UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CARRERA DE SISTEMAS INFORMÁTICOS

"ANÁLISIS DE LA SEGURIDAD FÍSICA DEL SERVIDOR Y BACKUP DE BASE DE DATOS, EN LA COOPERATIVA JARDÍN AZUAYO"

Estudiante

Freddy Rafael Bermeo Aucay

Tutor

Ing. Marco Litúma

Cuenca – Ecuador

Noviembre 2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Ing. Marco Litúma Orellana

Director de Tesis

CERTIFICA:

Que el presente trabajo de investigación **"Análisis de la seguridad física del servidor y backup de base de datos, en la Cooperativa Jardín Azuayo",** realizado por el Sr. Freddy Rafael Bermeo Aucay, egresado de la Facultad de Sistemas Informáticos, se ajusta a los requerimientos técnico-metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 30 de Noviembre de 2011

_____

Ing. Marco Litúma Orellana

DIRECTOR DE TESIS

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIÓN DE DERECHOS

Yo, FREDDY RAFAEL BERMEO AUCAY, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Cuenca, 30 de Noviembre de 2011

_____

Freddy Rafael Bermeo Aucay.

C.I: 010447285-7

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORÍA

Los contenidos, argumentos, exposiciones, conclusiones son de Responsabilidad del autor.

_____

Freddy Rafael Bermeo Aucay.

C.I: 010447285-7

DEDICATORIA

Este trabajo está dedicado principalmente a mi Dios quien ha sido la persona que desde allá arriba a guiado mi camino, a mi hijo Matías, que ha sido el aliento para continuar es esta camino tan duro, a toda mi familia quienes de una u otra forma han contribuido con este esfuerzo, sacrificio, y dedicación, también dedicado a todos los maestros quienes han apoyado también a conseguir este logro.

AGRADECIMIENTO

Un agradecimiento muy grande a toda mi familia, a mis amigos y a esas personas que siempre me han apoyado en todo momento.

Un agradecimiento también al docente tutor: el Ing. Marco Litúma, por compartir sus conocimientos y guiarme para alcanzar este objetivo, y sin duda alguna un gran agradecimiento a todos los Profesores de la Universidad Israel quienes me enseñaron sus conocimientos a lo largo de esta carrera.

ÍNDICE GENERAL

Lista de anexos

LISTA DE TABLAS, FIGURAS Y FOTOS

Lista de Tablas

Lista de Figuras

Lista de Fotos

RESUMEN

La seguridad física que debe existir tanto en el servidor principal de base de datos como en sus respectivos respaldos debe ser de gran importancia para la institución, más aun si esta institución es una financiera, pues la base de datos almacena información de gran importancia, pues son datos numéricos.

Una de las mejores soluciones para garantizar la seguridad física del servidor y sus backup de la base de datos, es la creación de un datacenter que almacene a todo lo que tiene que ver con los servidores utilizados en la cooperativa.

La creación de un datacenter es sumamente complejo, pues existen estándares a nivel mundial que se debe regir para poder realizar la creación del mismo, en el cual se deben considerar varios aspectos como son: la infraestructura, seguridad de acceso, equipos internos, sensores contra incendios, entre otras cosas que puede hacer que la empresa invierta mucho dinero en la construcción del mismo.

Igualmente una vez creado el datacenter, también se debe manejar un estándar de administración para poder mantener al datacenter en buen estado, el hecho de tener el datacenter no quiere decir que este ya se va a dejar ahí, al contrario se debe estar realizando periódicamente chequeos para controlar que todo este correctamente funcionando como se lo planteo.

Los backup que se realizan de la base de datos, igualmente tienen su propio espacio físico para poderlos almacenar, este espacio físico también debe

cumplir con cierto requerimientos como los que se realizan en el servidor principal para garantizar que su almacenamiento sea adecuado.

El modo de respaldos depende de cada institución como los desee hacer, pero siempre es necesario un consejo de cómo debería ser el respaldo.

SUMMARY

Physical security should exist in both the main server database as in their backs should be of great importance for the institution, but even if this is a financial institution because the database stores information of great importance, since are numerical data.

One of the best solutions to ensure the physical security of your backup server and the database is the creation of a data center that stores everything that has to do with the servers used in the cooperative.

The creation of a datacenter is extremely complex, because there are global standards that should govern in order to perform its creation, which must consider several aspects such as: infrastructure, access security, internal computers, sensors from fires, among other things that can cause the company to invest heavily in the construction.

Likewise, once created the datacenter, you should also run a management standard to maintain the datacenter in good condition, having the data center does not mean that this is already going to stop there, on the contrary should be making periodic checks to check that everything is correctly working as I put it.

The backup is performed in the database, also have their own physical space so that they can store, this physical space must also meet certain requirements

such as those performed on the primary server to ensure that appropriate storage.

Backup mode depends on the institution as you want to do, but always need advice on how should be the backup.

CAPITULO I

INTRODUCCIÓN

1.1. Planteamiento del problema.

Falta de una correcta seguridad física en el servidor de base de datos y sus backup, que garantice la seguridad de los datos almacenados.

1.2. Antecedentes de la Cooperativa.

La Cooperativa de Ahorro y Crédito Jardín Azuayo nació en Paute, febrero de 1996, en el contexto de la reconstrucción del cantón Paute, luego de los daños causados por el desastre de La Josefina (1993). Empezó con 120 socios fundadores.

La reconstrucción fue una oportunidad para plantear un nuevo estilo de desarrollo con una base en la comunidad que permita mejorar sus formas de producir, se potencie sus capacidades, transforme el ahorro local y extra local en créditos que dinamicen las condiciones de vida del socio (a) y su entorno.

Jardín Azuayo trabaja de manera sostenible y solvente, generando nuevos actores sociales con conciencia ciudadana, solidaria y global, profundizando la confianza, apoyada en sus directivas locales, que permiten consolidarse como una institución propia en cada lugar en el que está presente.

En la actualidad está en la Costa, Sierra y Oriente distribuidos en 27 oficinas (30 puntos de atención) y más de 170.000 socios.

En el año en el que comienza a trabajar la cooperativa, lo hace con un sistema creado en el lenguaje de programación Visual Basic 6.0, y trabajando con una base de datos en SqlServer 7, ya que se trabajaba a nivel local.

En cuanto a visual Basic 6.0, tenía el inconveniente de que funcionaba en tecnología cliente-servidor[1], es decir no podía funcionar de una forma óptima en redes WAN[2] lo que impedía para poder expandirse por más lugares donde lo tenía planeado la cooperativa.

De igual manera el servidor que se utilizaba, era una PC normal, lo que debido a sus seguridades físicas impedía realizar el objetivo antes mencionado de la cooperativa.

Luego de detectar esos inconvenientes de crecimiento, lanza un cambio de sistemas, migrando toda la información de la base de datos a "Oracle[3]", desarrollando aquí también las nuevas interfaces del sistema, e igualmente montando su servidor en un Servidor IBM.

[1]**Cliente-servidor:** aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios
2**WAN:** Una red de área amplia, derivada de la expresión en idioma inglés widearеanetwork
[3]**Oracle:** es un sistema de gestión de base de datos objeto-relacional

Actualmente es así como se encuentra trabajando en la sociedad, teniendo inconvenientes en su servidor de base de datos, pero manteniéndose como la segunda cooperativa más estable del Ecuador.

1.3. Causa – efectos

La falta de seguridad adecuada en el servidor general de base de datos puede traer efectos negativos considerables ya que se puede dar un adulteramiento de la información almacenada teniendo grandes consecuencias esta entidad financiera.

Al igual existe otra causa que es, la falta de seguridad en los respaldos respectivos que se generen del servidor principal que produce una inconsistencia en la información, en caso de que el servidor principal caiga, no se pueda recuperar la información para poder seguir operando normalmente.

Otra causa seria la mala administración del servidor, esto lo realizan las personas seleccionadas para dicha labor, que podrá traer un efecto de perdida enorme para la cooperativa, pues como se dijo anteriormente, aquí está toda la información que mantiene la cooperativa para poder laboral.

CAUSA	EFECTO
Falta en la seguridad del servidor principal de base de datos	Adulteramiento en los datos del servido
Falta en la seguridad de los respaldos respectivos de la base de datos	Información expuesta a terceras personas-.
Mala administración del servidor	Un completo desfase en las seguridades implementadas.

Tabla 1: Causa - efecto

1.4. Sistematización

- **Pronostico**

  Al no tener las respectivas seguridades dentro del servidor de base de datos y sus respectivos respaldos, se está exponiendo toda la información interna de la cooperativa, información que es de gran importancia para el funcionamiento de la misma, y que podría llevar a una pérdida total.

- **Control del pronostico**

  Realizando un análisis de las seguridades actuales tanto en el servidor como en los respaldos, y las seguridades que se debería implementar para evitar el daño a los datos existentes, y poder brindar la seguridad adecuada a todo el servidor y todos sus backup mediante una propuesta que esté de acuerdo a las necesidades encontradas.

1.5. Formulación de la problemática específica

1.5.1. Problema principal

Actualmente la cooperativa no posee las seguridades óptimas para proteger el servidor de base de datos y sus respaldos para garantizar la recuperación de los datos almacenados en dicho servidor.

1.5.2. Problemas secundarios

- Inconsistencia en la información.
- Retiro de fondos por parte de los socios al pensar que pudieran perder sus ahorros.
- Posible gasto en compra de nuevos servidores por robo o daño generado por la falta de seguridad.

1.6. Objetivos

1.6.1. Objetivo general.

Formular una sugerencia para la seguridad del servidor de base de datos, mediante un análisis de las amenazas que atentan contra la seguridad de la base de datos y todos sus respaldos, para poder garantizar la seguridad de dicho servidor.

1.6.2. Objetivos específicos

- Analizar la situación actual.
- Diseñar un data center para mantener los servidores de base de datos en un entorno más adecuado, con sus respectivos procedimientos para administrar un data center.
- Diseñar el esquema y espacio físico para almacenar los respaldos.

1.7. Justificación

1.7.1. Teórica

Para el análisis de las seguridades, comenzamos entendiendo lo que es un servidor y más aún un servidor de base de datos, que no son más que maquinas que brindan información a distintas maquinas que en este caso son denominados clientes.

Un servidor debe ser puesto con grandes seguridades para evitar ser adulterada la información de algún modo e igualmente sus respaldos para poder recuperarla en caso de que sucediera algo con el servidor de base de datos principal.

1.7.2. Metodológica

Me he inclinado por este tema ya que el hecho de laborar en esta institución me ha permitido notar las falencias que existen en el servidor de base de datos, permitiendo elegir este tema para poderlo desarrollar.

CAPITULO II

MARCO DE REFERENCIA

2.1. Marco Teórico

2.1.1. Base de datos

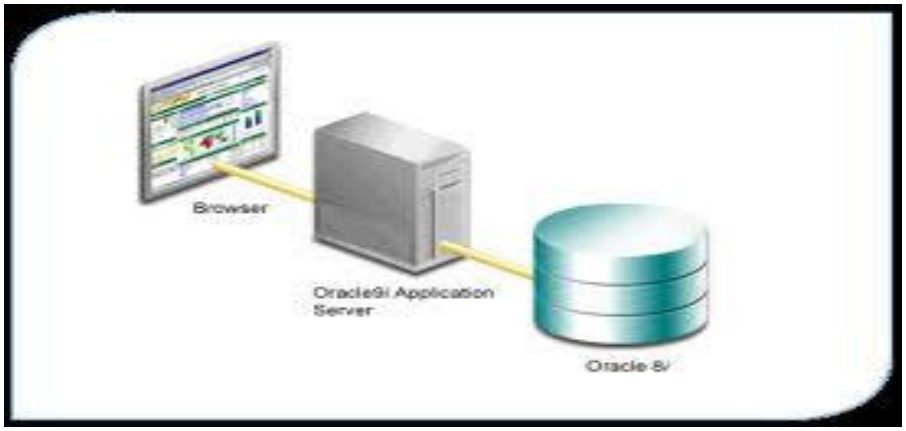


Figura 1: Diagrama de base de datos

“Una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico.”(masadelante)

2.1.1.1. Tipos de base de datos

Las bases de datos pueden clasificarse de varias maneras, de acuerdo al contexto que se esté manejando, la utilidad de las mismas o las necesidades que satisfagan.

- **Según la variabilidad de los datos almacenados**

Bases de datos estáticas

Son bases de datos de sólo lectura, utilizadas primordialmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, realizar proyecciones y tomar decisiones.

Bases de datos dinámicas

Éstas son bases de datos donde la información almacenada se modifica con el tiempo, permitiendo operaciones como actualización, borrado y adición de datos, además de las operaciones fundamentales de consulta.

- **Según el contenido**

Bases de datos bibliográficas

Sólo contienen un subrogante (representante) de la fuente primaria, que permite localizarla. Un registro típico de una base de datos bibliográfica contiene información sobre el autor, fecha de publicación, editorial, título, edición, de una determinada publicación, etc. Puede contener un resumen o extracto de la publicación original, pero nunca el texto completo, porque si no, estaríamos en presencia de una base de datos a texto completo.

Bases de datos de texto completo

Almacenan las fuentes primarias, como por ejemplo, todo el contenido de todas las ediciones de una colección de revistas científicas.

2.1.2. Servidor

"Es una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes."(Walus) (es.wikipedia.org). Un servidor no es necesariamente una máquina de última generación y de grandes proporciones, un servidor puede ser desde cualquier computadora desde una anterior hasta las últimas maquinas en el mercado.

Figura 2: modelo de servidor

2.1.2.1. Tipos de Servidores

Existen diferentes tipos de servidores que se pueden tener dentro de una institución, entre ellos tenemos:

- SERVIDOR DE ARCHIVOS: almacena varios tipos de archivo y los distribuye a otros clientes en la red.

- SERVIDOR DE BASE DE DATOS: Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

  Los sistemas de administración de base de datos (SGBD) generalmente proveen funcionalidades para servidores de base de datos, en cambio otros (como por ejemplo, MySQL) solamente proveen construcción y acceso a la base de datos.

- SERVIDOR DE COMUNICACIONES: Combinación de hardware y software que permite el acceso remoto a herramientas o información que generalmente residen en una red de dispositivos.

- SERVIDOR DE CORREO ELECTRÓNICO: almacena, envía, recibe, enruta[4] y realiza otras operaciones relacionadas con e-mail para los clientes de la red.

- SERVIDOR DE FAX: Un servidor de fax es una solución ideal para organizaciones que tratan de reducir el uso del teléfono pero necesitan enviar documentos por fax.

