALDOS

Tomando en cuenta que los respaldos de información no obedecen ningún procedimiento pero es necesario la obtención de los mismos se plantea que los respaldos se deban realizar de forma automática por el programa de copia y según la configuración indicada en la Tabla 3.15, se podrá realizar diariamente y semanalmente a una hora concreta, cuando el sistema se encuentre por debajo de la media operacional y se acordó con el jefe técnico mantener una retención de un año de los respaldos.

Tomando en cuenta que la empresa empieza sus labores a las 9 horas y finaliza a las 18 horas se realizaron pruebas de su carga operacional en horas laborables y fuera de horas laborales, ver tabla 3.14, los datos tomados los podemos verificar en el Anexo 3 DATOS DE CARGA OPERACIONAL.

HORA	%CPU	%Uso Memoria
8:42	68.3	56
9:28	88.7	91
17:03	91.2	89
18:31	61.5	67

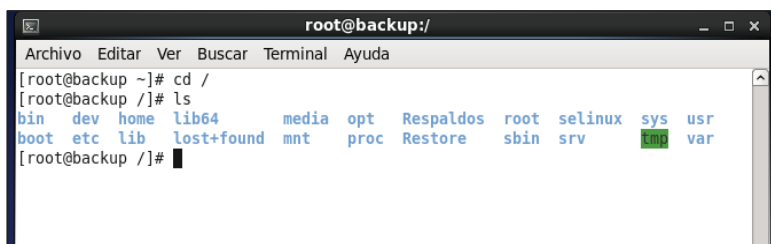
Tabla 3-14 Carga operacional del servidor de virtualización

# NODO	NODO	IP	OS	FILESYSTEM	TAMAÑO	BACKUP INCREMENTAL	BACKUP FULL	PROYECCION MENSUAL
1	SERVER52	192.168.100.52	CENTOS 6	/var/www/sitio1	96 GB	LUNES-VIERNES	SABADO	1 GB
				/var/www/sitio2		22h00	14h00	1 GB
				/var/www/sitio3		22h30	15h00	1 GB
2	SERVER57	192.168.10.57	CENTOS 6	/var/www/sitio1	20 GB	LUNES-VIERNES	SÁBADO	1 GB
				/var/www/sitio2		23h00	16h00	1 GB
3	SVN	192.168.100.55	CENTOS 6	/var/www/svn	46 GB	LUNES-VIERNES	SÁBADO	1 GB
4	HTTPDOLD	192.168.10.73	CENTOS 5	/var/www	3 GB	LUNES-VIERNES	SÁBADO	1 GB
5	MYSQL	192.168.10.54	CENTOS 7	/var/lib/mysql	11 GB	LUNES-VIERNES	SÁBADO	1 GB
6	POSTGRESS	192.168.100.58	CENTOS 7	/var/lib/postgress	16 GB	LUNES-VIERNES	SÁBADO	1 GB

Tabla 3-15 Planificación de Respaldos

3.2.3.7. RESTAURACIÓN DE DATOS

Como se ha dicho la restauración de datos es el tema más importante de una planificación de respaldos, para la empresa se ha determinado un espacio en disco para restauración de los datos que se realizaran bajo demanda en caso de que se lo requiera, el directorio asignado a disco para la restauración es /Restore en la dirección a disco 192.168.X.X los cuales se verificarán en las pruebas con la debida autorización del Jefe Técnico.



```
root@backup:/  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@backup ~]# cd /  
[root@backup /]# ls  
bin  dev  home  lib64  media  opt  Respaldos  root  selinux  sys  usr  
boot  etc  lib  lost+found  mnt  proc  Restore  sbin  srv  tmp  var  
[root@backup /]#
```

Figura 3-5 Directorio de Restauración de Archivos

3.2.4. POLITICAS DE RESPALDOS

1. El respaldo de información, debe realizarse exclusivamente en un servidor destinado para todas las actividades de respaldos.
2. El Área de Informática es la responsable de realizar un respaldo diario de las carpetas que contiene el Servidor de Archivos respaldo Incremental y guardar mensualmente en disco compacto la correspondiente a los tres últimos días de cada mes.
3. El Área Administrativa es la responsable de custodiar la copia del disco de respaldos.
4. El Área de Informática es la responsable de custodiar el respaldo mensual.
5. En caso de presentarse alguna falla al guardar la información del día, es responsabilidad del operador reportarla al Área de Informática. De no hacerlo, la pérdida de información será su responsabilidad.

6. Cuando un integrante de la Coordinación solicite disponer de información respaldada anteriormente, debe justificar por escrito al Coordinador las causas y la fecha del respaldo requerido.
7. Llevar un registro o bitácora de los respaldos que se realizan, así como también las eventuales recuperaciones.
8. Las claves de usuario NO serán respaldadas.
9. El administrador del sistema de respaldos deberá comprobar la confiabilidad del sistema de respaldo y recuperación de la información.
10. Verificar por lo menos una vez mes la integridad física del medio de respaldos.
11. Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la base de datos para así asegurar la integridad de la información respaldada.
12. Mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad y otros.
13. El estándar de etiquetas para los archivos de respaldo obtenidos por la herramienta de automatización debe indicar: tipo de respaldo, nombre del servidor, fecha del respaldo.
14. Cuando el espacio en el disco duro supere 1 TB es responsabilidad del Jefe técnico obtener el respaldo físico en discos y ubicarlos en un lugar fuera de la empresa y tenga un custodio.

3.2.5. PLAN DE CONTINGENCIA

En este plan se han identificado claramente los diferentes tipos de emergencia que pudieran acontecer en el desarrollo de las actividades del área de TI y cada uno de ellos tendrá un componente de respuesta y control.

Objetivo

El objetivo del Plan de Contingencia es establecer un procedimiento escrito, que indique la manera correcta de proceder ante una emergencia y establezca acciones operativas, responsabilidades para minimizar los riesgos, a fin de reducir significativamente el impacto negativo o pérdida que se pueda presentar.

3.2.5.1. FUNCIONES Y ORGANIZACIÓN SOBRE CONTINGENCIAS DEL MODELO

El poner en práctica el Plan de Contingencias debe ser el jefe Técnico quien tendrá la responsabilidad de ejecutar las acciones para hacer frente a las distintas contingencias que pudieran presentarse (accidentes laborales, incendios, entre otros) y se plantea que jefe técnico será el responsable de ejecutarlo.

El Plan de Contingencia también puede ser ejecutado por las personas a las que el jefe Técnico asigne y capacite como personal de apoyo.

3.2.5.1.1. FUNCIONES

COORDINACIÓN DE LA EMERGENCIA

Se encargara de manejar las comunicaciones con los medios informativos.

RESPUESTA ANTE EMERGENCIA

Asignar los recursos necesarios para la implementación de las medidas preventivas ante la ocurrencia de una emergencia. Informar a todos los departamentos afectados que se ha producido una emergencia.

LOGISTICA

En la Logística debe haber un responsable de proveer recursos, materiales, equipos. Necesarios para el control y mitigación de la contingencia.

OPERACIONES DE INTERVENCIÓN

Es la función de identificar y confirmar el grado de la emergencia, asegurar que todas las acciones de respuesta que deben realizarse con seguridad extrema para controlar y mitigar la emergencia con los recursos técnicos disponibles.

PLANEAMIENTO

Se evaluara los daños y se tomara las medidas correctivas a adoptar ante una emergencia y establecer las necesidades inmediatas que puedan darse durante el desarrollo de las actividades de mitigación.

COMUNICACIÓN

Tendrá a su cargo la definición del contenido y oportunidad de envío de la información referida al suceso, para su comunicación a las áreas afectadas e interesadas.

3.2.5.1.2. ORGANIZACIÓN SOBRE CONTINGENCIAS DEL MODELO

IDENTIFICACIÓN DE LAS PRINCIPALES CONTINGENCIAS

El data center de la empresa podría estar expuesta a diversas eventualidades y/o emergencias durante su operación, que pueden poner en riesgo los recursos. Bajo este contexto se han definido las posibles amenazas que pueden afectarla a fin de proponer una alternativa para controlar y/o mitigar sus efectos.

Para identificar las contingencias se establecieron los niveles de amenaza y vulnerabilidad de las actividades que se realizan.

De acuerdo al análisis de riesgos y la descripción del caso de estudio, se presentan las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta la red informática.

Para identificar las contingencias se hizo un listado de las amenazas y vulnerabilidades tomando en cuenta los riesgos identificados en los sistemas de información.

Se identificó los siguientes puntos:

- Cumplimiento
- Seguridad

Cumplimiento: Para mantener la integridad y confiabilidad de la información se cuenta con licenciamiento de Antivirus y paquetes de seguridad que consisten en asegurar que los recursos del sistema de información (material informático o programas) cumplan con el hecho de estar libres de peligro, daño o riesgo, de infección de virus informáticos.

Seguridad: el respaldo de información en servidores asegura que la información generada por las diferentes unidades administrativas, no se pierda y esté disponible en caso de desastre, o cualquier contingencia, como daño en los discos duros, o eliminación accidental de la Información o bien un caso de desastre natural.

NORMAS DE OPERACIÓN

- ✓ Los respaldos se harán diariamente después de las 18:00 horas.
- ✓ Los Respaldos de los servidores se realizan por día un diferencial y semana un full. En el caso de que no se puedan hacer los respaldos por algún problema con el Servidor (Virus o falla en unidad de almacenamiento) se procede a realizarlos al día siguiente.
- ✓ Se harán los respaldos diferenciales de lunes a viernes etiquetándolas con la fecha de respaldo.

- ✓ El respaldo full se los realizara los fines de semana etiquetándolas con la fecha de respaldo.

PLAN DE RECUPERACION

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, o desastre en el área de Informática.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

Las actividades a realizar en un Plan de Recuperación:

Actividades ante falla o desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de los activos de la información, que nos aseguren un proceso de Recuperación con el menor costo posible.

Plan de Acción

Se debe de establecer los procedimientos relativos a:

a) Equipos de Cómputo: Es necesario realizar un inventario actualizado de los equipos especificando su contenido (software y licencias que usa).

b) Obtención y almacenamiento de los Respaldos de Información: Se deberán establecer los procedimientos para la obtención de copias de:

- Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución del Software y/o Sistemas operativos que posee.
- Para lo cual se debe contar con respaldos del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

- RespalDOS del Software Base.

c) Políticas (Normas y Procedimientos de respaldos): Se debe establecer los procedimientos, normas, y determinación de responsabilidades, debiéndose incluir:

- Periodicidad de cada Tipo de respaldo (Semanal).
- Almacenamiento de los respaldos en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los respaldos en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje).
- Pruebas periódicas de los respaldos (Restauraciones), verificando su funcionalidad.
- El Respaldo se almacena por un año, la empresa en su área de Informática, se encarga de su resguardo.

PROCEDIMIENTO:

1. Todas las carpetas de los servidores deberán respaldarse periódicamente.
2. Todos los respaldos deberán conservarse conforme lo acordado con las áreas usuarias correspondientes.
3. Los respaldos se harán de acuerdo a las políticas de manejo y control de respaldos establecidos en este documento.
4. Todos los equipos centrales, bases de datos y sistemas informáticos deberán contar con planes de contingencia.
5. El usuario es responsable de los respaldos de los equipos personales.

3.3. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR.

Se utilizó el servidor provisto por la empresa Yakindu Cia. Ltda. la cual cuenta con las características necesarias para su uso.

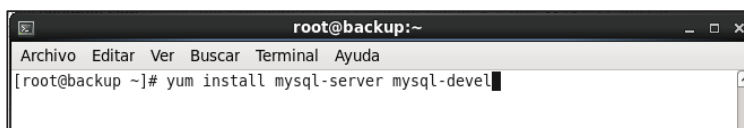
Se instaló un Centos 6.6, en el cual se configuro la ip 192.169.X.X, se descargaron los paquetes necesarios para su funcionalidad y se le asignó una contraseña robusta para su seguridad. Datos de configuración no se muestran por confidencialidad con la empresa.

