DECANATO DE INGENIERÍA E INFORMÁTICA

Escuela de Informática

Trabajo De Grado Para Optar Por El Titulo De:

Ingeniero(a) de Sistemas de Computación

Diseño e implementación de un plan de redundancia y alta disponibilidad mediante un sistema de base de datos (SQL Server) para la Contraloría General de la República, en Santo Domingo, en el periodo Septiembre – Diciembre 2014.

Sustentantes:

Saúl Espinosa de la Rosa	2006-2201
Luis Ramón Santos Custodio	2009-2058
Jorge Luis Beltré Cepeda	2010-0599

Asesor:

Ing. Freddy Jiménez

Santo Domingo, Rep. Dom.
Noviembre, 2014

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Tema:

Diseño e implementación de un plan de redundancia y alta disponibilidad mediante un sistema de base de datos (SQL Server) para la Contraloría General de la República, en Santo Domingo, en el periodo Septiembre – Diciembre 2014.

AGRADECIMIENTOS

A Dios

Por iluminarme el camino y llenarme de grandes bendiciones en mi vida, gracias padre amado por todo.

A mi Familia

Por su gran apoyo en especial a mi padre **Guarionex Espinosa Beltre,** por siempre darme su confianza en este proceso de mi vida y en muchos más. A mi querida madre **Reyita O. de la Rosa** por siempre confiar y creer en mí, de ti aprendí como se debe luchar para conseguir lo que uno quiere “eres una luchadora Incansable”.

A mi Esposa

Leidy Lee Camacho Acosta por su paciencia y confianza en que yo lo lograría, por darme su amor cuando estaba cansado y darme mi tres luceros en la vida Yolenny ,Sally Esther y Liz Maritza, las amos.

A mi asesor:

Ing. Freddy Jiménez, por su gran esfuerzo para que las cosas quedaran bien.

Gracias, porque siempre estuvo dispuesto a colaborar conmigo en todo momento.

Saul Espinosa de la Rosa

A mis compañeros de tesis:

Saúl Espinosa, Jorge Luis Beltré, por estar disponibles en todo momento y superar juntos este gran acontecimiento en nuestras vidas.

A mi asesor:

Ing. Freddy Jiménez, por la orientación y ayuda que me brindo para la realización de esta tesis, y su apoyo incondicional que me permitieron aprender muchas más que lo presentado en este proyecto.

A mi rectora:

Ing. Hayser Beltre y su Secretaria Aquino, por haber estado disponible siempre que presentamos cualquier inconvenientes referente a la universidad, sin ustedes no hubiera estado aquí, gracias de todo corazón.

A mis compañeros de universidad:

James Martínez, Waldo José, Ricardo González, por superar juntos todos los retos que nos fueron presentados en el transcurso de la carrera, gracias por siempre estar disponibles para mí.

Luis Ramón Santos Custodio

A Dios,

Por qué siempre está presente en mi vida ayudándome a superar cualquier obstáculo, por darme la fuerza y la sabiduría para cumplir con los objetivos propuesto, muchas gracias **Dios** todopoderoso por cuidarme y protegerme.

A mis Padres,

Luis Manuel Beltré que siempre ha estado presente dándome sus más sabios consejos para el trayecto de mi vida, ayudándome en cada paso que doy día a día para lograr lo que me propongo, gracias al mejor padre que puede existir en el universo porque gracias a ti estoy hoy aquí. **María Isabel Cepeda** por todo el amor que me das y por haberme cuidado nueve maravillosos meses dentro de tu vientre, haberme dado la vida es un privilegio y hoy les dedico este maravilloso paso de mi vida.

A mi Asesor,

Por haber aceptado el reto de brindar su ayuda y estar disponible cada vez que lo necesitábamos para llevar a cabo el cumplimiento de esta investigación, por su apoyo para que todo salga bien y por haber dicho como son las cosas, gracias **Ing. Freddy Jiménez** más que un asesor y maestro un amigo.

A mis Compañeros de Trabajo de Grado,

Saúl espinosa y Luis Ramón, por ser de gran soporte para la elaboración de este trabajo y porque a pesar de los inconvenientes que tuvimos lo superamos conjuntamente, mis agradecimientos infinito para ambos de todo corazón.

Jorge Luis Beltré Cepeda

A Cisco

Por sus imágenes de sus routers.

A la Contraloría General de la Republica

Por permitirnos hacer este trabajo basado en su sistema actual y para una mejoría inmediata.

A Consentry

Por sus imágenes de sus Switchs

A Nuestra Universidad Apec

Por todas las facilidades brindadas a lo largo de nuestra carrera y en esta última etapa de la misma.