[4] **Enruta:** se refiere a la selección del camino en una red de computadoras por donde se envían datos

Almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.

- SERVIDOR DE IMPRESIÓN: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.

- SERVIDOR DE LOS SERVICIOS DE DIRECTORIO: es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red.

2.1.3. Servidor de Base de datos.

Figura 3: Servidor de Base de datos

"Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor." (ALEGSA, 1998).

Los datos están interrelacionados y estructurados de acuerdo a un modelo que sea capaz de recoger el máximo contenido Semántico, su finalidad es

servir a una o más aplicaciones de la mejor forma posible. Los datos se almacenan de modo que resulten independientes de los programas que los usan; se emplean métodos para incluir nuevos datos y para modificar o extraer los datos almacenados. La definición y descripción de estos datos, única para cada tipo, han de estar almacenados junto con los mismos.

El mundo real considera interrelaciones entre datos y restricciones semánticas que deben estar presentes en una base de datos. No solo debe almacenar entidades y atributos, sino que también debe almacenar interrelaciones entre datos.

2.1.3.1. Características elementales de un servidor de base de datos

- Integrado: Un servidor de base de datos puede considerarse como una unificación de varios archivos de datos independientes, donde se elimina parcial o totalmente cualquier redundancia entre los mismos.

- Compartido: Se entiende que partes individuales de la Base de Datos pueden compartirse entre varios usuarios distintos, en el sentido que cada uno de ellos puede tener acceso a la misma parte de la Base de Datos y utilizarla con propósitos diferentes, consecuencia del hecho de que la Base de Datos es integrada.

2.1.3.2. Ventajas de los servidores de base de datos

Referencia	Ventajas
Los Datos	· Independencia de estos respecto de los tratamientos y viceversa. · Mejor disponibilidad de los mismos. · Mayor eficiencia en la recogida, codificación y entrada.
Los Resultados	· Mayor coherencia. · Mayor valor informativo. · Mejor y más normalizada documentación de la información.
Los Usuarios	· Acceso más rápido y sencillo de los usuarios finales. • Más facilidades para compartir los datos por el conjunto de los usuarios. · Mayor flexibilidad para atender a demandas cambiantes.

Tabla 2. Ventajas de un servidor de base de datos

2.1.4. Seguridad en base de datos

Figura 4: Seguridad en Datos

En todo sistema abierto, debe proporcionarse un potente mecanismo de seguridad que garantice que ningún intruso pueda acceder o corromper la integridad del sistema. (Universidad de Murcia).

Seguridad en base de datos consiste en las acciones que se debe tomar al momento de crear

la base de datos, y su estructura física, tomando en cuenta el volumen de las transacciones y las restricciones que tiene que especificar en el acceso a los datos; esto permitirá que el usuario adecuado sea quién visualice la información adecuada al igual que el ingreso a personas autorizadas.

2.1.4.1. Tipos de seguridad en servidor de base de datos

En servidores de bases de datos hablaremos de la seguridad a 2 niveles básicos: Seguridad a nivel lógico y seguridad a nivel físico.

- **Seguridad a nivel lógico.**

Dentro de la seguridad a nivel lógico, tenemos dos puntos rescatables como por ejemplo:

Seguridad de Acceso.

La seguridad de acceso se implementará de dos maneras posibles:

Seguridad a nivel de acceso al sistema.

Cuyo caso el SGBD se apoya en la seguridad de entrada al sistema operativo para comprobar la validez del acceso a los datos almacenados.

Seguridad a nivel de objetos de datos.

La seguridad a nivel de objetos entra ya en el detalle del acceso a nivel de creación y administración de objetos de datos: tablas, vistas, índices, relaciones, reglas...etc.

Es decir, las responsabilidades y acciones que puede hacer el usuario en el esquema de la base de datos.

Seguridad a nivel de datos

La seguridad a nivel de datos entra ya en la capa de la información en sí. En la que indicaremos quién puede acceder a qué información para su consulta, actualización, inserción o borrado.

Las características de los diversos motores determinarán hasta qué grado de seguridad se llega en este apartado.

2.1.5. Backup o respaldo del servidor de base de datos.

Figura 5: Backup

Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo, como ser discos duros, CDs, DVDs o cintas magnéticas (DDS, Travan, AIT, SLR, DLT y VXA).

Los backups se utilizan para tener una o más copias de información considerada importante y así poder recuperarla en el caso de pérdida de la copia original.

Es evidente que es necesario establecer una política adecuada de copias de seguridad en cualquier organización; al igual que sucede con el resto de equipos y sistemas, los medios donde residen estas copias tendrán que estar protegidos físicamente; de hecho quizás deberíamos de emplear medidas más fuertes, ya que en realidad es fácil que en una sola cinta haya copias de la información contenida en varios servidores.

Para proteger más aun la información copiada se pueden emplear mecanismos de cifrado, de modo que la copia que guardamos no sirva de nada si no disponemos de la clave para recuperar los datos almacenados.

(ALEGSA, 1998)

2.1.5.1. Tipos de Backup

- **Backups completos**

El tipo de operación de backup más básico y completo es el backup completo. Como su propio nombre indica, este tipo de backup copia la totalidad de los datos en otro juego de soportes, que puede consistir en cintas, discos, o en un DVD o CD.

La ventaja principal de la realización de un backup completo en cada operación es que se dispone de la totalidad de los datos en un único juego de soportes. Esto permite restaurar los datos en un tiempo mínimo, lo cual se mide en términos de objetivo de tiempo de recuperación (RTO).

No obstante, el inconveniente es que lleva más tiempo realizar un backup completo que de otros tipos (a veces se multiplica por un factor 10 o más), y requiere más espacio de almacenamiento.

Por lo tanto, sólo se suelen realizar backups completos periódicamente. Los centros de datos que manejan un volumen de datos (o de aplicaciones críticas) reducido pueden optar por realizar un backup completo cada día, o más a menudo aún en ciertos casos. Lo normal es que en las operaciones de backup se combine el backup completo con backups incrementales o diferenciales.

- **Backups incrementales**

Una operación de backup incremental sólo copia los datos que han variado desde la última operación de backup de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último backup. Las aplicaciones de backup identifican y registran la fecha y hora de realización de las operaciones de backup para identificar los archivos modificados desde esas operaciones.

Como un backup incremental sólo copia los datos a partir del último backup de cualquier tipo, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de un backup incremental es que copia una menor cantidad de datos que un backup completo. Por ello, esas operaciones se realizan más deprisa y exigen menos espacio para almacenar el backup.

- **Backups diferenciales**

Una operación de backup diferencial es similar a un backup incremental la primera vez que se lleva a cabo, pues copiará todos los datos que hayan cambiado desde el backup anterior.

Sin embargo, cada vez que se vuelva a ejecutar, seguirá copiando todos los datos que hayan cambiado desde el anterior completo. Por lo tanto, en las operaciones subsiguientes almacenará más datos que un backup incremental, aunque normalmente muchos menos que un backup completo.

Además, la ejecución de los backups diferenciales requiere más espacio y tiempo que la de los backups incrementales, pero menos que la de los backup completos.(SearchStorage, 2010)

2.2. Marco Temporal / Espacial

El análisis y la propuesta de seguridades en servidor y respaldo de la base de datos de la cooperativa se lo realizaran dentro de su propia instalación, ubicada en la Sucre 6-46 y Hermano Miguel.

El tiempo estimado para en análisis y propuesta está determinado para tres meses, tiempo en el cual se dará la sugerencia para mejorar las falencias encontradas.

2.3. Marco Legal

Este análisis se encuentra dentro de todos los ámbitos legales, con las respectivas autorizaciones del área en la cual se basa la investigación.

Por lo que podemos decir que es un análisis completamente legal, y toda la información puesta es verídica y podría ser constatada en cualquier momento.

La información de análisis y la propuesta de funcionamiento está basada en **"La ley de comercio Electrónico, Firmas Electrónicas y Seguridad informática"**, donde en base al **Título V: "De las Infracciones Informáticas"**, no basamos en los artículos: 57, 58, 59 de infracciones informáticas, así como en el artículo 61: Daños Informáticos.

CAPITULO III

METODOLOGÍA

3.1. Metodología de investigación

3.1.1. Tipo de investigación.

Para el desarrollo de este análisis se desarrollara un proceso metodológico, para ello utilizaremos el tipo de investigación descriptiva, mediante la cual llegaremos a conocer las situación actuales, las costumbres de cómo se manejan en el servidor de base de datos, etc., mediante la descripción exacta de las actividades que se desarrollan al interior de la cooperativa.

3.1.2. Método

3.1.2.1. Método histórico-lógico

Este es uno de los métodos más apropiados para el desarrollo de este análisis puesto que nos permite determinar datos históricos, y poder centrarlos a la realidad en la que se encuentra determinado tema.

Con este método lograremos descubrir los errores o inconvenientes que se producían anteriormente, y los que se siguen produciendo, para poder encontrar la mejor alternativa de solución.

3.1.3. Técnica

3.1.3.1. La encuesta

La técnica que se utilizara para el desarrollo del análisis será la encuesta personal, esta nos servirá para poder recolectar la información de algunas personas que nos podrá servir de gran ayuda para analizar todas las seguridades que están personas consideran son las adecuadas, mediante un formulario que se establecerá con anticipación, para poder generar una tabla estadística de lo antes mencionado.

Mediante la encuesta lo que se pretende, es poder de alguna manera tabular la información que se nos sea proporcionada por parte de los encuestados, para saber cómo observan ellos el problema a ser analizado por nosotros.

Para realizar esta encuesta utilizaremos un formato, que es mediante el cual lo realizaremos a las personas que trabajan dentro de la cooperativa específicamente dentro de todo lo que es el área involucrada con sistemas, como son: Telecomunicaciones, infraestructura, ingeniería, desarrollo y producción.

Al realizar la encuesta a las áreas señaladas anteriormente, estamos consiguiendo que nuestra información a obtener sea más concreta y más acertada con la realidad que se está viviendo dentro de la institución.

Las preguntas puestas en la encuesta han sido tomadas en referencia a nuestro tema de investigación.

El formato definido para esta encuesta es el siguiente:

Encuesta interna para conocer el actual estado del servidor de Base de Datos y poder sugerir una solución en caso de encontrar las falencias.

Señale con una X, la opción que Ud. cree es la verdadera

1. **¿Qué opina del actual espacio donde se encuentra el servidor de Base de Datos?**
   a. **Malo** ☐
   b. **Regula** ☐
   c. **Bueno** ☐

2. **¿Cree que es el ambiente apropiado para el funcionamiento de dicho Servidor?**
   a. **Si** ☐
   b. **No** ☐

3. **¿Cómo es la seguridad del espacio donde está el servidor de Base de Datos?**
   a. **Malo** ☐
   b. **Regula** ☐
   c. **Bueno** ☐

4. **¿Cree que se debería mejorar las actuales seguridades del espacio donde se encuentra dicho servidor?**
   a. **Si** ☐
   b. **No** ☐

5. **¿Cree que los respaldos que se realizan del servidor principal de base de datos son los adecuados?**
   a. **Si** ☐
   b. **No** ☐

6. **¿El lugar donde se almacenan los respaldos son los óptimos para garantizar su seguridad?**
   a. **Si** ☐
   b. **No** ☐

7. **¿Existen seguridades físicas donde se almacenan los respaldos de información?**
   a. **Si** ☐
   b. **No** ☐

8. **¿Cree conveniente readecuar la actual situación tanto del servidor de base de datos principal como sus respaldos?**
   a. **Si** ☐
   b. **No** ☐

9. **¿Se debe mejorar las seguridades físicas de dicho servidor y sus respaldos?**

   a. **Si** ☐

   b. **No** ☐

10. **¿Cree que el diseñar un Data Center será una buena opción para el servidor de base de datos y sus respaldos?**

    a. **Si** ☐

    b. **No** ☐

Agradecemos sus opiniones y comentarios, mediante esta encuesta hemos obtenido información para poder desarrollar nuestros objetivos planteados.

Realizado por: Freddy Bermeo.

Tabla 3: Modelo de la encuesta a realizar

Con el modelo indicado lo que se pretende es tabular los datos obtenidos para ser analizados y poder cambiar la actual forma de llevarlos o a su vez mejorar los actuales procedimientos dentro de la Cooperativa.

3.2. Resultado de la encuesta

A continuación realizaremos una tabulación de los datos obtenidos luego de realizar la encuesta según el modelo de la tabla 4.0.

Para la obtención de los datos se encuestaron a un total de 30 personas, de las diferentes áreas el cual mostramos en la tabla 5.0

Departamento	**# de personas**	**Porcentaje**
Telecomunicaciones	2	6.67%
Infraestructura	3	10.00%
Ingeniería	21	70.00%
Desarrollo y Producción	4	13.33%
Total	**30**	**100%**

Tabla 4: Cantidad de personas encuestadas en sus departamentos.

3.3. Tabulación de las preguntas de la encuesta.

3.3.1. **Pregunta 1:**

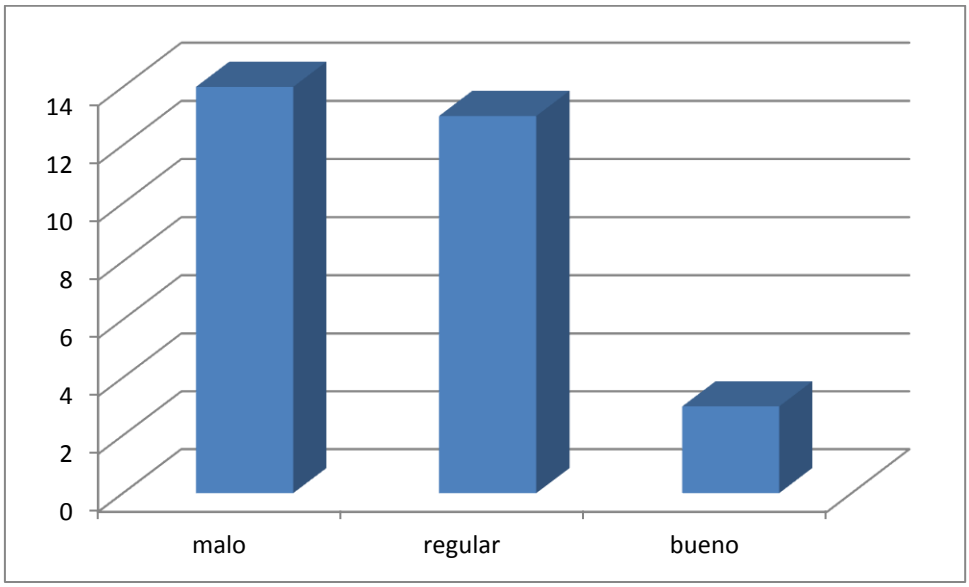
¿Qué opina del actual espacio donde se encuentra el servidor de Base de Datos?