3.3.1. PASO 1: INSTALACIÓN DEL SISTEMA OPERATIVO

Ver Anexo 4 INSTALACIÓN DEL SISTEMA OPERATIVO

3.3.2. PASO 2: INSTALACIÓN DEL SERVIDOR BACULA.

Bacula necesita una Base de Datos en este caso se instala mysql.



```

root@backup:~
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup ~]# yum install mysql-server mysql-devel

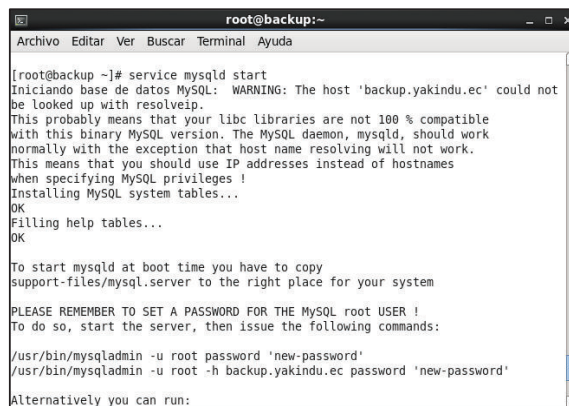
```

Figura 3-6 Instalación servidor Bacula

Iniciar servicio MySQL.

Comando: service mysqld start

Comando: chkconfig mysqld on



```

root@backup:~
Archivo Editar Ver Buscar Terminal Ayuda

[root@backup ~]# service mysqld start
Iniciando base de datos MySQL: WARNING: The host 'backup.yakindu.ec' could not
be looked up with resolveip.
This probably means that your libc libraries are not 100 % compatible
with this binary MySQL version. The MySQL daemon, mysqld, should work
normally with the exception that host name resolving will not work.
This means that you should use IP addresses instead of hostnames
when specifying MySQL privileges !
Installing MySQL system tables...
OK
Filling help tables...
OK

To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:

/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h backup.yakindu.ec password 'new-password'

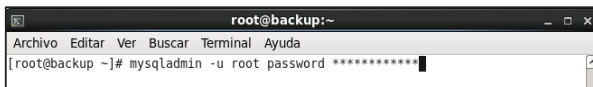
Alternatively you can run:

```

Figura 3-7 Configuración Mysql

Crear la contraseña de root para mysql.

Comando: `mysqladmin -u root password *****`



```

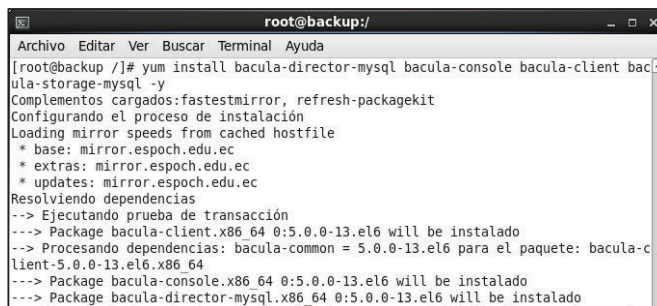
root@backup:~
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup ~]# mysqladmin -u root password *****

```

Figura 3-8 Contraseña Mysql

Con esta instrucción se instalará Bacula con todas sus herramientas para que funcione con MySQL.

Comando: `yum install bacula-director-mysql bacula-console bacula-client bacula-storage-mysql -y`



```

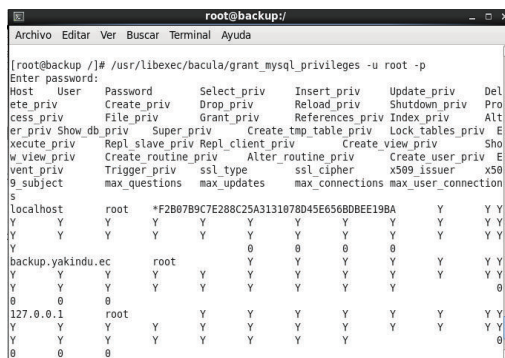
root@backup:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup /]# yum install bacula-director-mysql bacula-console bacula-client bacula-storage-mysql -y
Complementos cargados:fastestmirror, refresh-packagekit
Configurando el proceso de instalación
Loading mirror speeds from cached hostfile
* base: mirror.esPOCH.edu.ec
* extras: mirror.esPOCH.edu.ec
* updates: mirror.esPOCH.edu.ec
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Package bacula-client.x86_64 0:5.0.0-13.el6 will be instalado
--> Procesando dependencias: bacula-common = 5.0.0-13.el6 para el paquete: bacula-client-5.0.0-13.el6.x86_64
--> Package bacula-console.x86_64 0:5.0.0-13.el6 will be instalado
--> Package bacula-director-mysql.x86_64 0:5.0.0-13.el6 will be instalado

```

Figura 3-9 Instalación de herramientas Bacula

Luego ejecutar los siguientes comandos uno por uno para crear tablas de base de datos y necesarios para Bacula. Aquí "-u root" significa que Acceda con su cuenta root y "-p" significa preguntar por el password root mysql.

`# /usr/libexec/bacula/grant_mysql_privileges -u root -p`



```

root@backup:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup /]# /usr/libexec/bacula/grant_mysql_privileges -u root -p
Enter password:
Host      User      Password      Select_priv  Insert_priv  Update_priv  Delete_priv
Create_priv  Drop_priv    Reload_priv  Shutdown_priv
Process_priv File_priv    Grant_priv   References_priv
Index_priv  Alter_priv  Show_db_priv Super_priv   Create_tmp_table_priv
Lock_tables_priv
Execute_priv Repl_slave_priv
Repl_client_priv Create_view_priv Show_view_priv
Create_routine_priv
Alter_routine_priv Create_user_priv
Event_priv Trigger_priv
ssl_type      ssl_cipher   x509_issuer  x509_subject
max_questions
max_updates   max_connections
max_user_connections

localhost    root      *F2B07B9C7E288C25A3131078045E656B0BEE19BA
Y Y Y Y Y Y Y Y Y Y Y Y
Y Y Y Y Y Y Y Y Y Y Y Y
Y Y Y Y Y Y Y Y Y Y Y Y
Y Y Y Y Y Y Y Y Y Y Y Y
Y Y Y Y Y Y Y Y Y Y Y Y
0 0 0 0 0 0 0 0 0 0 0 0
127.0.0.1   root      Y Y Y Y Y Y Y Y Y Y Y Y
Y Y Y Y Y Y Y Y Y Y Y Y
Y Y Y Y Y Y Y Y Y Y Y Y
0 0 0 0 0 0 0 0 0 0 0 0

```

Figura 3-10 Privilegios Mysql

```
# /usr/libexec/bacula/create_mysql_database -u root -p
```

```
root@backup:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup /]# /usr/libexec/bacula/create_mysql_database -u root -p
Enter password:
Creation of bacula database succeeded.
[root@backup /]#
```

Figura 3-11 Creación Base de datos

```
# /usr/libexec/bacula/make_mysql_tables -u root -p
```

```
root@backup:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup /]# /usr/libexec/bacula/make_mysql_tables -u root -p
Enter password:
Creation of Bacula MySQL tables succeeded.
[root@backup /]#
```

Figura 3-12 Creación de tablas en Base de datos

```
# /usr/libexec/bacula/grant_bacula_privileges -u root -p
```

```
root@backup:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup /]# /usr/libexec/bacula/grant_bacula_privileges -u root -p
Granting MySQL privileges
Enter password:
Host      User      Password      Select_priv  Insert_priv  Update_priv  Del
ete_priv    Create_priv  Drop_priv    Reload_priv  Shutdown_priv Pro
cess_priv   File_priv    Grant_priv   References_priv Index_priv  Alt
er_priv Show_db_priv Super_priv   Create tmp_table_priv Lock tables_priv E
xecute_priv Repl_slave_priv Repl_client_priv Create view_priv Sho
w view_priv Create routine_priv Alter routine_priv Create user_priv E
vent_priv   Trigger_priv ssl_type     ssl_cipher   x509_issuer  x509
9_subject   max_questions max_updates  max_connections max_user_connection
S
localhost  root      *F2B07B9C7E288C25A3131078D45E656B0BEE198A  Y      Y      Y      Y      Y      Y      Y
Y          Y          Y          Y          Y          Y          Y          Y          Y          Y      Y
Y          Y          Y          Y          Y          Y          Y          Y          Y          Y      Y
Y          Y          Y          Y          Y          Y          Y          Y          Y          Y      0
0          0          0          0          0          0          0          0          0          0
127.0.0.1  root      Y          Y          Y          Y          Y          Y          Y          Y      Y
Y          Y          Y          Y          Y          Y          Y          Y          Y          Y      Y
Y          Y          Y          Y          Y          Y          Y          Y          Y          Y      0
0          0          0          0          0          0          0          0          0          0
```

Figura 3-13 Privilegios elementos de Bacula

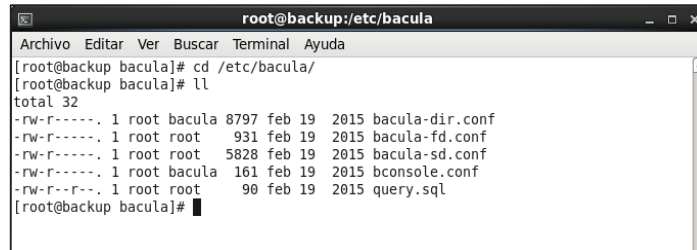
3.3.3. PASO 3: CONFIGURACIÓN BACULA

Una vez instalados todos los elementos de Bacula se procede a modificar los archivos de configuración necesarios para que las diferentes instancias de Bacula puedan interactuar entre sí.

En el directorio `/etc/bacula/`, se encuentran todos los archivos de configuración necesarios para poder configurar Bacula, estos archivos son:

- `bacula-dir.conf`, archivo de configuración de Bacula director.
- `bacula-sd.conf`, archivo de configuración del storage daemon.

- bacula-fd-conf, archivo de configuración de file daemon.
- bconsole.conf, consola para realizar respaldo



```

root@backup:/etc/bacula
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup bacula]# cd /etc/bacula/
[root@backup bacula]# ll
total 32
-rw-r-----. 1 root bacula 8797 feb 19 2015 bacula-dir.conf
-rw-r-----. 1 root root 931 feb 19 2015 bacula-fd.conf
-rw-r-----. 1 root root 5828 feb 19 2015 bacula-sd.conf
-rw-r-----. 1 root bacula 161 feb 19 2015 bconsole.conf
-rw-r--r--. 1 root root 90 feb 19 2015 query.sql
[root@backup bacula]#

```

Figura 3-14 Archivos configuración de Bacula

Configuración de Bacula Director:

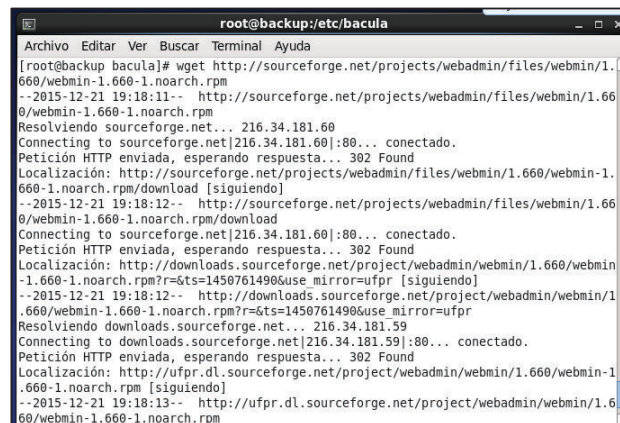
Ver Anexo 5 CONFIGURACIÓN DEL SERVIDOR BACULA

3.3.4. PASO 4: INSTALACIÓN Y CONFIGURACIÓN DE BACULA WEBMIN

Webmin es una interfaz basada en web para la administración del sistema de respaldo Bacula. El uso de cualquier navegador web moderno, puede configurar cuentas de usuario, Apache, DNS, compartir archivos y mucho más.