En esta pregunta sobresale la opción mala, con un total de 14 personas (46,67%), las cuales opinan que el espacio actual se encuentra en malas condiciones, seguido muy cerca por la opción de regular con un total de 13 personas (43,33%), y tan solo 3 personas (10,00%) opinan que el espacio es adecuado.

Opción	**# de personas**	**porcentaje**
Bueno	14	46.64 %
Regular	13	43.33 %
Malo	3	10 %
Total	**30**	100 %

Tabla 5: Tabulación pregunta 1.

Figura 6. Resultados de la pregunta número 1 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis del grafico 1.0.**

Según la tabulación de los datos podemos darnos cuenta claramente que la actual situación física donde se encuentra el servidor de base de datos no es la más óptima para su funcionamiento.

3.3.2. Pregunta 2:

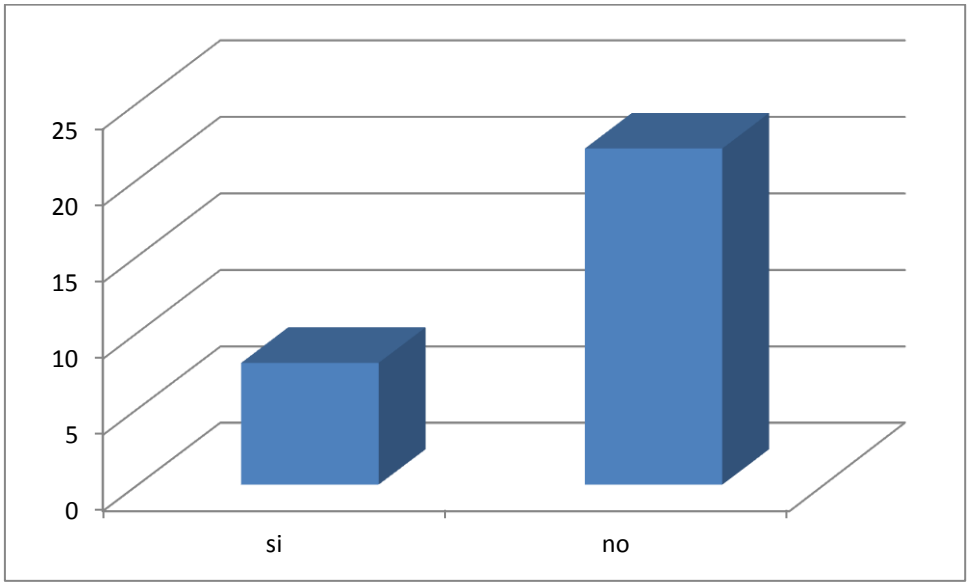
¿Cree que es el ambiente apropiado para el funcionamiento de dicho Servidor?

En la segunda pregunta, el no con un total de 22 personas (73,33%) coinciden en que el ambiente no es el apropiado para el servidor de base de datos, mientras que un total de 8 personas (26,67), opina lo contrario.

Opción	**# de personas**	**Porcentaje**
Si	8	26.67 %
No	22	73.33 %
Total	**30**	**100 %**

Tabla 6: Tabulación pregunta 2.

Figura 7. Resultados de la pregunta número 2 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 2 de la encuesta**

Luego de tabular los datos de esta pregunta, deducimos que las personas que tienen acceso a verificar como es el ambiente donde se encuentra el servidor coinciden en que no es el más apropiado.

3.3.3. Pregunta 3:

¿Cómo es la seguridad del espacio donde está el servidor de Base de Datos?

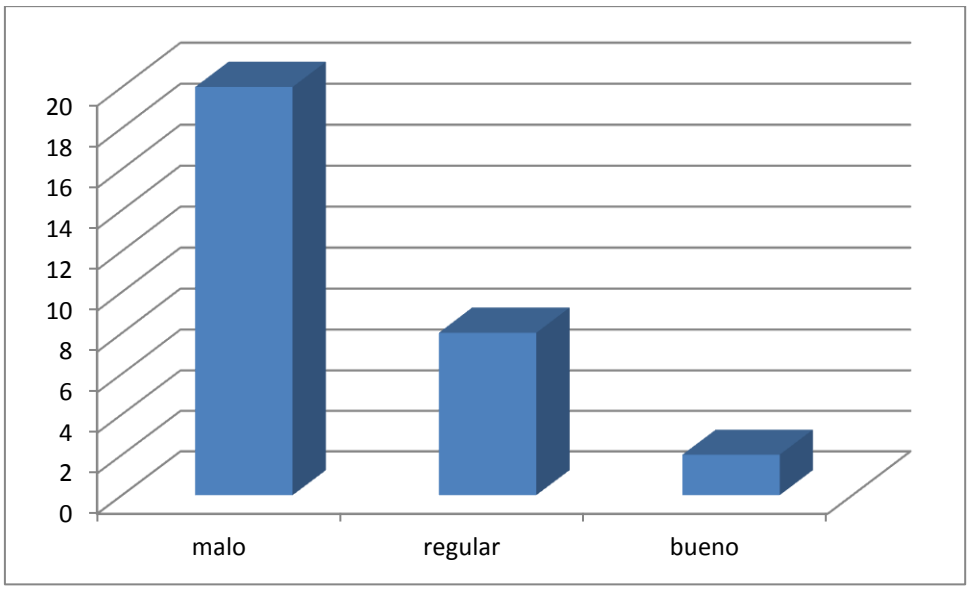
En la pregunta, sobresale la opción mala, con un total de 20 personas (66,67%), las cuales opinan que la seguridad donde está el servidor es mala, seguido muy cerca por la opción de regular con un total de 8

personas (26,67%), y tan solo 2 personas (6,67%) opinan que la seguridad es buena.

Opción	# de personas	Porcentaje
Bueno	20	66.67 %
Regular	8	26.67 %
Malo	2	6.67 %
Total	**30**	**100 %**

Tabla 7: Tabulación pregunta 3.

Figura 8. Resultados de la pregunta número 3 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 3 de la encuesta**

Evidentemente la seguridad del servidor de base de datos no es la más adecuada, lo que significaría que estamos poniendo en riesgo la información.

3.3.4. Pregunta 4:

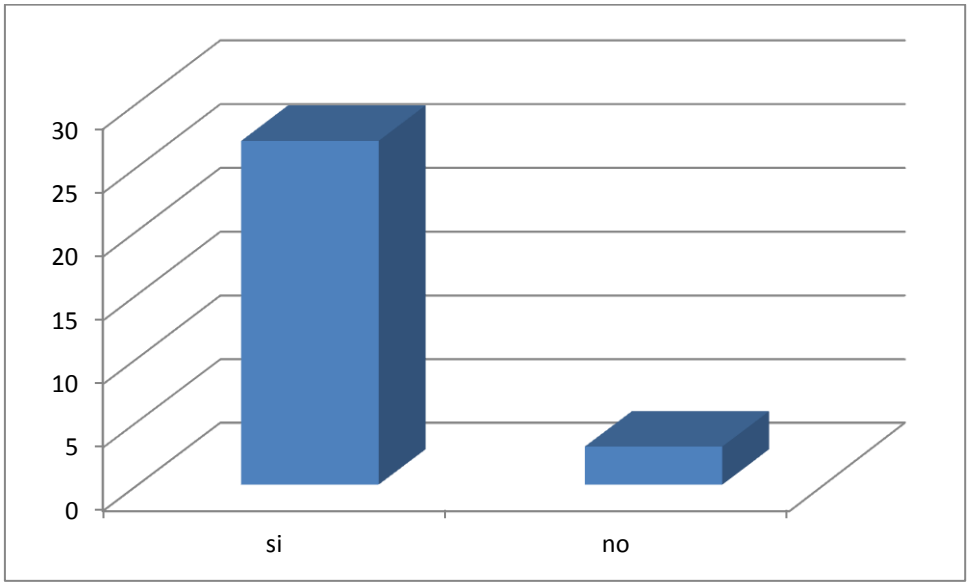
¿Cree que se debería mejorar las actuales seguridades del espacio donde se encuentra dicho servidor?

En esta pregunta 27 personas (90,00%) coinciden en que se debería mejorar las seguridades actuales del servidor, mientras que 3 personas (10,00%) creen que ahí está seguro.

Opción	# de personas	Porcentaje
Si	27	90 %
No	3	10 %
Total	**30**	**100 %**

Tabla 8: Tabulación pregunta 4.

Figura 9. Resultados de la pregunta número 4 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 4 de la encuesta**

  Sin duda alguna la mayoría de personas que tienen conocimiento sobre el tema apoyan la moción de mejorar las actuales seguridades del servidor de base de datos.

3.3.5. Pregunta 5:

¿Cree que los respaldos que se realizan del servidor principal de base de datos son los adecuados?

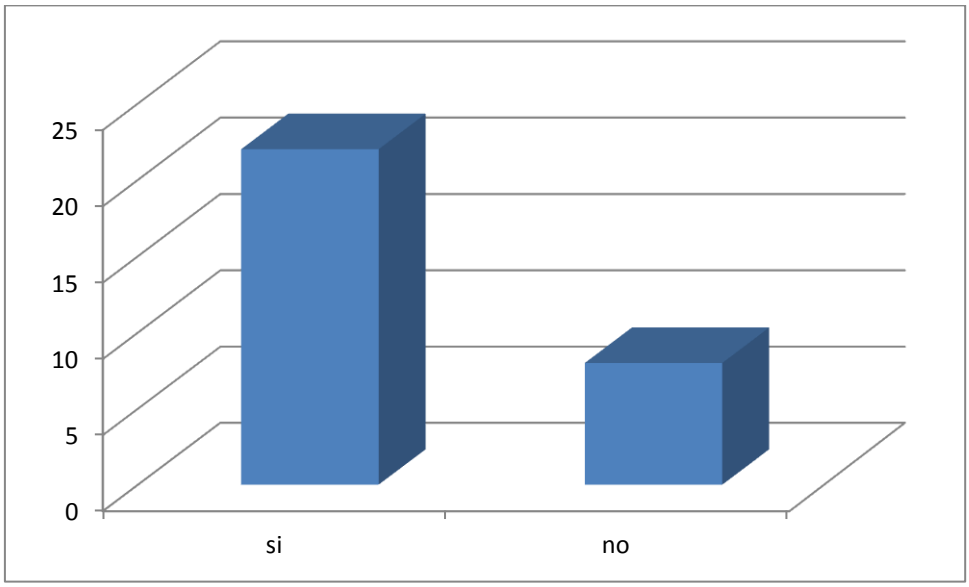
Aquí en esta pregunta, 22 personas encuestadas (73,33%), opina que los respaldos que se realizan del servidor principal de base de datos con los adecuados para garantizar que se puedan recuperar los datos en

caso de alguna circunstancia con el servidor principal, mientras que tan solo 8 opinan lo contrario.

Opción	# de personas	Porcentaje
Si	22	73.33 %
No	8	26.67 %
Total	**30**	**100 %**

Tabla 9: Tabulación pregunta 5.

Figura 10. Resultados de la pregunta número 5 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 5 de la encuesta**

Al tabular la opinión de las personas que tienen un mayor contacto con el servidor de base de datos, podemos darnos cuenta que la información actualmente donde se respalda no es la forma más óptima para garantizar su seguridad y garantizar que los datos no se pierdan.

3.3.6. Pregunta 6:

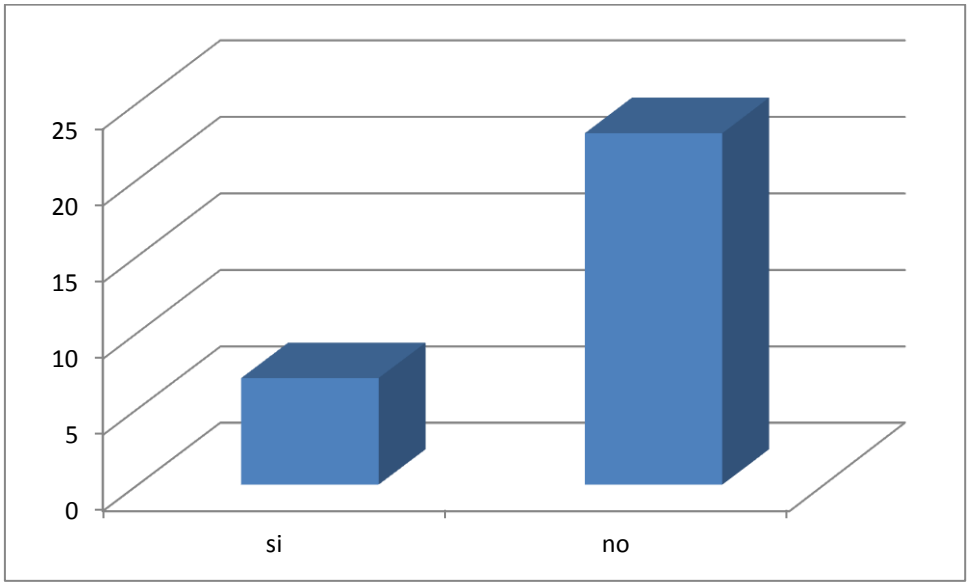
¿El lugar donde se almacenan los respaldos son los óptimos para garantizar su seguridad?

De un total de 30 personas encuestadas (100%), 23 personas (76,67%) opina que los espacios físicos donde se almacenan la información no es segura para garantizar que los datos respaldados reposen en un buen lugar, y tan solo 7 personas (23,33%) dicen que el actual espacio físico es adecuado.

Opción	**# de personas**	**Porcentaje**
Si	7	23.33 %
No	23	76.67 %
Total	**30**	**100 %**

Tabla 10: Tabulación pregunta 6.

Figura 11. Resultados de la pregunta número 6 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 6 de la encuesta**

  Analizando los resultado tabulados en el grafico 6.0, se puede deducir fácilmente que es necesario mejorara los espacios físicos en donde son almacenados los respaldos, para poder garantizar la seguridad en la información respaldada.

3.3.7. Pregunta 7:

¿Existen seguridades físicas donde se almacenan los respaldos de información?

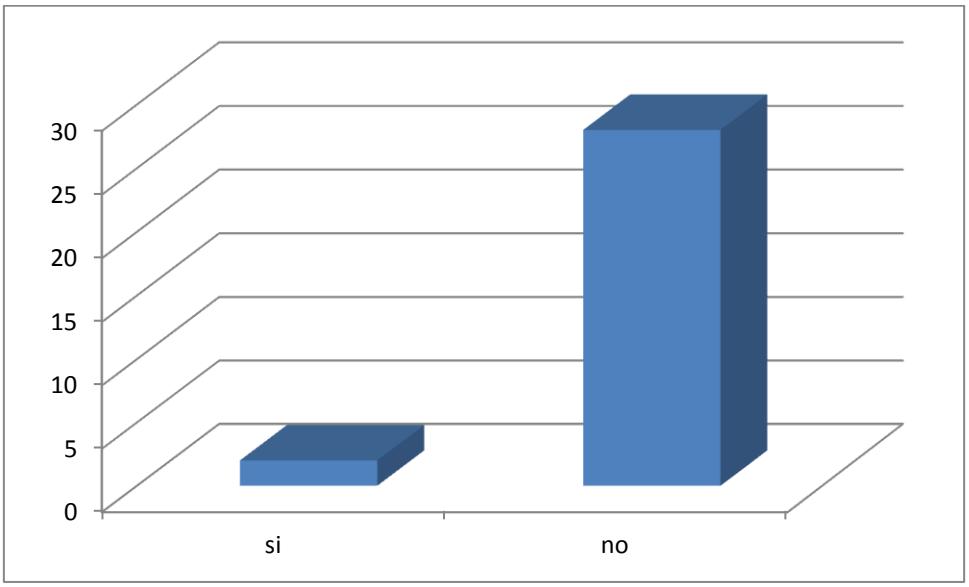
28 personas (93,33%) coinciden en que no existen seguridades físicas del lugar donde se almacenan los respaldos de información del servidor

de base de datos, mientras que tan solo el 6,67%, equivalente a 2 personas piensan que si existen dichas seguridades.

Opción	# de personas	Porcentaje
Si	2	6.67 %
No	28	93.33 %
Total	**30**	**100 %**

Tabla 11: Tabulación pregunta 7.

Figura 12. Resultados de la pregunta número 7 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 7 de la encuesta**

Evidentemente es necesario actuar rápidamente para mejorar las seguridades físicas del lugar donde se almacenen los respaldos, pues esta información es la que mantiene a la cooperativa a flote ante la sociedad.

3.3.8. Pregunta 8:

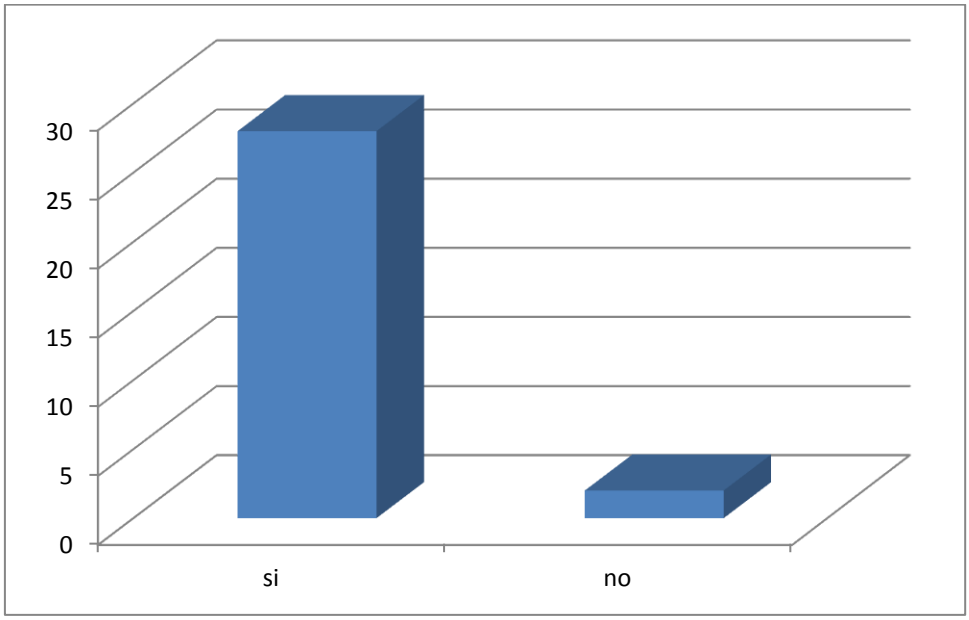
¿Cree conveniente readecuar la actual situación tanto del servidor de base de datos principal como sus respaldos?

Un total de 28 personas equivalente al 93,33%, cree que la mejor opción para mejorar las seguridades físicas, tanto del servidor de base de datos como de sus respaldos seria readecuar el aspecto físico, mientras que 2 personas (6,67%) creen que no sería buena idea readecuar el espacio físico.

Opción	**# de personas**	**Porcentaje**
Si	28	93.33 %
No	2	6.67 %
Total	**30**	**100 %**

Tabla 12: Tabulación pregunta 8.

Figura 13. Resultados de la pregunta número 8 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 8 de la encuesta**

  Sin duda alguna la mejor opción para mejorar la seguridad tanto del servidor principal de base de datos como sus respaldo, será readecuar o a su vez construir uno para garantizar la información contenida en ellos.

3.3.9. Pregunta 9:

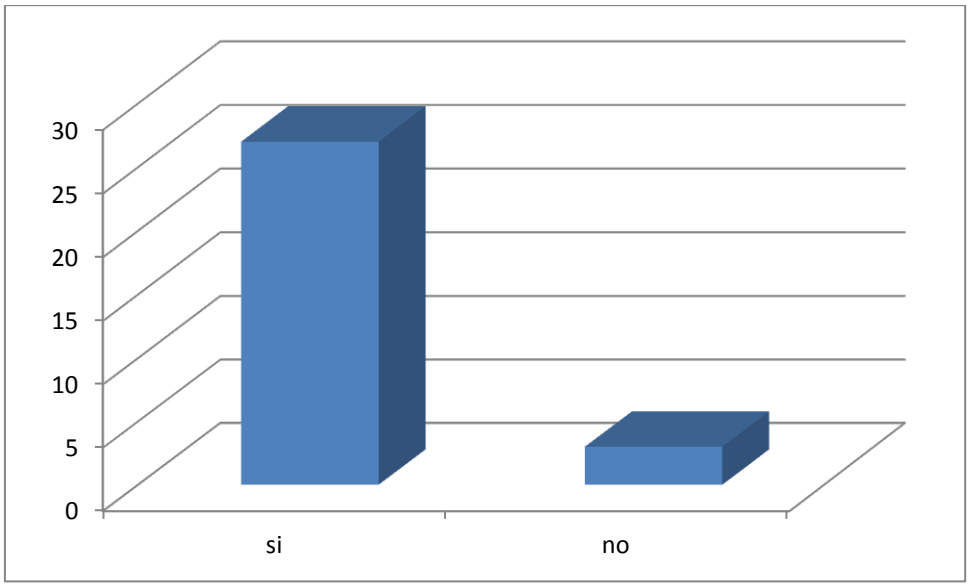
¿Se debe mejorar las seguridades físicas de dicho servidor y sus respaldos?

Un total de 27 personas (90%), cree que es conveniente mejorar las seguridades físicas, mientras que 3 personas (10%), creen que donde se encuentran están seguros.

Opción	# de personas	Porcentaje
Si	27	90 %
No	3	10 %
Total	**30**	**100 %**

Tabla 13: Tabulación pregunta 9.

Figura 14. Resultados de la pregunta número 9 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 9 de la encuesta**

Tomando en cuenta las anteriores preguntas, y en especial la anterior (8) y según el grafico 9.0. Vemos que el 90% de las personas encuestadas ven la necesidad inmediata de mejorar las seguridades de los servidores nombrados anteriormente.

3.3.10. Pregunta 10:

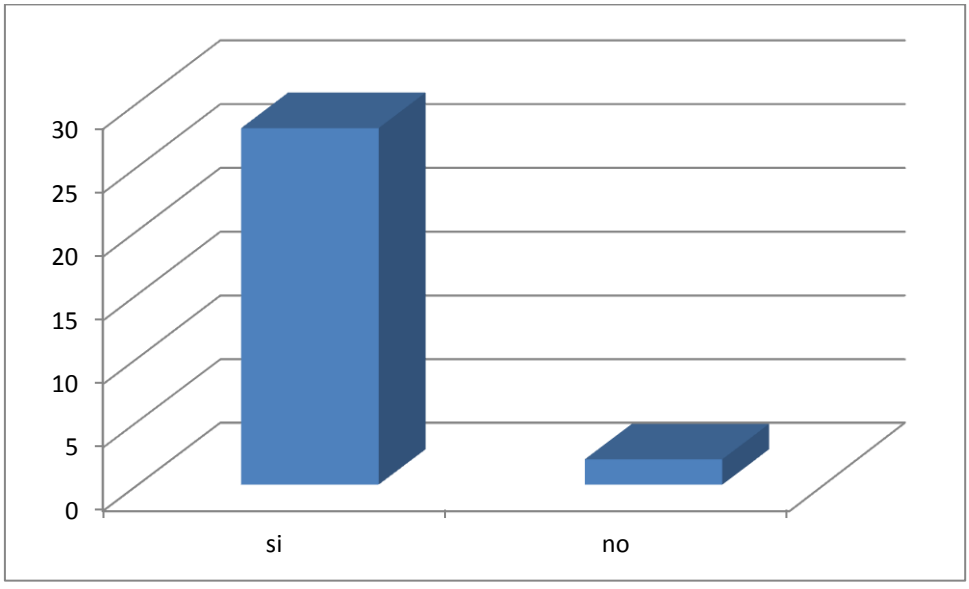
¿Cree que el diseñar un Data Center será una buena opción para el servidor de base de datos y sus respaldos?

28 personas (93,33%) de las personas encuestadas piensan que sería una buena opción, mientras que 2 personas (6,67%), piensan que no habría ningún cambio.

Opción	# de personas	Porcentaje
Si	28	93.33 %
No	2	6.67 %
Total	**30**	**100 %**

Tabla 14: Tabulación pregunta 10.

Figura 15. Resultados de la pregunta número 10 de la encuesta.



Fuente: resultados de la encuesta realizado en el área de sistemas

Realizado por: Freddy Bermeo.

- **Análisis de la pregunta 10 de la encuesta**

Según las respuestas dadas en esta última pregunta de la encuesta, más de un 90% ha creído conveniente el crear un data center (centro de datos), que pueda mejorar todas las falencias encontradas según la encuesta y mejorar la seguridad tanto del servidor de base de datos como de sus respaldo, así mismo las dos personas en contra de esta alternativa creen que el desarrollar un data center no garantizara la seguridad de los datos.

CAPITULO IV

ANÁLISIS DE LA SITUACIÓN FÍSICA ACTUAL

4.1. Servidor principal

Toda la información de la cooperativa está en una base de datos Oracle, versión 10g, pero será migrada en un futuro a Oracle 11g.

Esta base de datos tiene dos funciones y es por eso que está dividida en dos partes denominadas:

- **Producción y base de datos**

  Esta función la utilizan los departamentos de Software de base de datos, Administración de base de datos, donde se encuentran los administradores de sistema operativos, cuchillas, optimización de la base, etc.

- **Hardware**

  Donde interviene todo el departamento de infraestructura.

Esta base de datos está montada en un Servidor IBM, la arquitectura de este servidor es la “Blade”, ya que esta permite compactarse en un espacio más pequeño, además de su mayor simplicidad al momento de operar y por algunas ventajas que brinda esta arquitectura.

Este servidor tiene un procesador power PC7, y el modelo es un P7-01,

4.2. Infraestructura.

El cuarto de servidor como se lo denomina en la cooperativa es un cuarto improvisado para su funcionamiento, por ende la infraestructura donde se encuentra el servidor principal de base de datos es sumamente reducida es por eso que la mejor opción en cuanto al servidor de base de datos fue usar un servidor “Blade”, por su tamaño reducido.

En cuanto a la ubicación del servidor, este está en una situación poco favorable para su seguridad y óptimo rendimiento pues la altura que debería tener para garantizar su funcionamiento no es la adecuada en caso de que en el interior de dicho lugar existiera alguna fuga de agua o algo relacionado que pudiera afectar a este servidor.

Las paredes que rodean al servidor están en condiciones poco favorables pues ya están desmoronándose poco a poco por su mal estado, al igual que su techo se ve que ya posee pequeñas abertura por donde se podría dar algún ingreso ya sea de agua, polvo, que pueden dañar el servidor.