Descargar el paquete de instalación webmin:

wget <http://sourceforge.net/projects/webadmin/files/webmin/1.660/webmin-1.660-1.noarch.rpm>



```

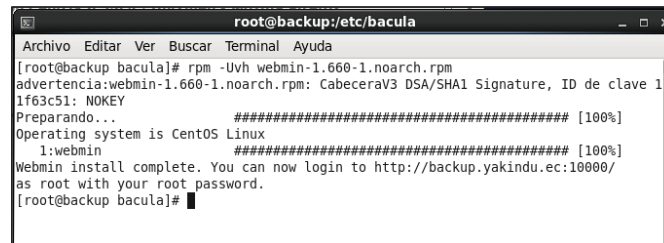
root@backup:/etc/bacula
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup bacula]# wget http://sourceforge.net/projects/webadmin/files/webmin/1.660/webmin-1.660-1.noarch.rpm
--2015-12-21 19:18:11-- http://sourceforge.net/projects/webadmin/files/webmin/1.660/webmin-1.660-1.noarch.rpm
Resolviendo sourceforge.net... 216.34.181.60
Connecting to sourceforge.net[216.34.181.60]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Localización: http://sourceforge.net/projects/webadmin/files/webmin/1.660/webmin-1.660-1.noarch.rpm/download [siguiendo]
--2015-12-21 19:18:12-- http://sourceforge.net/projects/webadmin/files/webmin/1.660/webmin-1.660-1.noarch.rpm/download
Connecting to sourceforge.net[216.34.181.60]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Localización: http://downloads.sourceforge.net/project/webadmin/webmin/1.660/webmin-1.660-1.noarch.rpm?r=sts=1450761490&use_mirror=ufpr [siguiendo]
--2015-12-21 19:18:12-- http://downloads.sourceforge.net/project/webadmin/webmin/1.660/webmin-1.660-1.noarch.rpm?r=sts=1450761490&use_mirror=ufpr
Resolviendo downloads.sourceforge.net... 216.34.181.59
Connecting to downloads.sourceforge.net[216.34.181.59]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Localización: http://ufpr.dl.sourceforge.net/project/webadmin/webmin/1.660/webmin-1.660-1.noarch.rpm [siguiendo]
--2015-12-21 19:18:13-- http://ufpr.dl.sourceforge.net/project/webadmin/webmin/1.660/webmin-1.660-1.noarch.rpm

```

Figura 3-15 Descarga paquete Webmin

Instalar el paquete descargado:

```
rpm -Uvh webmin-1.660-1.noarch.rpm
```

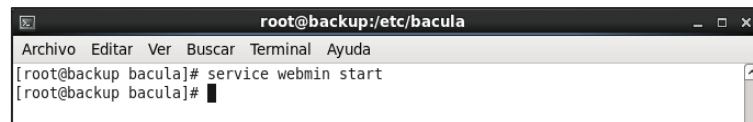


```
root@backup/etc/bacula
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup bacula]# rpm -Uvh webmin-1.660-1.noarch.rpm
advertencia:webmin-1.660-1.noarch.rpm: CabeceraV3 DSA/SHA1 Signature, ID de clave 1
1f63c51: NOKEY
Preparando... ##### [100%]
Operating system is CentOS Linux
1:webmin ##### [100%]
Webmin install complete. You can now login to http://backup.yakindu.ec:10000/
as root with your root password.
[root@backup bacula]#
```

Figura 3-16 Instalación paquete Webmin

Iniciar el servicio webmin:

```
service webmin start
```

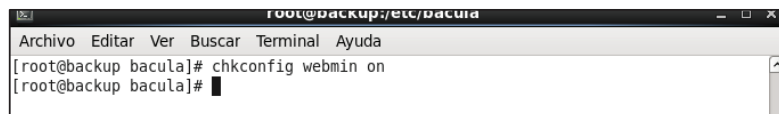


```
root@backup/etc/bacula
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup bacula]# service webmin start
[root@backup bacula]#
```

Figura 3-17 Iniciar servicio Webmin

Activar el servicio webmin:

```
chkconfig webmin on
```



```
root@backup/etc/bacula
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup bacula]# chkconfig webmin on
[root@backup bacula]#
```

Figura 3-18 Activar servicio Webmin

Para ingresar al portal Webmin:

<http://192.168.X.X:10000>



Figura 3-19 Portal Webmin Ingreso

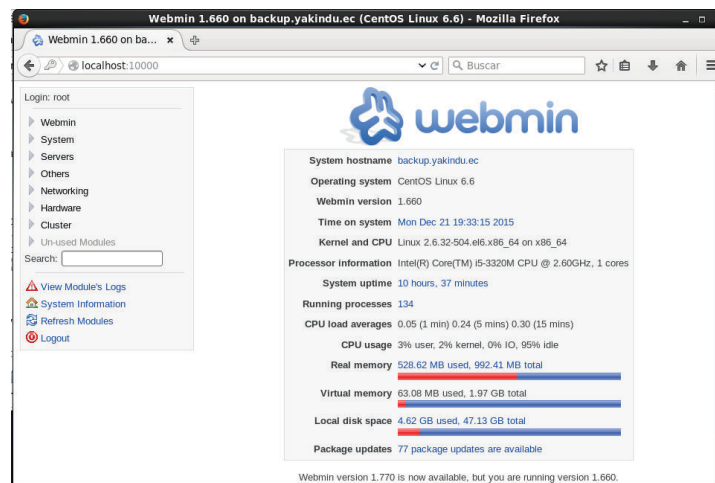


Figura 3-20 Portal Webmin

Configurar el portal webmin accediendo:

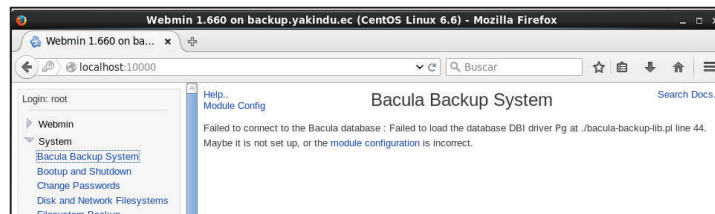


Figura 3-21 Inicio Portal Webmin

Agregamos la base de datos usada en este caso mysql con la clave de acceso:

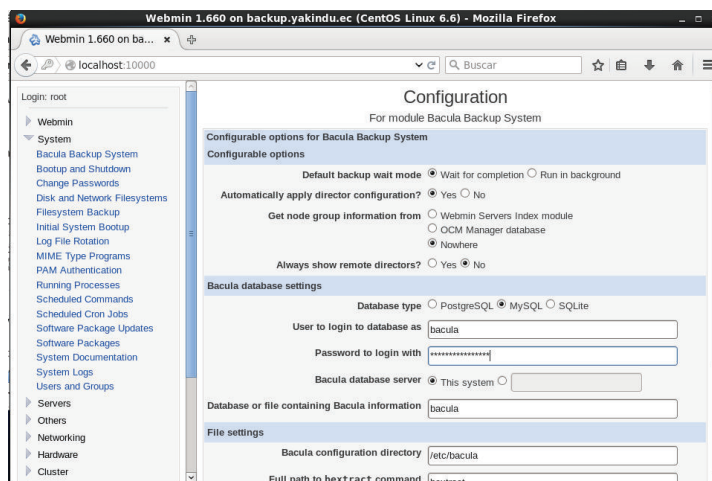


Figura 3-22 Configuración Base de datos

Desde el portal web es posible administrar Bacula de una manera sencilla y gráfica:

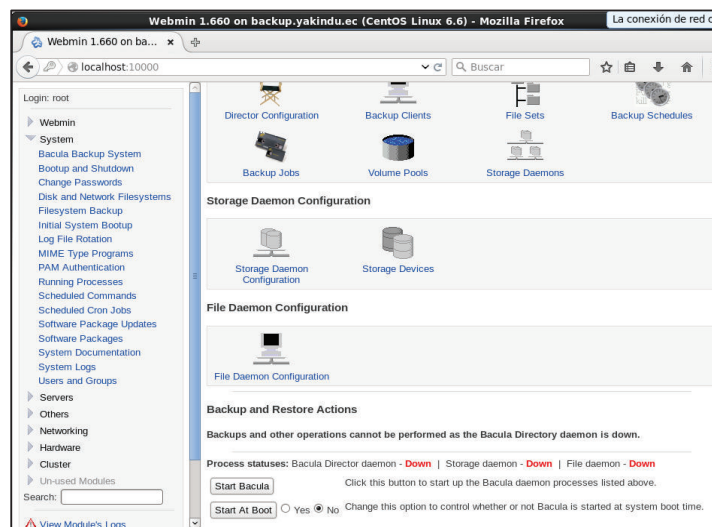


Figura 3-23 Elementos Bacula

3.4. INSTALACIÓN Y CONFIGURACIÓN DE LOS CLIENTES

Mediante este servicio (**bacula-fd**), Bacula obtiene los ficheros que necesita respaldar, éste es el componente que hay que instalar en las máquinas que necesiten respaldo. Realiza la función de **agente cliente**.

3.4.1. INSTALACIÓN Y CONFIGURACIÓN DE UN CLIENTE LINUX

Se instala el cliente Bacula y la consola con el comando siguiente:

yum -y install bacula-client bacula-console

```

root@httpdold:~# yum -y install bacula-client bacula-coonsole
Complementos cargados:fastestmirror, refresh-packagekit
Configurando el proceso de instalación
Determining fastest mirrors
 * base: mirror.cedia.org.ec
 * extras: mirror.cedia.org.ec
 * updates: mirror.cedia.org.ec
base                                     | 3.7 kB    00:00
extras                                  | 2.9 kB    00:00
updates                                 | 3.4 kB    00:00
No existe disponible ningún paquete bacula-coonsole.
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Package bacula-client.x86_64 0:5.0.0-13.el6 will be instalado
--> Procesando dependencias: bacula-common = 5.0.0-13.el6 para el paquete: bacula-client-5.0.0-13.el6.x86_64
--> Ejecutando prueba de Transacción
--> Package bacula-common.x86_64 0:5.0.0-13.el6 will be instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

```

Figura 3-24 Instalación Cliente Bacula

Editamos los archivos de configuración bacula-fd.conf y bconsole.conf.
vi bacula-fd.conf

```

root@httpdold:/etc/bacula
# List Directors who are permitted to contact this File daemon
#
Director {
  Name = bacula-dir.conf
  Password = "*****"
}
#
# Restricted Director, used by tray-monitor to get the
# status of the file daemon
#
Director {
  Name = bacula-dir.conf
  Password = "*****"
  Monitor = yes
}
#
# "Global" File daemon configuration specifications
#
FileDaemon {
  # this is me
  Name = 192.168.X.X
  FDport = 9102 # where we listen for the director
  WorkingDirectory = /var/spool/bacula
  Pid Directory = /var/run
  Maximum Concurrent Jobs = 20
}
# Send all messages except skipped files back to Director
Messages {
  Name = Standard
  director = bacula-dir = all, !skipped, !restored
}
-- INSERT --

```

Figura 3-25 Configuración Cliente Bacula

Configuración de la consola del cliente Bacula
vi bconsole.conf

```

root@httpdold:/etc/bacula
#
# Bacula User Agent (or Console) Configuration File
#
Director {
  Name = bacula-dir.conf
  DIRport = 9101
  address = localhost
  Password = "*****"
}

```

Figura 3-26 Configuración de consola Cliente Bacula

3.4.2. INSTALACIÓN Y CONFIGURACIÓN DE UN CLIENTE WINDOWS

Descargamos el cliente Bacula para Windows (dependiendo de la arquitectura que se está usando de 32 o 64 bits), en este caso **bacula-win32-5.2.3**.

Iniciar la instalación y aceptar los términos de licencia.