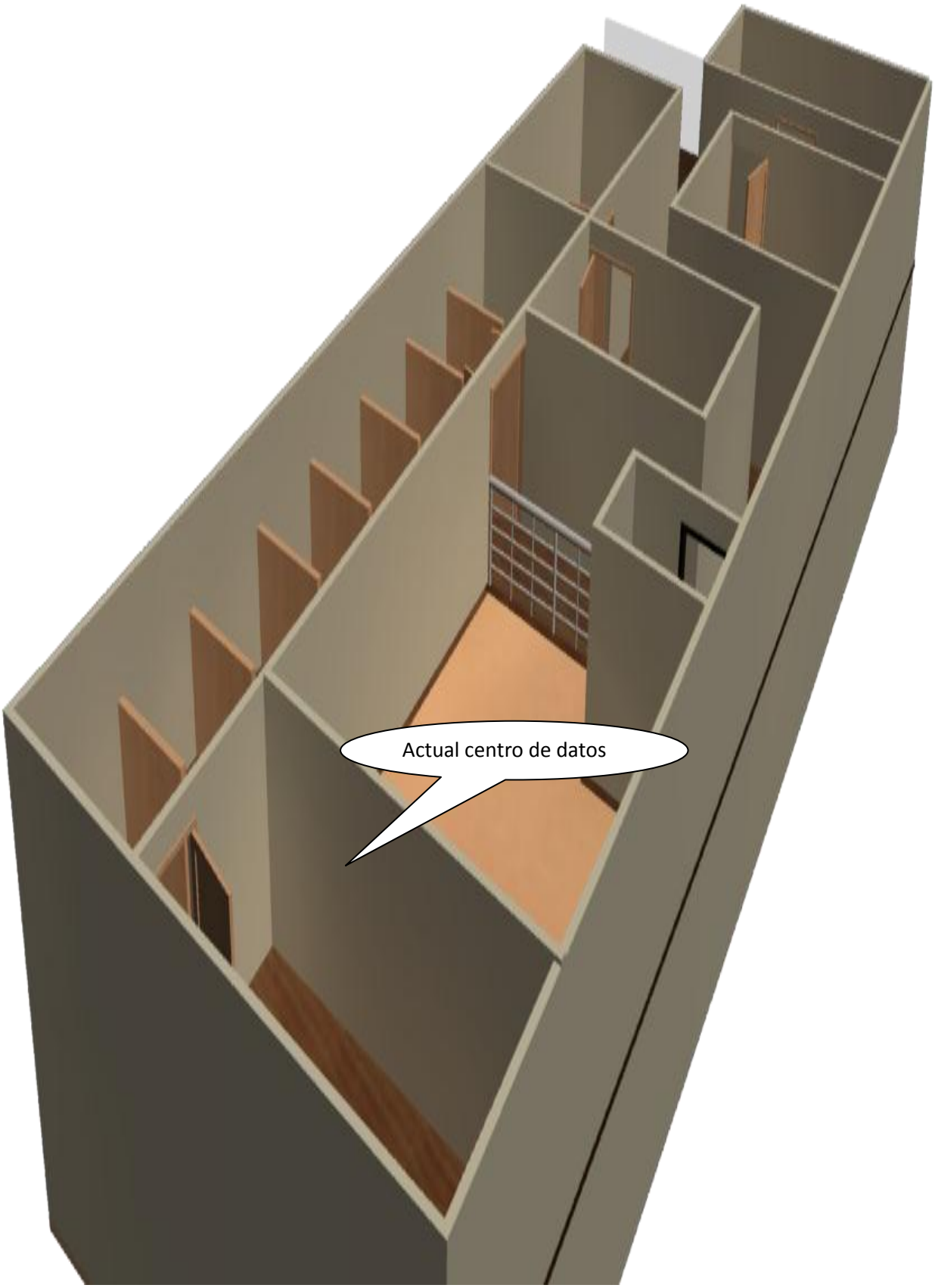


Figura 16: Plano actual Centro de Datos

4.3. Situación climática.

Haciendo referencia a la situación climática dentro del lugar donde se encuentra el servidor principal de base de datos, esta no cuenta con un sistema de refrigeración apropiado para el correcto desenvolvimiento del servidor, pues con lo único que cuenta este lugar es con un ventilador para enfriar todo los equipos utilizados en dicho servidor.

Foto 1: Equipo de Refrigeración.

Fuente: Cooperativa Jardín Azuayo.

No cuenta con un sistema de aire acondicionado lo que pone en riesgo al servidor en caso de posible calentamiento exponiendo toda la información a una posible perdida.

4.4. Rack de servidores y cableado de red

La actual situación del rack donde se encuentran todos los servidores y principalmente nuestro objetivo a investigar como lo es el servidor de base de datos, se encuentra saturado debido a su poco espacio físico lo que ha

dificultado la adquisición de otro rack para poder mermar sus cargas y poder administrarlo de la mejor manera.

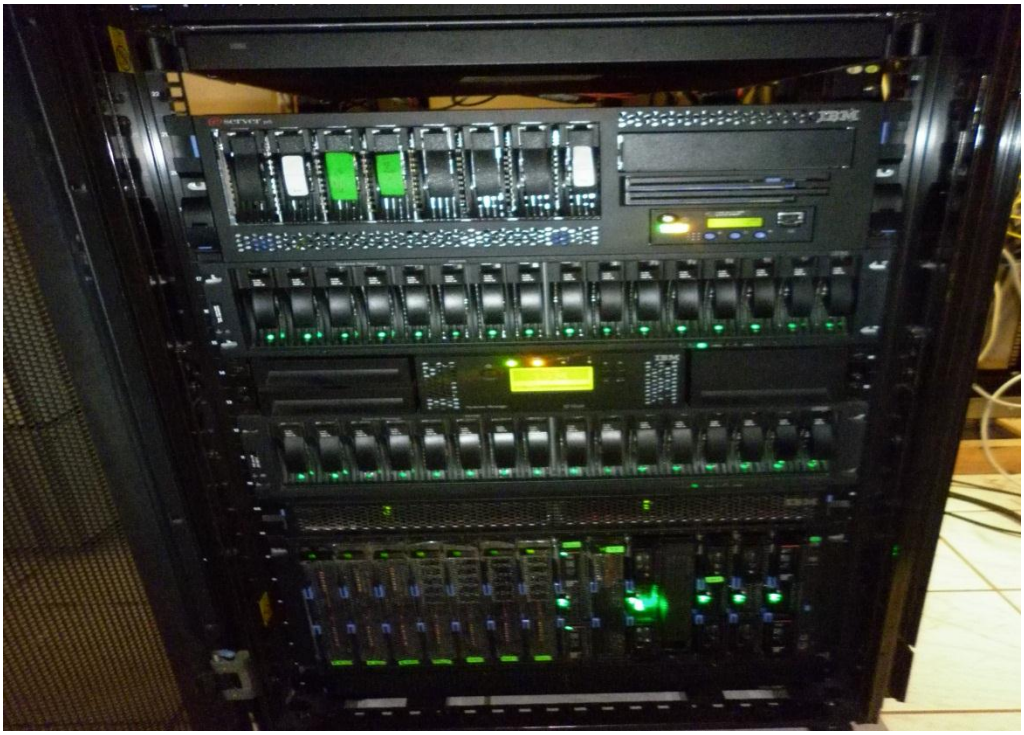


Foto 2: Rack de Servidores.

Fuente: Cooperativa Jardín Azuayo.

En este rack podemos ver como se encuentra completamente lleno y no da opción para poder adquirir un nuevo servidor en caso de que fuese necesario.

Refiriéndonos al ámbito de tendido de la red, es aun pero, pues tanto el ingreso de los cables de red y telecomunicaciones, como la salida de los mismos hacia las diferentes áreas de trabajo se los realiza por el mismo espacio de ingreso y salida, el mismo que está en deplorables condiciones lo que puede ocasionar la perdida de información o señal al ingreso y a la salida de la información procesada.

Por ende todo el cableado estructurado que se debería tener está completamente obsoleto.

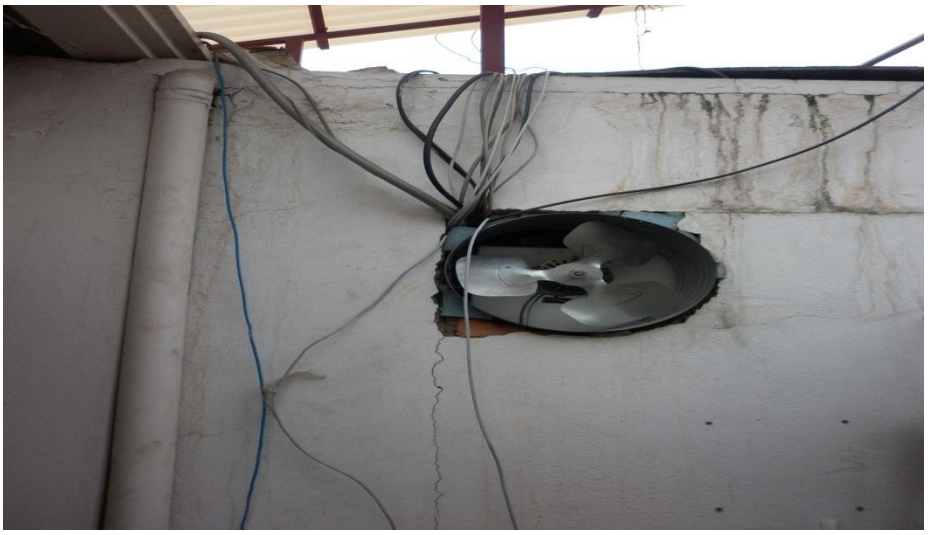


Foto 3: Ingreso y Salida de Cables de Red.

Fuente: Cooperativa Jardín Azuayo.

4.5. Situación eléctrica.

El sistema de red eléctrica dentro del espacio donde se encuentra el servidor es sumamente obsoleta por existen cables por doquier lo que puede traer consecuencia nefastas en caso de roce con otros cable que pueda traer consigo algún incendio o desastre que afecte los datos almacenados.

Foto 4: Tomas de Corriente.

Fuente: Cooperativa Jardín Azuayo.

4.5.1. Planta alterna de energía.

Este servidor está conectado a un UPS, con capacidad de funcionamiento durante 15 minutos hasta que se pueda iniciar el funcionamiento con el generador alterno.

Foto 5: UPS.

Fuente: Cooperativa Jardín Azuayo.

Esta planta de generación de corriente alterna, que funciona en caso de interrupción de la electricidad normal tiene una capacidad de funcionamiento de 6 horas continuas por cada abastecimiento completo de combustible.

El mantenimiento que se le da a este generador es mensual por lo que su funcionamiento siempre está garantizado para que soporte cualquier emergencia que surgiere.

Foto 6: Generador de corriente alterna.

Fuente: Cooperativa Jardín Azuayo.

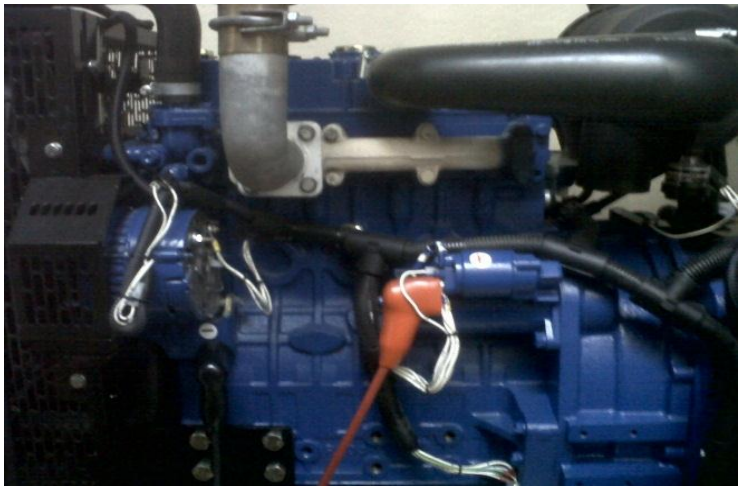


Foto 7: Generador de corriente alterna.

Fuente: Cooperativa Jardín Azuayo.

Foto 8: Generador de corriente alterna.

Fuente: Cooperativa Jardín Azuayo.

En caso de que dicho generador no funcionare adecuadamente o no se encendiera, el servidor quedaría fuera de servicio lo que involucraría que toda la cooperativa a nivel de todas sus agencias deje de funcionar.

4.6. Sensores y extintores.

Refiriéndonos a extintores, este espacio no cuenta con un sistema automático de extinción en caso de que se diere algún desastre dentro del espacio donde se encuentra dicho servidor, lo que cuentan es con un solo extintor manual, con polvo químico para evitar daño en los equipos.

Foto 9: Extintor.

Fuente: Cooperativa Jardín Azuayo.

En tal motivo, tampoco posee ningún tipo de sensores al interior, ya sea sensores de humo, sensores de agua, o cualquier tipo de sensor que debiese tenerse al interior y exterior de este espacio físico para el servidor.

4.7. Ingreso de personal

Dentro del área de sistemas existe las políticas internas en donde está reglamentado que nadie puede ingresar solo personal autorizado.

Se da permiso para su ingreso previo aprobación del coordinador del área, este permiso debe ser solicitado de forma escrita al antes mencionado, indicando el porqué del ingreso y la cantidad de personas que van a ingresar.

Pero el área física como tal, no cuenta con un sistema de seguridad automático como por ejemplo lector de huellas, sensores o algo seguro, lo único que cuenta es con la persona encargada del lugar el mismo que tiene el ingreso mediante una llave común y corriente.

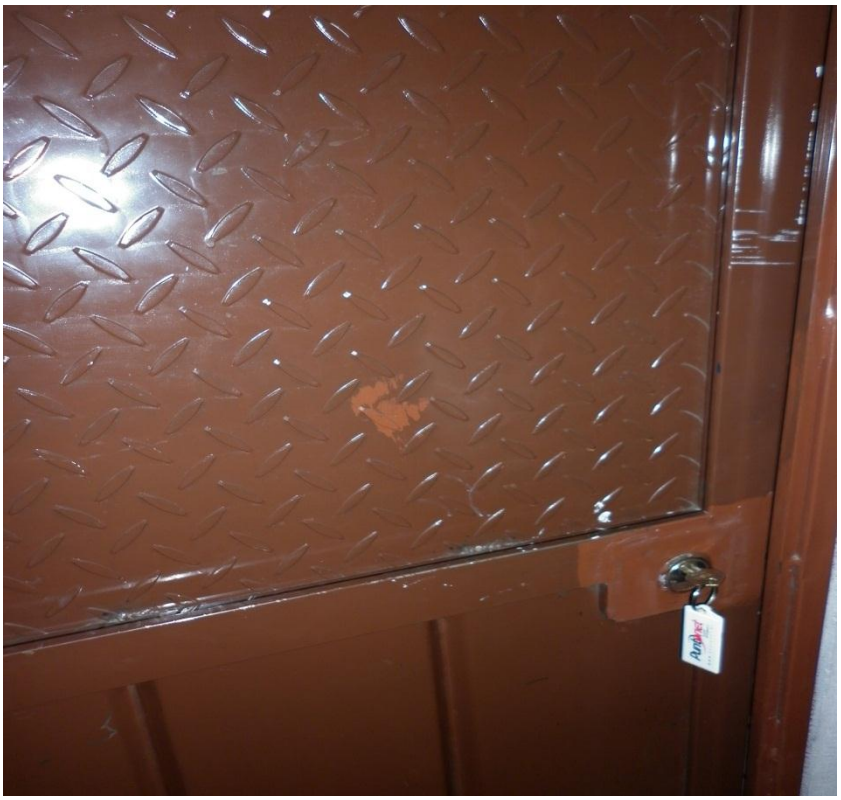


Foto 10: Ingreso a los Servidores.

Fuente: Cooperativa Jardín Azuayo.

No posee personal que trabaje las 24 horas si se diere algún inconveniente en el servidor, pero lo que está dispuesto en la normativa interna es que las personas que trabajan en esta área deben estar vigentes a cualquier hora ya sea desde sus hogares para poder dar solución en caso de algún inconveniente.

4.8. Respaldos del servidor principal.

Los respaldos de información de la base de datos se los realiza a través de una aplicación que nos brinda la base de datos Oracle.

Esta herramienta se denomina RMAN (recovery manager), que es la que nos permite realizar la copia de respaldo.

Este respaldo se lo realiza diariamente a las 4 AM, dicha información respaldada se lo va almacenando en un array de discos.

Esta información se va pasando igualmente diariamente a cintas de respaldo mediante un robot de cintas, que luego serán almacenadas en las bóvedas del Banco Bolivariano.

CAPITULO V

PROPUESTA

DISEÑO DE UN DATACENTER, ESQUEMA DE RESPALDO CON SU ESPACIO FÍSICO Y ADMINISTRACIÓN DEL DATACENTER

5.1. Data Center

Un centro de datos (data center) es uno de los recursos claves en las empresas, para evitar posibles grandes pérdidas como consecuencia del ingreso no autorizado de personal, deficiente estructura eléctrica, etc.

Un datacenter dentro de la institución nos brindara confiabilidad y seguridad tanto en los equipos a nivel físico como los datos lógicos que se encuentran dentro de estos servidores.

El construir un data center completo que satisfaga todas las necesidades no es tarea fácil, pues los avances tecnológicos, las reestructuraciones organizativas e incluso los cambios de la sociedad en general pueden imponer nuevas exigencias lo cual dificulta garantizar que un data center permanecerá intacto varios años.

En la construcción de un Datacenter, existen estándares internacionales que garantizan el funcionamiento del mismo.

En la construcción de un Datacenter se debe considerar los “Tier”, que no es más que la manera de describir la:

- Disponibilidad
- Confiabilidad.

- Costos estimados de construcción y mantenimiento.

Es decir entre mayor Tier se tenga en un datacenter mayor confiabilidad se tendrá en el mismo.

5.1.1. Clasificación de los Tier.

Según el estándar TIA-942, mediante el cual nos guiaremos, los Tier se clasifican en 4, y estos son:

- Tier I: Infraestructura básica
- Tier II: Infraestructura con componentes redundantes
- Tier III: Infraestructura con Mantenimiento simultáneo
- Tier IV: Infraestructura Tolerante a Fallas

	Tier I	**Tier II**	**Tier III**	**Tier IV**
Tiempo promedio de caída anual	28.8 hrs	22.0 hrs	1.6 hrs	0.4 hrs
Disponibilidad	99.671%	99.741%	99.982%	99.995%

Tabla 15: Tabla comparativa de Tier

La tabla detallada, muestra el promedio que pudiere tener en datacenter anualmente, dependiendo de nuestro Tier, al igual que la disponibilidad que tendrá dicho datacenter para operar con confiabilidad.

El Tier a lograr en esta propuesta en el “Tier IV”, logrando así la máxima disponibilidad y un tiempo de caída anual del menor lapso posible.

Según la Norma TIA-942 estos son los requerimientos de los diferentes elementos de un Data Center:

- Estructura y Ubicación
- Acceso
- Protección.
- Equipos
- Esquema de respaldo.
- Diseño físico para los respaldos.

Conociendo que la cooperativa tiene una muy buena capacidad económica para solventar la construcción y equipamiento de un datacenter lanzamos la propuesta de construir dicho espacio.

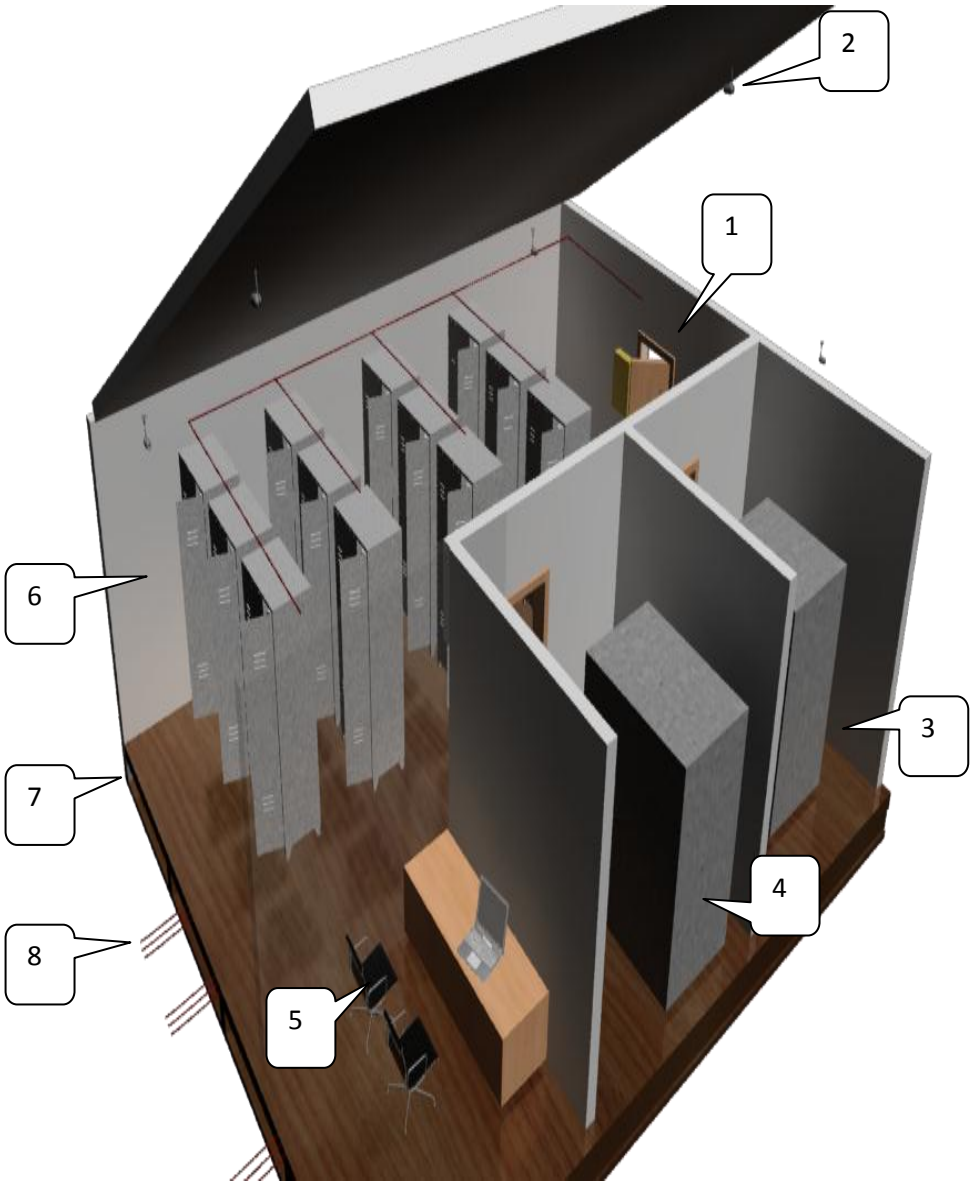


Figura 17: Diseño Data Center

Descripción

1. Sistema Biométrico.
2. Sensores y cámaras de vigilancia.
3. Sistema PDU
4. UPS
5. Equipos de control
6. Rack de servidores.

7. Piso Flotante

La propuesta tomando en cuenta los estándares requeridos según las normas, y teniendo en cuenta la situación actual de la cooperativa el monto aproximado en la construcción del datacenter para su correcto funcionamiento tendría el costo de: 15585.00 dólares.

A Realizar	**Costo de Desarrollo**
Estructura y Ubicación	5900.00 dólares
Accesos	1800.00 dólares
Protección	3200.00 dólares
Equipos	4685.00 dólares
Total	**15585.00 dólares**

Tabla 16: Costo Total Datacenter

A continuación desglosaremos cada uno de los puntos, y sus respectivos implementos que serán utilizados para conseguir dichos puntos.

5.2. Estructura y ubicación

5.2.1. Piso, Techo y paredes

Piso.

La construcción del piso base para la implementación del datacenter, será construido a base de hormigón, en el espacio que se cree conveniente implementar este moderno centro de datos.

Una vez construido el piso base, se procederá a colocar un sistema de piso falso, un sistema de Piso Falso es usualmente recomendado para instalaciones de Datacenter.

Este tipo de sistema no solamente nos permitirá construir un ambiente estéticamente agradable y cómodo sino que también nos facilitara la instalación y colocación del cableado de energía eléctrica y el cableado de datos. También, nos permitirá mayor flexibilidad para el acceso y cambios en el cableado, que el que se conseguirá mediante canaletas fijas empotradas.

Adicionalmente, se manejara una conveniente separación entre cables de energía y cables de datos, a fin de prevenir cualquier tipo de interferencia electromagnética.

El Sistema de Piso de Falso va a estar constituido por los siguientes elementos:

Pedestales y Travesaños

Los pedestales y travesaños definen la estructura que va a soportas a los paneles que conforman el “piso falso”, los cuales, a su vez, se asientan sobre el piso base de hormigón.

Figura 18: Pedestales y Travesaños

Paneles

Los paneles serán rígidos, no combustibles y adicionalmente van a serán diastáticos.

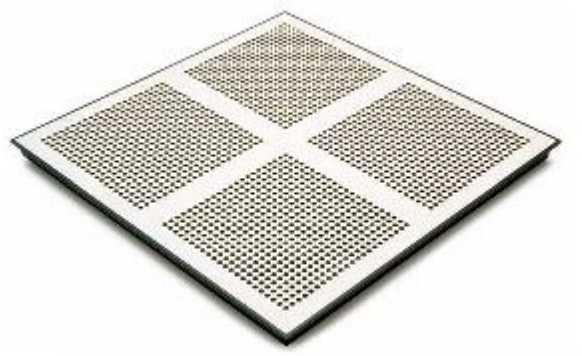


Figura 19: Paneles

En definitiva en piso falso a colocarse cumplirá con las siguientes especificaciones.

- El área total a ser cubierta es de 42 mts2.
- Los paneles serán de 61cm x 61 cm.
- La altura del piso falso va a ser de 40 cm.
- Se realizara los cortes y/o agujeros necesarios en el piso falso para permitir el paso del cableado de conexiones respectivas para todos los equipos.

Techo y paredes

El techo será cubierto por un sistema de cielorraso, que cubrirá cualquier molécula de basura que puedan dañar los equipos al interior.

Igualmente las paredes serán cubiertas con vinil antiestático, que nos garantizara la seguridad de los equipos.

5.2.2. Área física.

Como se indicó el espacio designado para la construcción del datacenter en la figura 6, una vez construida la parte física tendremos el ares física de la siguiente manera:

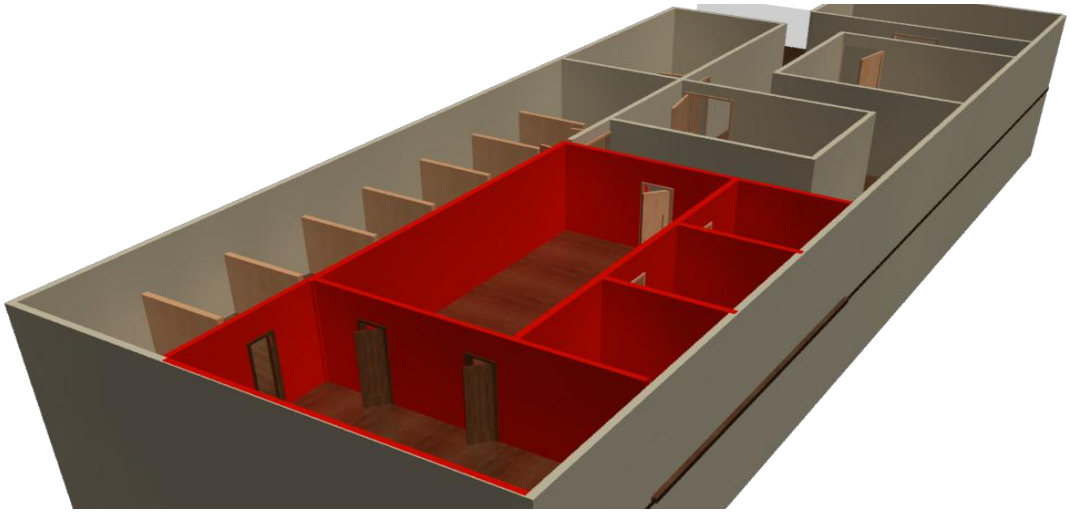


Figura 20: Plano de colocación Data Center

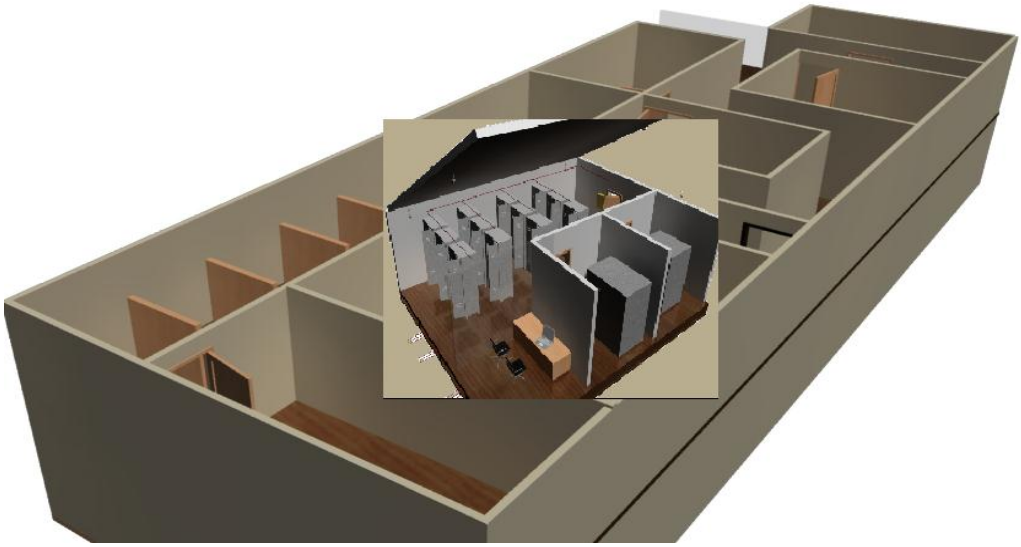


Figura 21: Colocación Data Center

La construcción de toda esta parte de estructura y ubicación del datacenter tendrá un costo de: 13100.00 dólares.

Estructura y ubicación	**Tiempo Propuesto**	**Costo de Desarrollo**
Estructura de piso, paredes y techo	25 días	3000.00 dólares
Colocación del piso falso	7 días	600.00 dólares
Colocación de cielorraso	3 días	200.00 dólares
Colocación de vinil en las paredes	2 días	100.00 dólares
Mano de obra.	O días	2000.00 dólares
Total	**32 días**	**5900.00 dólares**

Tabla 17: Costo Estructura Física

5.3. Acceso

5.3.1. Sistema biométrico

Figura 22: Sistema Biométrico

Para tener una seguridad optima al momento de ingresar al datacenter, se propone utilizar un sistema biométrico actual, para ello utilizaremos el “HandKey II”.