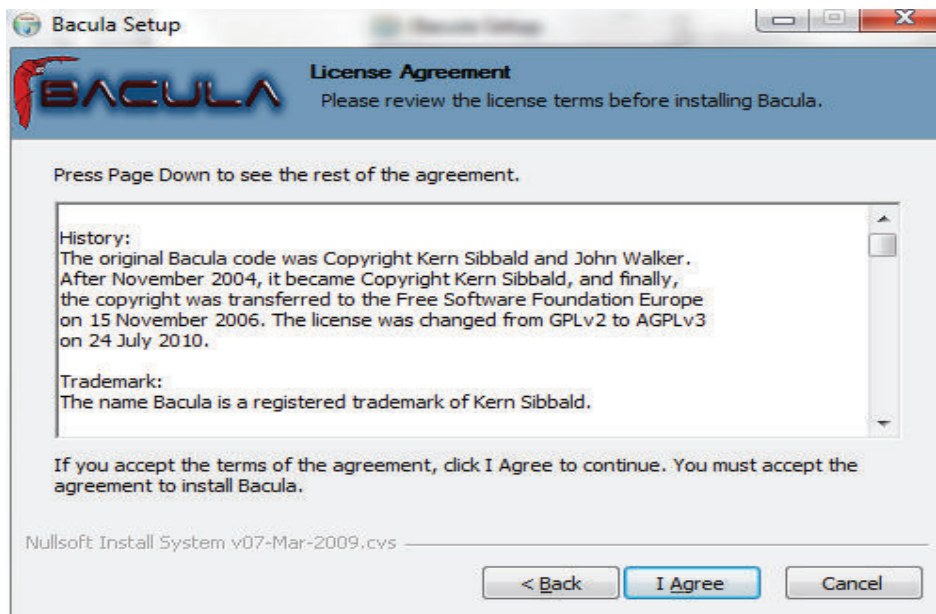


Figura 3-27 Instalación Cliente Bacula Windows

Escoger la instalación del cliente y consola, la documentación no es necesaria.

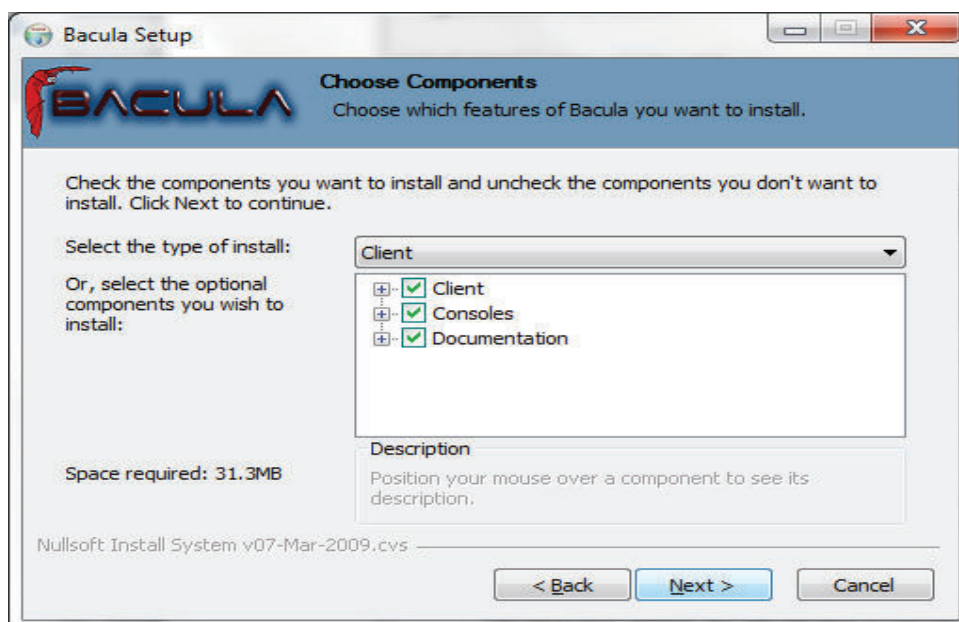


Figura 3-28 Escoge Elementos Cliente Bacula Windows

Agregamos los datos del director Bacula con el que va a comunicarse.

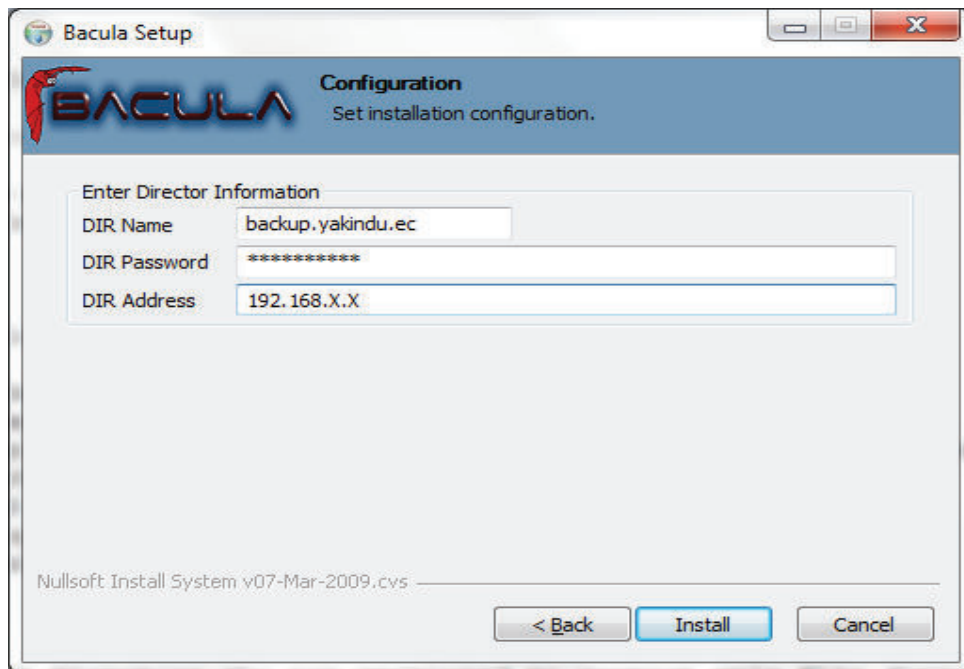


Figura 3-29 Configura datos servidor Bacula

Plantilla que contiene información del cliente y finalizamos.

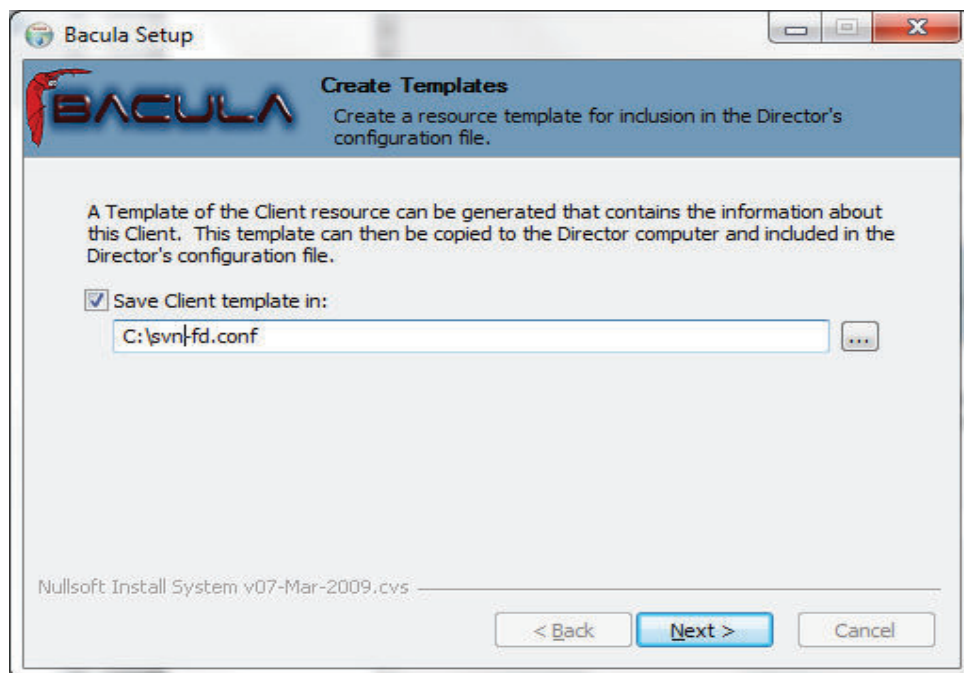


Figura 3-30 Configura nombre del cliente Bacula

3.5. CONFIGURACIÓN DE TAREAS PROGRAMADAS

Para configurar las tareas programadas se edita el archivo bacula-dir.conf en la función schedule de acuerdo a la Tabla 3.13 Planificación de Respaldos.

Schedule: Define cuando se va a ejecutar un trabajo y el tipo de copia que se va a hacer full, incremental o diferencial.

Name: nombre que se le asigna al recurso.

Run: configuración de la programación de la tarea puede ser incremental, full, diferencial.

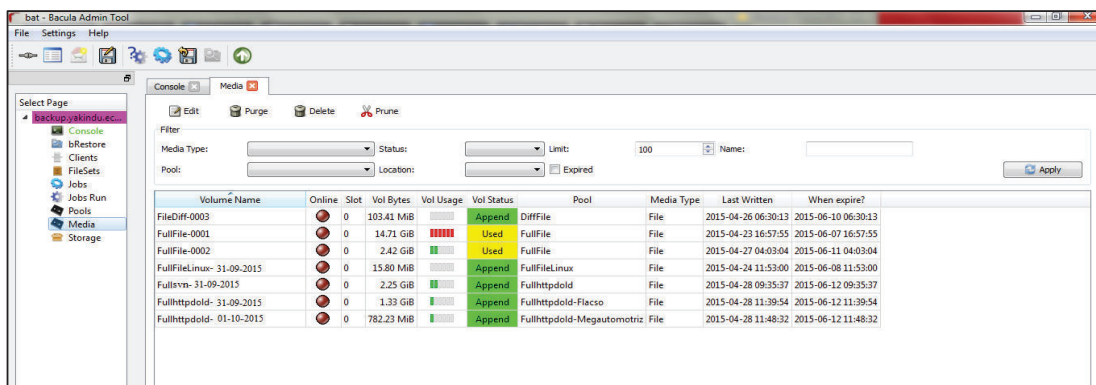
Ver Anexo 6 CONFIGURACIÓN DE LAS TAREAS PROGRAMADAS

3.6. PRUEBAS

Las pruebas del Modelo de Respaldos se realizan con el objetivo de verificar la funcionalidad de los procedimientos aplicados a la obtención de respaldos en la empresa, para lo cual se realizó pruebas de respaldo y restauración de la información.

RESPALDOS

Los respaldos se realizaron sin ningún inconveniente en los tiempos programados y podemos verificarlos en consola o vía web:



Volume Name	Online	Slot	Vol Bytes	Vol Usage	Vol Status	Pool	Media Type	Last Written	When expire?
FileDiff-0003	●	0	103.41 MiB		Append	DiffFile	File	2015-04-26 06:30:13	2015-06-10 06:30:13
FullFile-0001	●	0	14.71 GiB	■■■■■	Used	FullFile	File	2015-04-23 16:57:55	2015-06-07 16:57:55
FullFile-0002	●	0	2.42 GiB	■■■■■	Used	FullFile	File	2015-04-27 04:03:04	2015-06-11 04:03:04
FullFileLinux- 31-09-2015	●	0	15.80 MiB		Append	FullFileLinux	File	2015-04-24 11:53:00	2015-06-08 11:53:00
FullInro- 31-09-2015	●	0	2.25 GiB	■■■■■	Append	Fullhttpdold	File	2015-04-28 09:35:37	2015-06-12 09:35:37
Fullhttpdold- 31-09-2015	●	0	1.33 GiB	■■■■■	Append	Fullhttpdold-Flecco	File	2015-04-28 11:39:54	2015-06-12 11:39:54
Fullhttpdold- 01-10-2015	●	0	782.23 MiB	■■■■■	Append	Fullhttpdold-Megautomotriz	File	2015-04-28 11:48:32	2015-06-12 11:48:32

Figura 3-31 Respaldo de servidores

RESTAURACIÓN

La restauración de información es parte de los procedimientos que se deben aplicar para la definición del modelo de respaldos, por tal motivo el proceso definido para desarrollar las pruebas corresponden al proceso de restauración que se aplicará en la empresa.

La petición de restauración de información se la realizará mediante el formulario “Solicitud de Restauración”.

Para esta prueba restauramos el nodo httpdold y svn.

Solicitud de restauración httpdold.