Este sistema biométrico utiliza una tecnología biométrica de geometría de la mano, probada en el campo que gráfica y verifica el tamaño de la mano

en menos de un segundo.

Adicional a esto, este moderno sistema de seguridad biométrico viene con un controlador de puerta completo que provee operación de cerradura a la puerta, solicitud de salida y monitoreo con alarma.

ESPECIFICACIONES HANDKEY II	
Dimensiones	Ancho 22.3 cm Alto 29.6 cm Profundidad 21.7 cm
Peso	2.7 kg.
Tiempo de registro	De un segundo
Mantenimiento de datos	5 años
Controles de puertas	Entrada bajo solicitud ingresada. Control de cerradura de puerta.
Monitoreo de alarma	Seguridad Puerta forzada Identificación rechazada
Garantía	24 meses.

Tabla 18: Especificaciones Sistema Biométrico.

5.3.2. Puertas de ingreso

También se instalara una puerta de seguridad que garantiza su inviolabilidad, a la vez que proteja contra siniestro como incendios o ingreso de personal no autorizado.

La puerta será sumamente sólida para que impida cualquier tipo de vandalismo.

Las cerraduras de esta puerta estarán controladas por el sistema biométrico para que garantice su funcionamiento.

La puerta constara con las siguientes especificaciones:

- La dimensión será de 1.10 mts de ancho por 2.1. mts de alto.
- La puerta será elaborada en hierro laminado en caliente.
- El espesor de la plancha de hierro será de 2mm.
- Contendrá planchas de lana de fibra de vidrio para aislamiento térmico.

El costo total para la implementación en la seguridad de acceso al datacenter estará dividido en:

COSTO EN SEGURIDAD DE ACCESO	
Sistema biométrico HandKey II	1400.00 dólares
Puerta de seguridad	400.00 dólares
Total	1800 dólares

Tabla 19: Costo Seguridad en Acceso

5.4. Protección

5.4.1. Sensores

Figura 23: Piso Flotante

Los sensores realizan la función de detectar la posibilidad de un evento de incendio o calentamiento. Lo hace mediante una detección cruzada entre dispositivos que

pueden detectar humo, calor o fuego, de esta manera se garantiza la confiabilidad operativa.

Dentro de los sensores que utilizaremos dentro de nuestro datacenter serán los sensores Panasonic, serie IP51 | 4350, que son los sensores que nos enviaran señales de alerta tanto de humo como de calor dentro del data center, estos sensores tienen las siguientes características.

- Este detector es de perfiles múltiples.
- Contiene un fotoeléctrico (óptico) detector de humo y un detector de calor dentro de un espacio físico.
- Tiene una cámara de detección de humo, con un sistema de alta eficiencia óptica que consiste en un LED y un fotodiodo con dos lentes.
- Posee un sensor de calor.

5.4.2. Cámaras (CCTV).

Figura 24: Software GV-AUTOSW

Las cámaras también cumplen un rol importante dentro del datacenter, pues son estas quienes grabaran todo lo que suceda dentro de dicho espacio físico.

Para controlar y vigilar todo lo que suceda al interior del datacenter utilizaremos un sistema de CCTV llamado “Software GV-AUTOSW”, mediante el cual controlaremos todas

las cámaras a ser instaladas en su interior desde lo que sería el área de sistemas.

Este sistema cuenta con cámaras **IP tipo DOMO, serie NIB-213M.**

Figura 25: Cámara Tipo Domo

Estas son las especificaciones técnicas del software “GV-AUTOSW”

ESPECIFICACIONES GV-AUTOSW	
Audio / Video grabación	MPEG-4, MJPEG
Cámara de compatibilidad	IP tipo DOMO, serie NIB-213M
Velocidad de grabación de imagen	de hasta 30 cuadros por segundo
Monitoreo	video vigilancia remota a través de la interfaz gráfica de usuario intuitiva
Búsquedas	Búsqueda inteligente por evento y fecha / hora / cámara
Idiomas	Inglés, francés, portugués y español
Sistemas operativos de Servidor	Windows XP Pro SP2 o 3, Windows 7, Windows 2008 (32 bits)
Notificación	De Alarma SMTP (correo electrónico), notificación SMS de eventos de cámara: el cierre de movimiento y de contacto. Notificación de alarma gráficos en el software de cliente

Tabla 20: Especificaciones Sistema CCTV

5.4.3. Sistema de refrigeración y antiincendios

Sistema de refrigeración

Al interior de nuestro datacenter contaremos con modernos sistemas de refrigeración que evitaran sobrecalentamientos en los equipos que se encuentren implementados.

Figura 26: Sistema de Refrigeración.

Nuestro sistema de refrigeración será un: “bastidor HP G2 de profundidad (AF057A).

SISTEMA DE REFRIGERACIÓN “HP G2 AF057A”	
marca	HP
Dimensiones	12,7 x 6 x 20 cm ; 115 Kg
Ventiladores	Ventiladores intercambiables en caliente
Aire	Proporciona aire helado a lo largo de toda la altura del bastidor.

Tabla 21: Características del sistema refrigeración

Sistema antiincendios

Para nuestro sistema de extinción en caso de incendio se colocaran tanto tubería de conducción, como tuberías de dispersión al interior del datacenter.

Las tuberías de conducción serán colocadas con el fin de poder agilitar la circulación del polvo químico que se utilizara para rociar los equipos del interior.

Las tuberías de dispersión se encargaran de dispersarlas por las diferentes partes de los equipos.

CARACTERÍSTICAS SISTEMA ANTIINCENDIOS	
Tubería de conducción	Serán de 1 pulgada Galvanizadas
Tuberías de dispersión	Acero inoxidable La dispersión será de 180 a360 grados La distancia de los equipos de 5 mts
Cilindro de polvo químico	La presión interna del cilindro será de 360 psi Liberara el polvo una vez recibida la alarma de incendio. Se utilizara polvo químico seco PC-34 Cilindros que cumplan las normas : DGN, NOM.102-STPS-1994 (para datacenter)

Tabla 22: Características Sistema Antiincendios.

El costo total en la implementación de la protección esta desglosada en:

COSTO EN PROTECCIÓN	
Sensores (Panasonic IP51)	600.00 dólares
Sistema CCTV (GV-AUTOSW)	1100.00 dólares
Sistema de refrigeración	1000.00 dólares
Construcción de tuberías	300.00 dólares

Cilindros polvo químico	200.00 dólares
Total	3200 dólares

Tabla 23: Costo sistema de Protección.

5.5. Equipos

5.5.1. Rack o Gabinetes

Dentro del datacenter vamos a tener dos tipos de gabinetes o Rack, el primer rack será para poder colocar los servidores, estos Gabinetes o Rack deben tener ciertas especificaciones estándares.

- Altura máxima 2.4m, preferiblemente 2.1m
- 42U de espacio mínimo
- Profundidad de 1.0 a 1.1 m
- Regletas: al menos una de 20Amp/120V

Figura 27: Rack de Servidores

Los segundos tipos de rack, los utilizaremos para colocar nuestro cableado estructurado.

Figura 28: Rack de Cables

Como existe ya un cableado estructurado dentro de la cooperativa, lo que se pretende es únicamente modificar ciertos tendidos de red que se encuentran en condiciones poco óptimas para el funcionamiento correcto de la transmisión de datos.

Para reestructurar en cableado estructurado existente, utilizaremos La categoría 5e, que es uno de los grados de cableado UTP descritos en el estándar EIA/TIA 568B el cual se utiliza para ejecutar y transmitir datos a velocidades de hasta 100 Mbps a frecuencias de hasta 100 Mhz.

Este tipo de cables tiene ciertas características.

- 4 pares trenzados sección AWG24
- Cada par de cable esta distinguido por colores, siendo estos naranja, verde, azul y marrón
- Aislamiento del conductor de polietileno de alta densidad, de 1,5 mm de diámetro.
- Cubierta de PVC gris
- Disponible en cajas de 305 m

COSTO EN RACKS	
Rack hp AF046A	530.00 dólares
Rack HP 12u60	255.00 dólares
2 rollos de cable UTP 5	250.00 dólares
Total	1035.00 dólares

Tabla 24: Costo Racks

5.5.2. UPS

El UPS, nos va a proporcionar energía momentánea mientras el generador arranca para poder continuar con las labores normalmente hasta poder retomar la energía normal para el funcionamiento del datacenter.

Figura 29: UPS

El Ups sugerido a comprar, es un UPS “TOWER WP-906 / WP-9010, que nos brindara las siguientes características.

- Tecnología de doble conversión en línea y de alta frecuencia.
- Amplio rango de tensión de entrada.

- Tecnología de control digital.
- Redundancia en paralelo N+1 (6 ~10 kVA).
- Auto diagnóstico durante el inicio del UPS.
- Administración avanzada de batería.
- Función de arranque en frío (encendido con CC).
- Carga automática de baterías en modo UPS apagado.
- Protección contra descarga eléctrica y sobretensión
- Protección contra cortocircuitos y sobrecarga.
- Regulación automática de ventilación según variación de carga.
- Batería externa opcional.
- Programación de apagado y reinicio.
- Abastecimiento de energía de 10KVA / 7000W, durante 30 minutos.

Estas son las principales características de nuestro sistema UPS, con el cual se va a dar abastecimiento de energía a todo el rack de servidores, sistema de refrigeración y el sistema de protección.

El costo para la obtención de este UPS será de: **1200.00 dólares**

5.5.3. Generador

Se va a contar con un generador de corriente alterna que garantice el funcionamiento de todo el datacenter en caso de falla en la corriente normal, para poder evitar posibles pérdidas por el desabastecimiento de corriente.

Se pretende adquirir un generador de corriente **“Doosan”,** que es el apropiado para solventar las necesidad del datacenter.

Figura 30: Generador

Las características de este generador son las siguientes:

- El tanque del generador alcanza 8 horas de funcionamiento continuo
- Motor diesel de 700kva/560kw.
- Generador de poco ruido
- Supresor de transigentes
- Cumple las normas de calidad ISO 9001
- Paneles de distribución

El costo de este generador será de: **1100.00 dólares.**

5.5.4. PDU

Los PDU o los conocidos como Unidad de Distribución de Energía, el mismo que se debe tener obligadamente para que este haga el cambio de energía automáticamente cuanto procese que alguna de las fases de corriente normal falle, para que de paso a la corriente alterna.

Figura 31: PDU

El PDU que utilizaremos en esta propuesta será un: PDU **Eaton Powerware 5125,** que tiene las siguientes características:

- Integra aislamiento, monitoreo y distribución de la energía con una gran variedad de opciones.
- Ofrece una arquitectura escalable que garantiza máxima flexibilidad, en un diseño compacto.
- Opciones adicionales de gran utilidad, especialmente útiles para monitoreo y conectividad.
- Inigualable facilidad de uso gracias a que sólo requiere acceso frontal para su servicio.
- Entradas para cable en la parte superior e inferior del gabinete, facilitando su instalación.

El costo de este moderno sistema de distribución de energía esta en: **1350.00 dólares.**

El costo total en la adquisición de equipos que nos servirán para el correcto funcionamiento del datacenter será:

COSTO TOTAL EN EQUIPOS	
Costo en Racks	1035.00 dólares
UPS	1200.00 dólares
Generador	1100.00 dólares
PDU	1350.00 dólares
Total	4685.00 dólares

Tabla 25: Costo total de equipos

5.6. Esquema de respaldos

El actual modo de respaldo que maneja la cooperativa va de acuerdo a las necesidades que este tiene.

Sin embargo se debe mejorar la disponibilidad de la base de datos, para ello se propone la utilización de otro servidor en modo espejo.

Debido al alto costo que tiene un servidor nuevo, ya que un servidor nuevo como el que posee actualmente la cooperativa está alrededor de 35.000 dólares, por lo que se pretende es adecuar el anterior servidor que se tenía, este es un IBM P5

Lo que se pretende es mejorar la disponibilidad de la base de datos en caso de que esta llegara a caer, inmediatamente debería entrar a funcionar nuestro servidor espejo pues este va a estar a la par con el servidor principal.

Lo que se pretende es desarrollar una copia de información tipo espejo, para ello tenemos nuestro servidor principal, un IBM P7, y utilizaremos nuestro servidor anterior un IBM P5.

Para poder desarrollar este método de disponibilidad de la base debemos considerar tres cosas importantes:

- Hardware (físico)
- Sistema Operativo
- Base de Datos

Hardware

Para poder generar una copia en espejo, lo que se refiere al aspecto físico no es lo importante, pero si se debe tratar de que tanto el servidor principal como el servidor de copia sea de características físicas similares.

Figura 32: Servidor P7 y P5

Sistema Operativo

En cuanto lo que se refiere al sistema operativo, es recomendable tener en ambos servidores el mismo sistema operativo, pues esto garantizara su funcionamiento tanto en la copia de información como al momento de poner a prueba su disponibilidad ante algún desastre que pudiera suceder.

En nuestro caso nuestro servidor de base de datos principal como el servidor que vamos a utilizar como respaldo, utilizan el sistema operativo propio de IBM como es AIX versión 5.1

Base de Datos

En cuanto a la base de datos, es necesario que se encuentren las mismas versiones tanto en el servidor principal como en el servidor espejo.

Si en caso se pretende implementar una nueva versión de base de datos, es necesario realizarlo este cambio de versión en primera instancia en el servidor espejo, para poder verificar que no existan error y luego de eso poder implementarlo en el servidor principal, garantizando así que en el cambio de versión la copia al servidor espejo no se va alterar.

De tal manera se plantea realizar la copia espejo del servidor principal IBM P7 a un IBM P5, el mismo que será ubicado momentáneamente en el espacio físico donde trabaja ahora el actual servidor principal.

La sugerencia es colocar a nuestro servidor espejo en Paute, pero por el momento no es factible, ya que se está pensando en cambiar de localidad en la oficina antes mencionada.

Sin embargo se planteara un diseño del espacio físico.

5.7. Diseño físico para los respaldos.

El espacio físico para los respaldos será algo similar al diseño físico del datacenter general, pues la información que se va a manejar es igualmente delicada para la empresa.

Por el momento como lo dijimos anteriormente vamos a diseñar el espacio físico donde se colocaran el o los servidores de respaldo.

El diseño que se implementara será el siguiente:

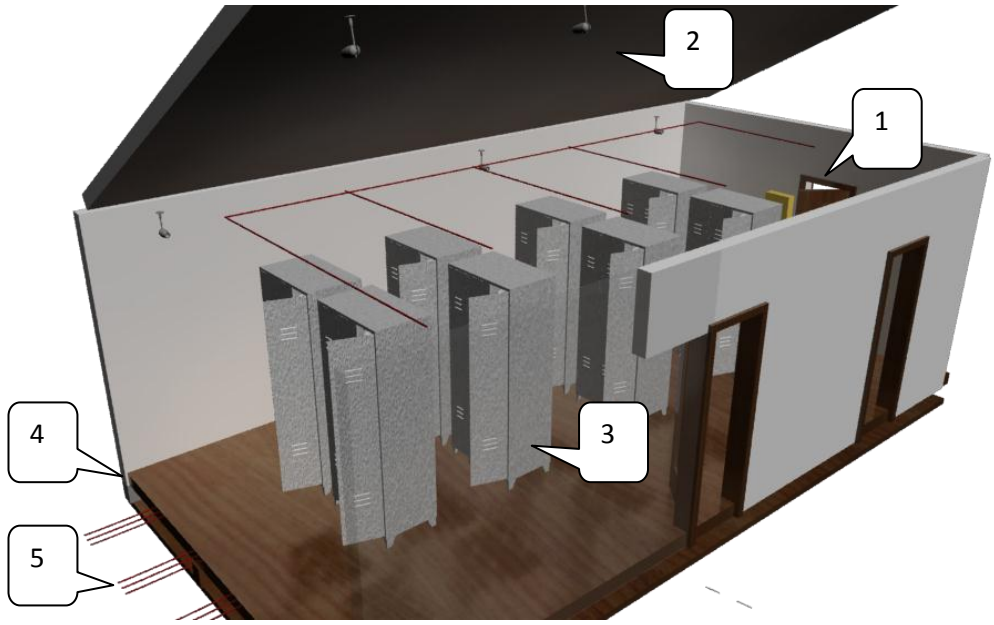


Figura 33: Diseño de respaldos

Descripción.

1. Sistema biométrico
2. Sensores y sistemas de vigilancia
3. Racks.

4. Piso flotante
5. Canaletas de conexión.

La construcción del área física donde se vaya a colocar los respaldos

La construcción y adecuación del espacio físico para los respaldos tomando en cuenta los gastos en la construcción del data center

A Realizar	**Costo de Desarrollo**
Estructura y Ubicación	2500.00 dólares
Accesos	800.00 dólares
Protección	1500.00 dólares
Equipos	2800.00 dólares
Total	**7600.00 dólares**

Tabla 26: Costo espacio Respaldos

5.8. Plan de recuperación.

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

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.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento.

Las actividades a realizar en un Plan de Recuperación se pueden clasificar en tres etapas:

- Actividades Previas a la falla o desastre.
- Actividades Durante la falla o Desastre.
- Actividades Después de la falla o Desastre.

Actividades Previas al Desastre

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

Actividades Durante el Desastre

Una vez presentada la Contingencia, Falla o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

- Plan de Emergencias.
- Entrenamiento.

Actividades después del desastre.

Realizar la averiguación pertinente sobre los acontecimientos que han sucedido, para que se haya producido el desastre, definiendo responsables de lo acontecido, teniendo establecidas las sanciones en caso de ser negligencia de la persona encargada de determinada labor.

5.8. Administración del datacenter.

Para la administración del datacenter una vez que este se encuentre funcionando dentro de la organización, debemos tener en cuenta algunos puntos

5.8.1. Revisiones

Una vez implementado el datacenter y ya funcionando, debemos realizar revisiones constantes de sus diferentes partes como son: los pisos, el techo, cableado de red eléctrica, cableado de red de datos, etc.

Siempre es necesario que se contrate a empresas terceras para que realicen los mantenimientos de ciertos equipos que están dentro del datacenter, entre esos debemos realizar las revisiones de:

- Mantenimiento periódico del generador de corriente

  Este mantenimiento se lo debe realizar mensualmente garantizando así el correcto funcionamiento del mismo en caso de ser necesario su intervención en la cooperativa.

- Mantenimiento de los sistemas CCTV

Se los debe ir realizando igualmente mensualmente, haciendo su revisión sobre todo en la calidad de imágenes que se están obteniendo, y la memoria donde se están almacenando dichas imágenes.

- Mantenimiento de la estructura física.

  Se deben realizar las revisiones periódicas, estas pueden ser trimestrales ya que la infraestructura no tiende a destruirse continuamente, pero de ser necesaria su intervención en los momentos que sean necesarios.

Al igual existen revisiones que los debe realizar personal de la misma cooperativa pues son revisiones que se deben manejar internamente para poder generar las respectivas bitácoras de control.

Esta revisión será:

- Revisión del cableado

  Se deben realizar revisiones aleatoriamente en los cables de red para poder verificar si la velocidad que se implementó o la que se tenía se sigue manteniendo.

  Igualmente personal de telecomunicaciones debe realizar también revisiones en los tendidos de energía, tanto al interior como al exterior del datacenter para verificar que no existan falencias en las líneas de corriente.

- Revisión en los servidores

Se debe realizar revisiones diarias en los servidores para evitar que cualquier cosa que pudiere lastimar o agredir al funcionamiento correcto de dicho servidor que se esté revisando.

- Revisiones de los sistemas biométricos

Se tiene que verificar que los sistemas de seguridad tanto de ingreso como los que vigilan el correcto funcionamiento estén en condiciones óptimas para garantizar el funcionamiento en la seguridad del data center.

5.8.2. Bitácoras

Se deben llevar unas bitácoras de información sobre todos los mantenimientos que se van realizando, ya sea diariamente, semanalmente o mensualmente, ya sea cada requerimiento del mantenimiento que se necesite.

Figura 34: Bitácoras

Los datos que deben tener las bitácoras para las empresas terceras a la cooperativa será el siguiente:

- Fecha de registro o mantenimiento
- Empresa que lo va a realizar
- Persona que lo realiza
- Aspectos a revisar
- Observaciones de lo encontrado.
- Mantenimiento realizado.

- recomendaciones de cambio.
- Conclusiones del mantenimiento.
- Próximo mantenimiento.

Igualmente debemos realizar las bitácoras para los mantenimientos generados al interior de la cooperativa, estos serán:

- Fecha de revisión
- Área que lo realiza
- Persona que lo realiza
- Detalle de la revisión de lo planteado
- Sugerencia a lo analizado
- Próxima fecha de mantenimiento.

Adicional a esta, también se deben generar todas las bitácoras de ingreso al datacenter para poder tener un reporte específico de todos los usuarios que han tenido ingreso al datacenter:

- Fecha de reporte
- Fecha y hora de ingreso
- Usuario que ingreso
- Fecha y hora de salida

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

Como conclusiones podemos decir, que la seguridad física del lugar donde se encuentra el servidor de base de datos, debe ser muy bien creado y resguardado con todas las seguridades pertinentes para evitar cualquier tipo de robo o daño de los equipos por algún inconveniente.

Remontándonos a lo analizado en lo referente la situación actual física del servidor de base de datos, podemos darnos cuenta que este espacio físico no cumple con los estándares mínimos de seguridad física planteado por organizaciones internacionales.

Al no tener ciertos estándares de seguridad estamos sumergiéndonos en un gran riesgo para la institución como tal, exponiendo toda su información a posibles ataques de terceras personas o sencillamente al ataque propio de la naturaleza.

Es por esto que en el desarrollo de este tema hemos podido considerar la mayor parte de puntos necesarios al momento de crear un datacenter y su correcto funcionamiento.

Con esto se pretende mejorar la situación actual física y estar inmersos ya dentro de los estándares que se deben seguir, y de esta manera poder dar la garantía de un buen funcionamiento a la institución.

6.2. RECOMENDACIONES

Para empezar a tener garantías sobre el servidor de base de datos y sus respectivos respaldo debemos tener en cuenta el espacio físico donde se piensa colocar los servidor, principalmente el de base de datos, adecuarlo correctamente para que el rendimiento del servidor sea optimo y poder aprovechar todas sus ventajas en el desarrollo de la empresa.

Garantizar que el espacio físico donde será colocado dicho servidor, cumpla con los estándares mínimos de funcionamiento, como la correcta colocación de canaletas para el tendido de cables de red, e igualmente para el tendido correcto de la energía eléctrica, contar con un piso flotante para que los servidores no se encuentren expuestos a posibles humedades, la correcta ubicación de los Rack para colocar los servidores, entre las más importantes a destacar, en cuanto a lo físico.

Se les recomienda implementar un moderno sistema de ingreso del personal, esto podría ser el control mediante un sistema biométrico, que garantice llevar un registro apropiado de todas las personas que realizan el ingreso al datacenter, al igual que no solo debería ser este el único sistema de seguridad.

También se recomienda instalar los sistemas de CCTV, para poder controlar al datacenter desde exteriores y así garantizar aún más su seguridad tanto interna como externa.

En cuanto al suministro de energía, se recomienda la correcta adquisición de una planta generadora de corriente para dar solución a posibles fallas en la corriente normal, recordar también que se tiene que tener un UPS en el

datacenter para que este sea quien proporcione de energía momentánea, hasta que se encienda el generador de corriente y poder continuar con las labores correctamente.

Es importante no olvidarse de las revisiones periódicas que se tienen que dar al datacenter creado para que este mantenga su curso normal y así evitar posibles paras en el servicio del servidor y evadir riesgos de perdida para la cooperativa.

Es recomendable que las revisiones a todos los componentes que forman parte del datacenter sean en lo posible mensualmente, pero de ser necesaria la intervención antes se debe realizar con el único objetivo de mantener el datacenter funcionando todos los días.

Por otro lado no debemos descuidar también la seguridad de los respaldos que se generen de la base de datos principal, pues estos nos serán de gran ayuda en caso de que nuestro servidor principal caiga por algún motivo que pueda darse.

Se recomienda que estos respaldos sean almacenados en otro lugar diferente al del servidor principal, siempre y cuando que este lugar físico para los respaldos, también garantice el correcto almacenamiento de los mismos, e igualmente con sus respectivas revisiones mensuales.

BIBLIOGRAFÍA

ALEGSA. (1998). *Servicio Informaticos.* Recuperado el 14 de noviembre de 2011, de http://alegsa.com.ar/

masadelante. (s.f.). *disenio grafico y programacion.* Recuperado el 14 de noviembre de 2011, de http://www.masadelante.com/

SearchStorage. (2010). *SearchStorage en espanol.* Recuperado el 14 de noviembre de 2011, de http://www.searchstorage.es/

Universidad de Murcia. (s.f.). *U. de Murcia.* Recuperado el 2011 de noviembre de 14, de http://www.um.es

Walus, J. (s.f.). *Wikipedia Libre.* Recuperado el 14 de noviembre de 2011, de http://es.wikipedia.org/wiki/Servidor

IBM (s.f.).*Servidores Ibm.* Recuperado el 08 de noviembre de 2011, de http://www.ibm.com/ec/services/ss/

Microsoft (s.f.). *Msdn.* Recuperado el 05 de noviembre de 2011, de *http://social.msdn.microsoft.com/Forums/es/sqlserveres/thread/8116d0a4-4d8e-4dcf-89ad-a15da82739df*

Teach Center de Microsoft (s.f.). *Seguridad de servidores de base de dastos*. Recuperado el 08 de noviembre de 2011, de *http://technet.microsoft.com/es-es/library/bb432625.aspx*

Tech-Faq (s.f.). *Securing Databse Servers.* Recuperado el 06 de noviembre de 2011, de *http://www.tech-faq.com/securing-database-servers.html*

Naciones Unidas (s.f.). *Introduccion a Base de datos.* Recuperado el 10 de noviembre de 2011, de *http://www.un.org/spanish/Depts/dpi/seminario/pdf/basesdedatos.pdf*

Walus, J. (s.f.). *Base de datos.* Recuperado el 14 de noviembre de 2011*, de http://es.wikipedia.org/wiki/Base_de_datos*

SliderShare (s.f.). *Universidad Tecnica Particula de Loja – Seguridad Base de Datos.* Recuperado el 10 de noviembre de 2011, de *http://www.slideshare.net/juank_my/seguridades-en-bases-de-datos*

Sanchez, F. (s.f.). *Consultora Sisp – Ciencias de la Seguridad.* Recuperado el 12 de noviembre de 2011, de *http://fms-seguridades.blogspot.com/*

Los Tiempos (s.f.). *Seguridades.* Recuperado el 14 de noviembre de 2011, de *http://www.lostiempos.com/diario/opiniones/columnistas/20110820/seguridades_138448_283332.html*

Walus, J. (s.f.). *Copia de Seguridad.* Recuperado el 14 de noviembre de 2011, de *http://es.wikipedia.org/wiki/Copia_de_seguridad*

Leyton, E (03.2000). *Auditoria a la seguridad y ambiente de control informatico.* Recuperado el 16 de noviembre de 2011, de *http://www.eduardoleyton.com/apuntes/Programas_Auditorias.pdf*

Cotas (2007). *DataCenter.* Recuperado el 08 de noviembre de 2011, de *http://www.datacenter.cotas.net/Datacenter.html*

CII 7 (s.f.). *Expo DataCenter.* Recuperado el 06 de noviembre de 2011, de *http://www.expodatacenter.com/*

Entelgy (s.f.). DataCenter 3.0. Recuperado el 10 de noviembre de 2011, de *http://www.entelgy.com/que-hacemos/areas-de-especializacion/data-center-30.php*

SIS (s.f.). *Servidores Dedicados.* Recuperado el 10 de noviembre de 2011, de *http://www.sisargentina.com/datacenter.html*

Data Consultores (s.f.). *DataCenter Green.* Recuperado el 14 de noviembre de 2011, de *http://www.datacenterconsultores.com/*

SINAR (s.f.). *Sistema Nacional de Archivos - Ley de Comercio Electronico.* Recuperado el 14 de noviembre de 2011, de *http://www.sinar.gov.ec/downloads/L_comercio.pdf*

Horvanth, Al (1972.). *Firmesa - DataCenter.* Recuperado el 05 de noviembre de 2011, de *http://www.firmesa.com/web/index.php?option=com_aicontactsafe&view=message&layout=message&pf=6&Itemid=215*

ANEXOS

Anexo I

Encuestas

Anexo II

Artículos de derecho de seguridad informática