SOLICITUD DE RESTAURACIÓN	
GESTION DE TECNOLOGÍA DE INFORMACIÓN	
+	
Solicitante:	Ing. Mario Morocho
Área:	Desarrollo
Gerencia:	Soporte y Desarrollo
Fecha de restauración:	17 de Noviembre de 2015

Datos de restauración:

Fecha del respaldo: 01 de Noviembre del 2015

Nombre del equipo: httpdold

Sistema operativo:

Linux

Windows

Detalle de información a restaurar:

Se requiere restaurar archivos de aplicación

Ing. Mario Morocho
SOLICITANTE

Ing. Byron Jumbo
JEFE TÉCNICO

Figura 3-32 Solicitud de restauración httpdold

Solicitud de restauración svn.

SOLICITUD DE RESTAURACIÓN	
GESTION DE TECNOLOGÍA DE INFORMACIÓN	
Solicitante:	Ing. Mario Morocho
Área:	Desarrollo
Gerencia:	Soporte y Desarrollo
Fecha de restauración:	17 de Noviembre del 2015

Datos de restauración:

Fecha del respaldo: _____ 31 de Octubre del 2015 _____

Nombre del equipo: _____ svn _____

Sistema operativo:

Linux

Windows

Detalle de información a restaurar:

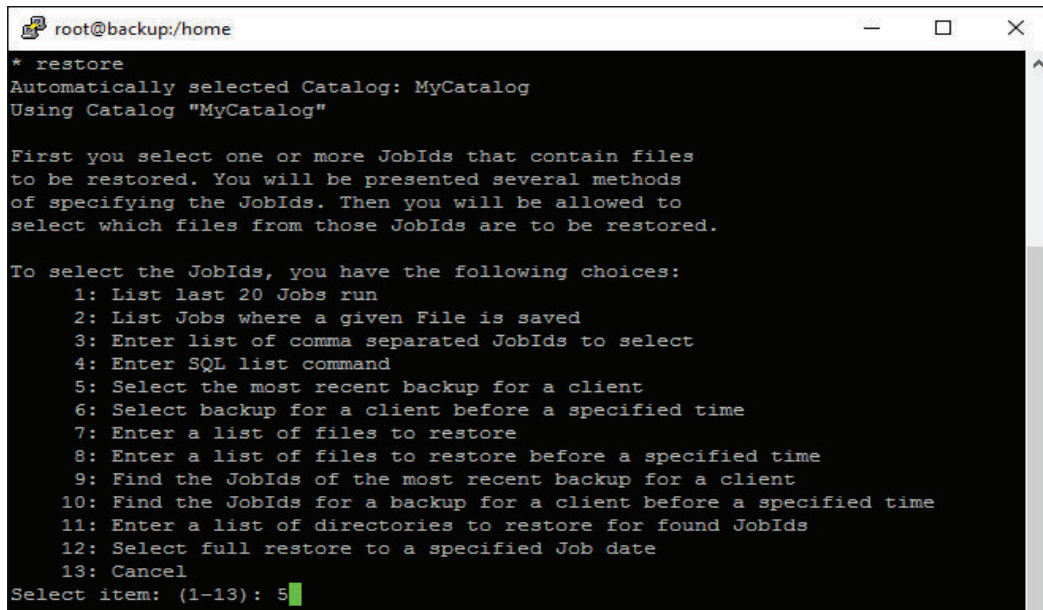
Se requiere restaurar archivos de aplicación _____

Ing. Mario Morocho
SOLICITANTE

Ing. Byron Jumbo
JEFE TÉCNICO

Figura 3-33 Solicitud de restauración svn

La restauración tiene varias opciones y se la puede realizar por consola en la dirección configurada en el archivo director de Bacula (bacula-dir.conf), para esta prueba se restaurara el último respaldo del servidor de nombre httpdold:



```

root@backup:/home
* restore
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"

First you select one or more JobIds that contain files
to be restored. You will be presented several methods
of specifying the JobIds. Then you will be allowed to
select which files from those JobIds are to be restored.

To select the JobIds, you have the following choices:
  1: List last 20 Jobs run
  2: List Jobs where a given File is saved
  3: Enter list of comma separated JobIds to select
  4: Enter SQL list command
  5: Select the most recent backup for a client
  6: Select backup for a client before a specified time
  7: Enter a list of files to restore
  8: Enter a list of files to restore before a specified time
  9: Find the JobIds of the most recent backup for a client
 10: Find the JobIds for a backup for a client before a specified time
 11: Enter a list of directories to restore for found JobIds
 12: Select full restore to a specified Job date
 13: Cancel
Select item: (1-13): 5

```

Figura 3-34 Tipo de restauración

Escoger el servidor a restaurar:



```

root@backup:/home
Defined Clients:
  1: server52-fd
  2: server57-fd
  3: svn-fd
  4: httpdold-fd
  5: mysql-fd
  6: postgres-fd
Select the Client (1-6): 4

```

Figura 3-35 Cliente a restaurar

Bacula hará un re escaneo de todos los datos que tiene el equipo. Puesto que el catálogo lo almacena en base de datos, no habrá que consultarlo en disco, por lo que será más rápido. Tras recuperar todo el catálogo se dará un acceso a otra pantalla similar a la navegación en shell de GNU/Linux. De esta forma veremos los archivos de los que tenemos respaldos y podremos navegar por carpetas y ficheros. Los comandos más importantes y necesarios aquí son **cd**, **ls**, **mark**, **markdir** y **done**.

Restauración de nodo httpdold:

```

root@backup:/home/bacula
Automatically selected FileSet: httpdold-fs
-----+-----+-----+-----+-----+-----+
| JobId | Level | JobFiles | JobBytes | StartTime | VolumeName |
-----+-----+-----+-----+-----+-----+
| 6,644 | F | 2,219 | 940,846 | 2015-10-01 02:06 | fullhttpdold-01-10-2015 |
| 6,671 | I | 12 | 786,796 | 2015-10-01 02:05 | fullhttpdold-01-10-2015 |
| 6,698 | I | 13 | 253,813 | 2015-09-31 02:05 | fullhttpdold-31-09-2015 |
| 6,725 | I | 12 | 287,815 | 2015-09-31 02:05 | fullhttpdold-31-09-2015 |
-----+-----+-----+-----+-----+-----+
You have selected the following JobIds: 6644,6671,6698,6725

Building directory tree for JobId(s) 6644,6671,6698,6725... ++++++
1,943 files inserted into the tree.

You are now entering file selection mode where you add (mark) and
remove (unmark) files to be restored. No files are initially added, unless
you used the "all" keyword on the command line.
Enter "done" to leave this mode.
$ done
Bootstrap records written to /var/lib/bacula/httpdold-dir.restore.1.bsr

The job will require the following
Volume(s) Storage(s) SD Device(s)
-----+-----+-----+-----+-----+
*fullhttpdold-01-10-2015 storage-daemon storage-daemon

Volumes marked with "*" are online.

1 file selected to be restored.

Run Restore job
JobName: RestoreFiles
Bootstrap: /var/lib/bacula/httpdold-dir.restore.1.bsr
Where: /Restore
Replace: always
FileSet: Full Set
Backup Client: httpdold--fd
Restore Client: httpdold-fd
Storage: storage-daemon
When: 2015-10-17 13:56:16
Catalog: MyCatalog
Priority: 10
Plugin Options: *None*
OK to run? (yes/mod/no): yes

```

Figura 3-36 Restauración de cliente httpdold

Restauración de nodo svn:

```

root@backup:/home/bacula
Automatically selected FileSet: svn-fs
-----+-----+-----+-----+-----+-----+
| JobId | Level | JobFiles | JobBytes | StartTime | VolumeName |
-----+-----+-----+-----+-----+-----+
| 6,489 | F | 2,219 | 2 740,824 | 2015-10-01 19:06 | fullhttpdold-31-09-2015 |
| 6,467 | I | 12 | 2 586,784 | 2015-10-01 19:05 | fullhttpdold-31-09-2015 |
| 6,459 | I | 13 | 2543,623 | 2015-09-31 19:05 | fullhttpdold-24-09-2015 |
| 6,393 | I | 12 | 2847,687 | 2015-09-31 19:05 | fullhttpdold-24-09-2015 |
-----+-----+-----+-----+-----+-----+
You have selected the following JobIds: 6644,6671,6698,6725

Building directory tree for JobId(s) 6489,6467,6459,6393... ++++++
1,943 files inserted into the tree.

You are now entering file selection mode where you add (mark) and
remove (unmark) files to be restored. No files are initially added, unless
you used the "all" keyword on the command line.
Enter "done" to leave this mode.

```

```

root@backup:/home/bacula
$ done
Bootstrap records written to /var/lib/bacula/svn-dir.restore.1.bsr
otstrap records written to /var/lib/bacula/svn-dir.restore.1.bsr

The job will require the following
Volume(s)          Storage(s)          SD Device(s)
=====
*fullsvn-31-09-2015  storage-daemon      storage-daemon

Volumes marked with "*" are online.

1 file selected to be restored.

Run Restore job
JobName:           RestoreFiles
Bootstrap:         /var/lib/bacula/svn-dir.restore.1.bsr
Where:             /Restore
Replace:           always
FileSet:           Full Set
Backup Client:     svn-fd
Restore Client:    svn-fd
Storage:           storage-daemon
When:              2015-10-17 15:36:39
Catalog:           MyCatalog
Priority:           10
Plugin Options:    *None*
OK to run? (yes/mod/no): yes

```

Figura 3-37 Restauración de cliente svn

En la prueba se puede observar que al escribir donde nos indica que se va a proceder a recuperar los ficheros y creará un nuevo trabajo de restauración para tal efecto. Si no modificamos ninguna de las opciones, por defecto nos dejará los ficheros seleccionados en /Restore del equipo remoto. Ya luego tendremos manualmente que moverlos a donde corresponda si procede.

```

root@backup:/Restore
Archivo Editar Ver Buscar Terminal Ayuda
[root@backup ~]# cd /Restore/
[root@backup Restore]# ls
httpdold svn
[root@backup Restore]#
[root@backup Restore]#
[root@backup Restore]#
[root@backup Restore]# █

```

Figura 3-38 Archivos restaurados

3.7. ANÁLISIS DE RESULTADOS

3.7.1. SITUACIÓN SIN LA APLICACIÓN DEL MODELO

Sin la aplicación del modelo la empresa no tenía ninguna gestión de respaldos de información, copias de seguridad del sistema, aplicaciones, datos o documentación ni dentro ni fuera de las instalaciones de la empresa, por lo cual la empresa era muy vulnerable en caso de algún incidente.

Ejemplo:

Sin la aplicación del modelo se realizó una copia manual como la realizaba el jefe técnico, se copió los datos de la base de datos Mysql que tenía de tamaño 11 GB el cual se respaldó en 1 hora con 18 minutos tomando en cuenta que la velocidad de transferencia de la red tenía una aproximación de 20 MB/S lo cual es un tiempo no óptimo por la carga operacional de esa hora.

3.7.2. SITUACIÓN CON LA APLICACIÓN DEL MODELO

Con la implementación del modelo de respaldos la empresa cuenta con un proceso de respaldos documentado basado en las mejores prácticas con los lineamientos de COBIT 5 según el catalizador DSS04.07 establecidos con los diferentes controles y actividades cumplidos e implementados para que la empresa pueda mantener a salvo su información y estar respaldada en caso de alguna contingencia. Se puede verificar el cumplimiento de los controles en la Tabla 3-16 Cumplimiento de los objetivos de TI.

Prefijo	Prácticas de Gobierno		
DSS04.07	Administrar disposiciones de salvaguardia		
	Mantenga la disponibilidad de la información crítica para el negocio		
Entradas	Salidas		
Descripción	Desde	Descripción	A
.		Resultados de las pruebas de copia de seguridad de datos	interna

Actividades		Cumple	No Cumple
1	Guarde los sistemas, aplicaciones, datos y documentación con el programa definido, teniendo en cuenta:		
	Frecuencia (mensual, semanal, diaria, etc.).	X	
	Modo de copias de seguridad (por ejemplo, discos espejo para copias de seguridad en tiempo real frente a DVD-ROM para retenciones de larga duración).	X	
	Tipo de copias de seguridad (por ejemplo, completa o incremental).	X	
	Tipo de soporte.	X	
	Copias de seguridad automatizadas en línea.	X	
	Tipos de datos (por ejemplo, voz, óptica).	X	
	Creación de registros.	X	
	Datos de cálculos críticos para el usuario final (por ejemplo, hojas de cálculo).	X	
	Localización física y lógica de las fuentes de datos.	X	
	Seguridad y derechos de acceso.	X	
	Cifrado.	X	
2	Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes. Considerar acuerdos de depósito.	X	
3	Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.	X	
4	Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP).	X	
5	Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.	X	

Tabla 3-16 Cumplimiento de los objetivos de TI

Ejemplo:

Dentro del análisis de resultados en el proyecto se verificó la ejecución de la planificación de los respaldos que se realizaron sin ningún inconveniente y en los tiempos programados tomando en cuenta que se realizaron en las noches para no afectar con el desempeño de las aplicaciones y los servidores, la red tenía una velocidad de 60[MB/s] lo cual permitía realizar un 1 GB de los respaldos en tiempo de 2 minutos con 23 segundos[s] lo cual es un tiempo conveniente y óptimo para respaldar el tamaño de los servidores escogidos.

3.7.3. EVALUACIÓN

Al mitigar los riesgos en la empresa se determinó que en caso de incidentes no cuenta con un plan de recuperación o continuidad, generalmente, una de las actividades primordiales que está relacionada con el uso de respaldos de información.

Con el uso del proceso de Gestión de la Continuidad (con identificador DSS04), perteneciente al dominio de entrega, servicio y soporte (DSS por las siglas de Deliver, Service and Support) se detallan aspectos de las medidas de seguridad, por ejemplo, se incluyen objetivos, métricas, prácticas, actividades, entradas y salidas que retroalimentan la Gestión de acuerdos de respaldo (DSS04.07), que tiene como propósito mantener la disponibilidad de la información crítica para el negocio.

Evaluación del nivel de madurez sin la implementación del modelo

Se puede ver a continuación en la Tabla 3-17 Evaluación del proceso sin la implementación del modelo.

Nombre del Proceso	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
DSS04	La empresa no tiene procesos ni procedimientos establecidos con ninguna base tecnológica ni estándares, además no se tienen actas de aceptación de la gerencia o de algún comité de TI.	PA 1.1	PA 2.1 PA 2.2	PA 3.1	PA 3.2 PA 4.1 PA 4.2	PA 5.1 PA 5.2
Clasificación por criterios	Ninguno					
Nivel de Capacidad Cumplido	Ninguno					

N- 0%-15%	P- 15%-50%	L- 50%-85%	F- 85%-100%
-----------	------------	------------	-------------

N – Not Achieved (No Cumplido)
P – Partially Achieved (Parcialmente Cumplido)
L – Largely Achieved (Ampliamente Cumplido)
F- Fully Achieved (Completamente Cumplido)

DSS04	Gestión de la Continuidad						
	Continuar las operaciones críticas de negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa en caso de una interrupción significativa.						
Propósito	Criterios	Los criterios se cumplen S/N	Comentario	No Cumplido (0-15%)	Parcialmente Cumplido (15%-50%)	Ampliamente Cumplido (50%- 85%)	Completamente Cumplido (85-100%)
Nivel 0 Incompleto	Evaluar si se logran los siguientes resultados. El proceso no se lleva a cabo, o no cumple el propósito del proceso.	En este nivel, hay poca o ninguna evidencia de un logro del propósito del proceso.	N	La empresa no tiene procesos ni procedimientos establecidos con ninguna base tecnológica ni estándares, además no se tienen actas de aceptación de la gerencia o de algún comité de TI.	2% (Comunicación Oral)		

Tabla 3-17 Evaluación del proceso sin la implementación del modelo

Resultados de evaluación sin el modelo implementado

RESULTADO DE EVALUACION DE PROCESOS								
Proceso ID	Nombre del Proceso	Para ser Evaluado	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
	Procesos para la gobernanza de las TI de las empresas							
	Entrega, servicio y soporte							
DSS04	Gestión de la Continuidad	➤	N	N	N	N	N	N

N- 0%-15%	P- 15%-50%	L- 50%-85%	F- 85%-100%
-----------	------------	------------	-------------

Tabla 3-18 Matriz de resultados de evaluación sin el modelo implementado

La empresa no contaba con procesos ni procedimientos establecidos con ninguna base tecnológica o estándares, además no se tenían actas de aceptación de la gerencia o algún comité de TI por lo cual se determina un nivel cero de madurez de la empresa como se muestra en la Tabla 3-18 Matriz de resultados de evaluación sin el modelo implementado.

En la Tabla 3-17 Evaluación del proceso sin la implementación del modelo se puede ver que en el nivel cero de madurez es no cumplido pero se le agrego un 2% por el trabajo realizado por el jefe técnico que eran respaldos manuales realizados en sus horarios de menor exigencia laboral, calificado como comunicación oral.

Evaluación del nivel de madurez con la implementación del modelo

Se puede ver a continuación en la Tabla 3-19 Evaluación del proceso sin la implementación del modelo.

Nombre del Proceso	Nivel 0	Nivel 1		Nivel 2		Nivel 3		Nivel 4		Nivel 5			
		PA 1.1	Cumplido	PA 2.1	Cumplido	PA 2.2	Cumplido	PA 3.1	3.2	PA 4.1	4.2	PA 5.1	PA 5.2
DSS04	Para este catalizador de COBIT 5 todos los controles han sido cumplidos	PA 1.1	Cumplido	PA 2.1	Cumplido	PA 2.2	Cumplido	PA 3.1	3.2	PA 4.1	4.2	PA 5.1	PA 5.2
Clasificación por criterios	Todos los criterios cumplidos	Todos los criterios cumplidos		Cumplido		Cumplido		P					
Nivel de Capacidad Cumplido	Todos los niveles de capacidad cumplidos	Todos los niveles de capacidad cumplidos		Cumplido		Cumplido		P					



N – Not Achieved (No Cumplido)
P – Partially Achieved (Parcialmente Cumplido)
L – Largely Achieved (Ampliamente Cumplido)
F - Fully Achieved (Completamente Cumplido)

DSS04		Gestión de la Continuidad						
	Propósito	Continuar las operaciones críticas de negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa en caso de una interrupción significativa.						
	Evaluar si se logran los siguientes resultados.	Criterios	Los criterios se cumplen S/N	Comentario	No Cumplido (0-15%)	Parcialmente Cumplido (15% -50%)	Ampliamente Cumplido (50% - 85%)	Completamente Cumplido (85-100%)
Nivel 0 Incompleto	El proceso no se lleva a cabo, o no cumple el propósito del proceso.	En este nivel, hay poca o ninguna evidencia de un logro del propósito del proceso.						F
Nivel 1 Rendimiento	PA 1.1 El proceso implementado logra	Se están logrando los siguientes resultados del proceso: DSS04-O1 La información crítica del negocio está disponible para el negocio en línea con los niveles mínimos de servicio requerido. DSS04-O2 Suficiente capacidad de recuperación está en su lugar para los servicios críticos. DSS04-O3 Pruebas de continuidad de servicios han verificado la eficacia del plan. DSS04-O4 Un plan de continuidad actualizada refleja los requerimientos actuales del negocios. DSS04-O5 Las partes internas y externas han sido capacitados en el plan de continuidad.		Evaluación general del proceso				
			S	La información se encuentra en línea para cualquier eventualidad que necesite la empresa.				F
			S	Con la implementación del modelo se solventa los servicios críticos del negocio.				F
			S	Se han ejecutado las diferentes pruebas validando que el plan funcione.				F
			S	EL modelo implementado cubre las necesidades actuales del negocio para el cliente.				F
			S	Se dio la capacitación al personal técnico y autorizado por la empresa para la obtención del Gestión de respaldos.				F

Nivel 2 Gestionado	<p>PA 2.1 Gestión del rendimiento - Una medida del alcance para el cual el rendimiento del proceso es gestionado.</p>	<p>Como resultado del completo cumplimiento de este atributo:</p> <p>a) Objetivos para el rendimiento del proceso son identificados.</p> <p>b) Rendimiento de los procesos es planificado y monitoreado.</p> <p>c) Rendimiento de los procesos se ajustan para cumplir los planes.</p> <p>d) Se definen, asignan y comunican Responsabilidades y autoridades para llevar a cabo los procesos.</p> <p>e) Recursos e información necesarios para llevar a cabo el proceso son identificados, puestos a disposición, asignados y utilizados.</p> <p>f) Las interfaces entre las partes involucradas son gestionados para asegurar tanto la comunicación eficaz y también la asignación clara de responsabilidades.</p>	S	<p>Todos los controles roles y responsabilidades han sido aplicados y fueron definidos según los estándares de COBIT 5 y con la aprobación de la gerencia de tecnología y el cliente.</p>				F
		S						
	<p>PA 2.2 Trabajo Gestión del Producto - Una medida del grado en que los productos de trabajo producidos por el proceso se ordenan adecuadamente. Los productos de trabajo (o salidas del proceso)</p>	<p>Como resultado del completo cumplimiento de este atributo:</p> <p>a) Los requisitos para los productos de trabajo del proceso son definidos.</p> <p>b) Requisitos para la documentación y el control de los productos de trabajo son definidos.</p> <p>c) Productos de trabajo están apropiadamente identificados, documentados y controlados.</p>	S	<p>Todos los requerimientos y procesos fueron debidamente definidos y documentados según los estándares de COBIT 5 y con la aprobación de la gerencia de tecnología y el cliente.</p>				F
		S						

<p>Nivel 3 Establecido</p>	<p>son definidos y controlados.</p>	<p>d) productos de trabajo se revisarán de acuerdo con los planes previstos y se ajustan si es necesario para cumplir con los Requerimientos.</p>	<p>S</p>			
<p>PA 3.1 Definición de proceso - Una medida del grado en que un proceso estándar se mantiene para apoyar el despliegue del proceso definido.</p>	<p>Como resultado del completo cumplimiento de este atributo:</p> <p>a) un proceso estándar, incluyendo las guías de adaptación adecuadas, se define que describe los elementos fundamentales que deben ser incorporados en un proceso definido.</p> <p>b) La secuencia y la interacción del proceso estándar con otros procesos son determinados.</p> <p>c) Las competencias y funciones requeridas para llevar a cabo un proceso se identifican como parte del proceso estándar.</p> <p>d) La infraestructura requerida y ambiente de trabajo para realizar un proceso se identifican como parte del proceso estándar.</p> <p>e) se determinan los métodos adecuados para el seguimiento de la eficacia y adecuación del proceso.</p>	<p>S</p> <p>N</p> <p>S</p> <p>N</p> <p>S</p>	<p>El modelo cumple con los estándares internacionales y las buenas prácticas recomendadas, el alcance solo involucra la gestión de respaldos y se requiere la generación de otros proyectos para los demás servicios de TI.</p>		<p>P</p>	
<p>PA 3.2 Proceso de implementación - Una medida del grado en que el proceso estándar se implementa de</p>	<p>Como resultado del completo cumplimiento de este atributo:</p> <p>a) Un proceso es desplegado basándose en un proceso estándar seleccionado apropiadamente y/o adaptado.</p>	<p>S</p>	<p>El modelo cumple con los estándares internacionales y las buenas prácticas recomendadas, el alcance solo involucra la gestión de respaldos y se requiere la</p>		<p>P</p>	

<p>manera efectiva como un proceso definido para lograr los resultados del proceso.</p>	<p>b) Se asignan y comunican los roles, responsabilidades y autoridades requeridas para llevar a cabo el proceso definido.</p>	S	<p>generación de otros proyectos para los demás servicios de TI.</p>		
	<p>c) El personal que realiza el proceso definido son competentes en la base de la apropiada educación, capacitación y experiencia.</p>	S			
	<p>d) Son puestos a disposición, asignación y utilización los recursos y la información requeridos para realizar el proceso definido.</p>	N			
	<p>e) Infraestructura requerida y ambiente de trabajo para realizar el proceso definido se ponen a disposición, gestión y mantenimiento.</p>	N			
	<p>f) Los datos correspondientes se recogen y analizan como una base para entender el comportamiento de, y para demostrar la idoneidad y la eficacia de los procesos, y para evaluar dónde puede realizarse la mejora continua de los procesos.</p>	N			

Tabla 3-19 Evaluación del proceso con la implementación del modelo

Resultados de evaluación con el modelo implementado

RESULTADO DE EVALUACION DE PROCESOS								
Proceso ID	Nombre del Proceso	Para ser Evaluado	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Procesos para la gobernanza de las TI de las empresas								
Entrega, servicio y soporte								
DSS04	Gestión de la Continuidad	➤	F	F	F	P		
			N- 0%-15%	P- 15%-50%	L- 50%-85%	F- 85%-100%		

Tabla 3-20 Matriz de resultados de evaluación con el modelo implementado

Este dominio tiene que ver con la entrega de los servicios que son requeridos, esto incluye: la provisión del servicio, la gestión de seguridad y continuidad, el soporte a los usuarios, la administración de los datos y la gestión de las instalaciones de plataforma tecnológica.

La empresa ahora cuenta con procedimientos establecidos con una base tecnológica o estándares, además actas de aceptación de la gerencia, con la realización de copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida de acuerdo a los requerimientos propuestos.

Se definió el almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio, se realizó un plan de contingencia en caso de cualquier eventualidad, se capacitó al personal.

Por todo ello en la evaluación del proceso se determina un nivel 2 de madurez completamente cumplido de la empresa como se muestra en la Tabla 3-20 Matriz de resultados de evaluación sin el modelo implementado y un nivel de madurez 3 parcialmente cumplido ya que es necesario unos tres meses de prueba para recolectar data y verificar el cumplimiento del modelo y poder evaluar con los datos actuales.

Ejemplo:

Con todo lo anteriormente expuesto, cabe mencionar que estas pruebas se realizarán con el objetivo de medir el rendimiento de la solución en el cual los tiempos de repuesta del esquema de puesta en producción son satisfactorios como se observa en la tabla 3.17:

ÍTEM	Tamaño del nodo	Velocidad transferencia	Tiempo respuesta	% DE MEJORA TIEMPO
Sin Modelo	11 GB	20 MB/s	1h 18min	X
Con Modelo	11 GB	60 MB/s	26 min 13s	66,67%

Tabla 3-21 Eficiencia de la solución de respaldos

Como se puede ver la eficiencia de la red mejora en la noche fuera de horarios laborables por lo que el tiempo de respuesta del respaldo ahorra considerablemente un tiempo de 52 minutos con 13 segundos, que es una mejora del 66,67% para el nodo de base de datos Mysql.

Una vez realizado este análisis, se concluye que los tiempos obtenidos de las pruebas, se encuentran justificados de acuerdo al ambiente en que se desenvuelven.

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- ✓ Se determinó que Yakindu Cia. Ltda. realizaba sus respaldos de forma manual sin seguir ningún tipo de proceso, estos respaldos los realiza el jefe técnico por precaución.
- ✓ En conjunto con el Jefe técnico se identificó que las necesidades principales son: la implementación de un sistema automatizado de respaldos, definir políticas que salvaguarden la información, la necesidad de un plan de contingencia en causa de desastre o pérdida de información.
- ✓ La propuesta establecida para la empresa es aplicar el modelo propuesto en el presente documento orientado a las mejores prácticas que se adapte a las necesidades de la empresa y así de esta manera permita asegurar la continuidad del negocio
- ✓ Se realizó con la instalación, configuración y parametrización de la herramienta Bacula con base al estudio de la situación actual de la empresa, tomando en cuenta los sistemas, las aplicaciones, el grado de confidencialidad de la información que se está respaldando y los procesos que se realizan para la obtención de información.
- ✓ Se ejecutaron pruebas de recuperación de la información dando como resultado que el respaldo obtenido es confiable y seguro por tal razón se comprobó que los procedimientos aplicados para el respaldo de información son confiables.
- ✓ La implementación automática de una gestión de respaldos disminuye el tiempo de las actividades del responsable de la obtención de los mismos.
- ✓ No se pudo evaluar el modelo implementado, por la inexistencia de una gestión de respaldos para tomarla como referencia, la primera lectura fue

extraída de la herramienta implementada en tres meses se debe volver a tomar una lectura para compararla con la inicial y así evaluar el desempeño de resultados.

- ✓ Se revisó que la carga operacional del sistema de la empresa estaba en su máximo nivel desde las 9 am hasta las 18 pm y se revisó que desde las 18 horas en adelante el consumo de CPU era mínimo por tal razón se estableció como hora de respaldos del sistema a las 19 pm hasta 8am.
- ✓ Se estableció roles y responsabilidades para seguir el procedimiento necesario para obtención de los archivos requeridos e íntegros para poder devolver la operación normal al negocio en caso de un imprevisto o desastre natural.
- ✓ Se estableció un tamaño en disco para obtener los respaldos de información y protegerlos fuera del recinto para de esta manera poder usarlos en una eventual situación de desastre natural.

4.2. RECOMENDACIONES

- ✓ Debe revisarse el Modelo de Respaldos de manera periódica, puesto que los sistemas y procesos varían de manera constante y estos a su vez, modifican los datos de los procedimientos aplicados en la obtención de respaldos
- ✓ Debe mantenerse un control de los respaldos y de las actualizaciones de las Solicitudes de Restauración puesto que esta información es necesaria para poder llevar el control de la información respaldada; así como también de las eventuales recuperaciones.
- ✓ Es importante realizar pruebas periódicas de restauración de la información de cada componente del Modelo de Respaldos, para asegurarse de que la información respaldada se pueden leer, escribir y restaurar.
- ✓ Realizar simulacros del Plan de Contingencia ayudará a proteger a la empresa de eventos que pongan en peligro su existencia y conservar los activos de la empresa.
- ✓ El responsable de los respaldos debe realizar un monitoreo constante de la ejecución del software aplicado (Bacula) para la obtención de los respaldos y así poder asegurar que los mismos están siendo obtenidos de acuerdo a las especificaciones del modelo.
- ✓ El responsable de respaldos debe buscar actualizar su modelo por nuevas metodologías, nuevo hardware y nuevo software para respaldos de información y mejora del procedimiento.

BIBLIOGRAFÍA

- [1] ISACA, Val IT Framework for Business Technology Management. [En línea], 2012.
- [2] E. R. Larrocha, MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización), UNED, 2010.
- [3] M. A. M. A. Rodrigo Muñoz Serna, Caracterización de Procesos de Gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria Editorial Colombiana, apoyando el proceso de transformación digital, ICESI, 2012.
- [4] L. L. Isvel, Implementación de una solución de respaldos de información en la empresa UniplexSystems en Quito, EPN, 2007.
- [5] V. P. Q. Reinoso, Definición e implementación de un modelo de respaldos de información en la compañía TRANSELECTRIC S.A., EPN, 2007.
- [6] D. G. T. Guerrero, IMPLEMENTACIÓN DE UN SISTEMA DE RESPALDO PARA LOS SERVIDORES DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES CON TECNOLOGÍA OPEN SOURCE UTILIZANDO BACULA, Universidad de Guayaquil, 2013.
- [7] OSIATIS, «ITIL FOUNDATION,» [En línea]. Available: <http://itilv3.osiatis.es/>.
- [8] OSIATIS, «COBIT Mapping: Mapping of ITIL V3 With COBIT 4.1,» [En línea]. Available: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Mapping-Mapping-of-ITIL-V3-With-COBIT-4-11.aspx>.
- [9] E. Cardoso, «Bacula vs Other Backup Solutions,» [En línea]. Available: <http://wiki.bacula.org/doku.php?id=comparisons>.
- [10] Bacula, «Bacula,» [En línea]. Available: <http://blog.bacula.org/>.
- [11] Bacula, «Bacula,» [En línea]. Available: <http://www.baculasystems.com/>.
- [12] V. Robles, «Victor Robles - Bacula,» 04 11 2013. [En línea]. Available: <https://victorroblesweb.es/2013/11/04/backups-red-bacula-funcionamiento/>.

GLOSARIO

- **Bacula:** es una colección de herramientas de respaldo capaz de cubrir las necesidades de respaldo de equipos bajo redes IP.
- **Amanda:** El archivador de disco automático avanzado para red de Maryland.
- **Tivoli (TSM):** productos Tivoli Storage Manager proporcionan soluciones de gestión de almacenamiento para entornos de sistema de varios proveedores.
- **Veritas:** Sistema de solución de respaldos propietario.
- **Legato Networker:** es un paquete de software de protección de datos de nivel empresarial que unifica y copia de seguridad automática.
- **CA ARCserve:** proporciona recuperación garantizada a través de tecnología robusta de respaldo, recuperación de desastres, replicación y alta disponibilidad.
- **Arkeia Network Backup:** es una compañía de software estadounidense que produce software de copia de seguridad de red para 200 plataformas, incluyendo Windows, Macintosh, Linux, AIX, BSD y HP-UX, y también un dispositivo de copia de seguridad, la integración de su software con el almacenamiento en disco y la conectividad de red.
- **Quest NetVault:Backup:** es un conjunto de soluciones de protección de datos desarrollados y apoyados por Quest Software.
- **LBackup:** Es un sistema de copia de seguridad de código abierto, dirigido a los administradores de sistemas que exigen copias de seguridad fiables.
- **PostgresSQL:** es un Sistema de gestión de bases de datos relacional orientado a objetos y libre, publicado bajo la licencia PosgreSQL , similar a la BSD o la MIT.
- **Open Source:** (Código abierto) es la expresión con la que se conoce al software o hardware distribuido y desarrollado libremente.

- **Webmin:** es una herramienta de configuración de sistemas accesible vía web para sistemas Unix, como GNU/Linux y OpenSolaris, GNU/Linux.
- **Bacula Admin Tool:** Bacula es un conjunto de programas para gestionar copias de seguridad, recuperación y verificación de los datos. GUI más avanzada para Bacula, la Herramienta de administración de Bacula (BAT) de la consola
- **Bacuvview:** La aplicación Bacuvview proporciona una vista basada en la web en el estado de un sistema de copia de seguridad Bacula.
- **Webacula:** es la interfaz Web de BACULA, un sistema de backup automatizado en red.
- **Reportula:** es un programa web basado en php que proporciona una salida de información resumida de las copias de seguridad Bacula.
- **Bacula-Web:** es la interfaz Web de BACULA.
- **Storage daemon:** El archivo de configuración de almacenamiento Daemon de Bacula.
- **File daemon:** El (o Demonio de archivos) de configuración del cliente es uno de los más simples de especificar.
- **FileSet:** es un grupo de archivos.
- **Schedule:** planificación de los respaldos de Bacula.
- **AutoPrune:** permite a Bacula podar automáticamente todos los volúmenes de la agrupación cuando se necesita Volumen para otro JOB.
- **MySQL:** es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.
- **SQLite:** es un sistema de gestión de bases de datos relacional compatible con ACID, contenida en una relativamente pequeña.
- **GNOME:** es un entorno de escritorio e infraestructura de desarrollo para sistemas operativos GNU/Linux, Unix y derivados Unix como, BSD o Solaris.

- **Dual-Core AMD Opteron:** es una línea de microprocesadores x86 de AMD para servidores y una arquitectura de memoria similar a la del Opteron para la familia Intel Core i7.
- **nVidia Quadro FX:** Tarjeta de video.
- **COBIT:** Objetivos de Control para Información y Tecnologías Relacionadas.
- **ITGI:** Instituto de Administración de las Tecnologías de la Información.
- **Risk IT:** es un ámbito de aplicación del marco de riesgos está totalmente incluida en el ámbito del marco COBIT 5.
- **Val IT:** es un framework de gobernabilidad que se puede utilizar para crear valor de negocio de las inversiones en TI.
- **ITAF:** es un marco de prácticas profesionales de auditoría de SI y profesionales de aseguramiento de buscar orientación, las políticas y los procedimientos de investigación.
- **BMIS:** Modelo de Negocio para la Información de Seguridad
- **ITIL:** es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma.
- **ISO:** sistema de normalización internacional para productos de diversas áreas.
- **PMBOK:** PMBOK es el estándar para la Administración de Proyectos y cuyas siglas significan en inglés Project Management Body of Knowledge (el Compendio del Saber de la Gestión de Proyectos en español).
- **PRINCE2:** (PRojects IN Controlled Environment) es un método estructurado de gestión de proyectos. Es una aproximación a las “buenas prácticas” para la gestión de todo tipo de proyectos que se ha convertido en el estándar de facto para la organización, gestión y control de proyectos.

- **FFIEC7:** (Federal Financial Institutions Examination Council) Consejo Federal de Inspección de Instituciones Financieras, Manual de Inspección Antilavado de Dinero Ley/Secreto Bancario
- **Stakeholders:** El término agrupa a trabajadores, organizaciones sociales, accionistas y proveedores, entre muchos otros actores clave que se ven afectados por las decisiones de una empresa. Generar confianza con estos es fundamental para el desarrollo de una organización.
- **CEO:** se refiere a un título corporativo en empresas, principalmente estadounidenses, y significa en inglés "Chief Executive Officer".
- **CMMI:** Capability Maturity Model Integration Modelo de Madurez de la Capacidad Integrado es un modelo de procesos que contiene las mejores prácticas de la industria para el desarrollo, mantenimiento, adquisición y operación de productos y servicios.
- **SEI :** Software Engineering Institute es un instituto federal estadounidense de investigación y desarrollo, fundado por Congreso de los Estados Unidos en 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de software, que dieran respuesta a los problemas que generaba al ejército estadounidense la programación e integración de los sub-sistemas de software en la construcción de complejos sistemas militares.
- **CMF:** CMMI Model Foundation cubre la gestión de procesos, gestión de proyectos y áreas de soporte en los procesos del gobierno y la industria.
- **CAR:** Análisis Causal y Resolución Tiene como propósito identificar las causas de los resultados seleccionados y tomar acción para mejorar la realización del proceso.
- **CM:** Gestión de Configuración su propósito es establecer y mantener la integridad de los productos de trabajo mediante la identificación de configuración, el control de configuración, el registro del estado de configuración, y las auditorías de configuración.

- **DAR:** Análisis de Decisiones y Resolución su propósito es analizar las posibles decisiones utilizando un proceso de evaluación formal que evalúe alternativas identificadas frente a criterios establecidos.
- **IPM:** Gestión Integrada del Proyecto Consiste en la aplicación de metodologías, técnicas y herramientas para la definición, planificación, ejecución, seguimiento y control, cierre de las actividades.
- **Medición y Análisis (MA):** Su propósito es desarrollar y mantener una competencia de medición que se usa para dar soporte a las necesidades de información de la gerencia.
- **Definición de Procesos de la Organización (OPD):** Establece y mantiene un conjunto utilizable de activos de proceso organizativos, estandare de entorno de trabajo, y reglas y guías para los equipos.
- **Enfoque en Procesos de la Organización (OPF):** Planifica, implementa y despliega mejoras de procesos organizativas en base a un conocimiento en profundidad de las fortalezas y debilidades actuales de los procesos y activos de proceso de la organización.
- **Gestión del Rendimiento de la Organización (OPM):** Gestiona proactivamente el rendimiento de la organización para cumplir sus objetivos de negocio.
- **Rendimiento de Procesos de la Organización (OPP):** Establece y mantiene un conocimiento cuantitativo del rendimiento de los procesos seleccionados de entre el conjunto de procesos estándar de la organización con el fin de dar soporte al logro de los objetivos de calidad y rendimiento de proceso.
- **Formación en la Organización (OT):** Desarrolla las habilidades y conocimientos de las personas para que puedan desempeñar sus roles eficaz y eficientemente.
- **Monitorización y Control del Proyecto (PMC):** Tiene como propósito proporcionar una comprensión del progreso del proyecto para que se

puedan tomar las acciones correctivas apropiadas, cuando el rendimiento del proyecto se desvíe significativamente del plan.

- **Planificación de Proyecto (PP):** Tiene como propósito establecer y mantener planes que definan las actividades del proyecto.
- **Aseguramiento de la Calidad del Proceso y del Producto (PPQA):** Proporciona al personal y a la gerencia un conocimiento objetivo de los procesos de sus productos de trabajo asociados.
- **Gestión Cuantitativa del Proyecto (QPM):** Tiene como propósito gestionar cuantitativamente el proyecto para alcanzar los objetivos establecidos de calidad y de rendimiento del proceso del proyecto.
- **Gestión de Requisitos (REQM):** Gestiona los requisitos de los productos y componentes de producto y asegurar que dichos requisitos estén alineados con los planes de trabajo y los productos de trabajo.
- **Gestión de Riesgos (RSKM):** Identifica problemas potenciales antes de que ocurran de modo que, a lo largo de la vida del producto o trabajo, se puedan planificar e invocar actividades de manejo de riesgos según se necesite para mitigar los impactos adversos sobre el logro de objetivos.
- **CMMI-DEV:** En él se tratan procesos de desarrollo de productos y servicios.
- **Integración del Producto (PI):** Esta área trata de la integración de componentes del producto dentro de componentes de producto más completos.
- **Desarrollo de Requisitos (RD):** Recopila las necesidades del cliente para convertirlas en requerimientos del producto esperado.
- **Gestión de Acuerdos con Proveedores (SAM):** Gestiona la adquisición de productos y servicios a suministradores.
- **Solución Técnica (TS):** Diseña, desarrolla e implementa soluciones para los requerimientos del producto establecido.

- **Validación (VAL):** Las actividades de validación se pueden aplicar a todos los aspectos del producto en cualquiera de sus entornos previstos tales como operación, formulación, mantenimiento y servicio de soporte.
- **Verificación (VER):** Su propósito es asegurar que los productos del trabajo seleccionados cumplan los requisitos específicos.
- **IEC: (International Electrotechnical Commission):** La Comisión Electrotécnica Internacional es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.
- **British Standards Institution (BSI):** es una multinacional cuyo fin se basa en la creación de normas para la estandarización de procesos. Entre sus actividades principales se incluyen la certificación, auditoría y formación en las normas.
- **NTC-ISO/IEC 27001:** es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.
- **ICONTEC: (Instituto Colombiano de Normas Técnicas y Certificación)** es el Organismo Nacional de Normalización de Colombia. Entre sus labores se destaca la creación de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales.
- **SGSI: (Sistema de Gestión de la Seguridad de la Información)** es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
- **Planear-Hacer-Chequear-Actuar (PDCA):** Plan (*planificar*): es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados. Do (*hacer*): es una

fase que envuelve la implantación y operación de los controles. Check (*controlar*): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI. Act (*actuar*): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

- **ISO/IEC 17799:2000:** (denominada también como ISO 27002) es un estándar para la seguridad de la información.
- **Zip drive:** Dispositivo periférico que almacena datos en disquetes especiales llamados Zip con capacidades de más de 100 MB.
- **Tarjetas PCM-CIA:** Están diseñadas para ciertos tipos de estándares de redes inalámbricas, por lo que tienen una velocidad máxima de transmisión de datos en bits por segundo (bps) acorde al estándar.
- **HTML: (HyperText Markup Language)** Es un estándar que sirve de referencia para la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código para la definición de contenido de una página web, como texto, imágenes, videos, entre otros.
- **PHP:** Es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.
- **DRUPAL:** Es un sistema dinámico: en lugar de almacenar sus contenidos en archivos estáticos en el sistema de ficheros del servidor de forma fija, el contenido textual de las páginas y otras configuraciones son almacenados en una base de datos y se editan utilizando un entorno Web.
- **WORDPRESS:** Es un sistema de gestión de contenidos o CMS (por sus siglas en inglés, Content Management System) enfocado a la creación de cualquier tipo de sitio, aunque ha alcanzado una gran relevancia usado para la creación de blogs.
- **JAVA:** Es un lenguaje de programación de propósito general, concurrente, orientado a objetos que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible.

- **JOOMLA:** Es un sistema de gestión de contenidos que permite desarrollar sitios web dinámicos e interactivos. Permite crear, modificar o eliminar contenido de un sitio web de manera sencilla a través de un "panel de administración".
- **PENTAHO:** Se define como una plataforma de BI “orientada a la solución” y “centrada en procesos” que incluye todos los principales componentes requeridos para implementar soluciones basados en procesos y ha sido concebido desde el principio para estar basada en procesos.
- **FILESERVER:** Es un ordenador conectado a una red que tiene el objetivo principal de proporcionar una ubicación para el acceso al disco compartido, es decir, de almacenamiento compartido de archivos de computadora que se puede acceder por las estaciones de trabajo que están conectados a la misma red de ordenadores.
- **EDM:** Evaluar, Orientar y Monitorizar, Asegura el establecimiento y mantenimiento del marco de referencia de gobierno, la entrega de beneficios, la optimización del riesgo, la optimización de recursos, y la transparencia hacia las partes interesadas.
- **APO:** Alinear, Planificar y Organizar, Gestiona el marco de gestión de TI, la estrategia, la arquitectura empresarial, la innovación, el portafolio, el presupuesto y los costes, los recursos humanos, las relaciones, los acuerdos de servicio, los proveedores, la calidad, el riesgo, la seguridad.
- **BAI:** Construcción, Adquisición e Implementación, Gestiona programas y proyectos, la definición de requisitos, la identificación y construcción de soluciones, la disponibilidad y la capacidad, la introducción del cambio organizativo, los cambios, la aceptación del cambio y la transición, el conocimiento, los activos, la configuración.
- **DSS:** Entregar, dar Servicio y Soporte, Gestiona operaciones, peticiones e incidentes de servicio, problemas, la continuidad, servicios de seguridad, controles de procesos de negocio.

- **Centos:** Es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente publicado por Red Hat.
- **Root:** Es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos (mono o multiusuario).
- **DNS:** Es una abreviatura para Sistema de nombres de dominio (Domain Name System), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios.
- **Apache:** Es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual.
- **shell de GNU/Linux:** Es en pocas palabras el entorno de escritorio (DE) o Manejador de Ventanas (WM) que utilizamos para trabajar en nuestros PC's, sin importar la distribución que utilicemos ya sea por medio de GUI's (entornos gráficos) o por la terminal respecto a la interacción que requerimos para poder utilizar los servicios y aplicaciones que ofrecen los sistemas operativos.
- **Prompt:** Es conjunto de caracteres que se muestran en una línea de comandos para indicar que está a la espera de órdenes. Éste puede variar dependiendo del intérprete de comandos y suele ser configurable.
- **SLAs:** Es un acuerdo contractual entre una empresa de servicios y su cliente, donde se define, fundamentalmente, el servicio y los compromisos de calidad.
- **Catalizador:** Un Catalizador es una unidad de cambio que al colocarse en medio de un proceso, este constituye un giro en el camino hacia la dirección que tenía como destino original. Un catalizador se le podría definir como al operador de una función matemática, el cual al ser interpuesto entre dos funciones con objetivos específicos, se les altera

su destino, llegando así, a una tercera función con el cambio realizado por el catalizador.

- **Servidor Svn:** Es un sistema de control de revisiones de código abierto y multiplataforma que se diseñó como sucesor del anterior.
- **Escrow:** Si su negocio depende de un software desarrollado a medida, se debe considerar la colocación de su software en custodia. Escrow, práctica prudente gestión de riesgos con el fin de reducir la exposición al riesgo de su empresa y garantizar la continuidad de sus operaciones del día a día de negocios que dependen en ese software.
- **BCP:** Es el último eslabón de la cadena y se aplica únicamente para proteger las aplicaciones que son vitales para la actividad de la empresa.
- **La matriz de la asignación de responsabilidades:** (RACI por las iniciales de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo).
- **CPU:** La unidad central de procesamiento o unidad de procesamiento central, es el hardware dentro de una computadora u otros dispositivos programables, que interpreta las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema.

ANEXOS

Anexo 1 PRESENTACIÓN Y UTILIZACIÓN DE LA INFORMACIÓN

Anexo 2 SOLICITUD DE RESTAURACIÓN

Anexo 3 DATOS DE CARGA OPERACIONAL

Anexo 4 INSTALACIÓN DEL SISTEMA OPERATIVO

Anexo 5 CONFIGURACIÓN DEL SERVIDOR BACULA

Anexo 6 CONFIGURACIÓN DE LAS TAREAS PROGRAMADAS