Agradecimientos en General

DEDICATORIAS

Quiero dedicarle este Proyecto a **DIOS**, el arquitecto de mi vida quien siempre me ha guiado en el camino del bien y me ha bendecido con la fuerza de voluntad para seguir siempre adelante y completar este largo recorrido.

A mis padres: **Reyita O. de la Rosa y Guarionex Espinosa Beltre**

Por su apoyo, comprensión y todo el amor que siempre me dan. Gracias por su sustento y el cariño incondicional que me han brindado. Muchísimas gracias por Haberme guiado por buen camino en todo el transcurso de mi vida y por apoyarme sin límites para mí preparación académica.

A mi esposa **Leidy lee Camacho Acosta**

Realmente un ser fuera de serie mi esposa, mi amiga mi todo. Gracias por soportarme y tolerarme, por ser luz en todas mis decisiones. Has sido para mí un ejemplo de fe y perseverancia y me has demostrado que con amor y entrega todo se puede lograr. Eres parte fundamental en mi vida y junto alcanzaremos todos nuestras metas esta es una y te la dedico agradeciéndote y diciendo que te amo.

A mis hijas: **Yolenny, Sally Esther y Lee Maritza**

Porque son mi gran motivación desde que llegaron a mi vida solo puedo decir que las amos.

Saul Espinosa de la Rosa

A mis hermanas: **Katiuska y Ninoska**

Porque son parte de mi familia que tanto aprecio y por soportarme siempre las quiero muchísimo.

A mis abuelos:

Vicenta Beltre y Carmelo Espinosa, André b. de la Rosa (niño), por su amor, buenos consejos y todo el cariño que siempre me han dado.

A mis tíos:

José (papo), Maribel (nana), por ser motivo de alegría en mi vida y por sus aportes para lograr mi preparación profesional. **Maritza mercedes Espinosa**, espero que Dios la tenga en gloria y desde aquí les mando mi más estimado agradecimiento por todo el amor y alegría que brindo en la tierra.

A mis sobrinos: **Abdiel y Samuel**

Porque me llenan de felicidad en cada momento, con sus ocurrencias y travesuras.

A mis primos:

Victalia, Leny, Yorkiris (mella), Joel (mello), Víctor. Que esto sea de motivación para que cumplan todas sus metas porque si se puede.

Saul Espinosa de la Rosa

A mis Compañeros y amigos:

Luis, Fido, Alberto (papolo), Jason, Anny, Jelinson, Lee, Jonathan, Martin, Jesusito, Waskar, Ariel, Josia, Eddy, Delwi, Thomas, Jean Carlo y todos los que me faltaron por mencionar gracias por siempre estar hay son personas maravillosas que han aportado algo en mi preparación.

Saul Espinosa de la Rosa

En primer lugar a Dios, el cual me ha permitido tener una vida llena de alegrías y aprendizaje, permitiéndome desarrollarme en la Universidad y demás etapas de mi vida.

A mis padres:

Luis Vicente Santos Hernández y Elizabeth Guillermina Custodio Cobo, por todo su apoyo incondicional, siempre estar dispuestos a dar la cara en todo momento independientemente de cuál sea el reto que me haya trazado, gracias por toda su paciencia y comprensión a lo largo de todos estos años.

A mi hermana:

Lorens María Santos Custodio, por estar siempre dispuesta a ayudarme en toda ocasión que la he necesitado.

A mi familia en general:

Por su incondicional apoyo a lo largo de mi vida y metas, por siempre aconsejar que si se quiere se puede lograr ya que no hay metas inalcanzables.

A mis amigos:

Que siempre estuvieron a mi lado para ayudarme, escucharme, aconsejarme y guiarme en todas las ocasiones que fueron necesarios.

Luis Ramón Santos Custodio

Antes que nada debo y quiero dedicarle esta etapa de mi vida al todopoderoso papa **Dios,** que me permitió culminar una de las maravilla de mi vida y que siempre me ha dado la sabiduría de seguir los buenos pasos siempre con cautela.

A mis padres,

Luis Manuel Beltré y María Isabel Cepeda, por toda su comprensión y amor que me han brindado durante todos estos años de mi vida, por darme el apoyo tanto familiar como económico y demás. Muchas gracias por siempre darme los mejores consejos de mi vida, por estar siempre presente para mí y dispuesto a colaborar, gracias por haberme hecho un hombre de bien.

A mis Hermanos,

Por estar siempre pendientes de mí y de cómo me iba en la universidad, por ayudarme en los momentos que lo necesitaba, gracias a **María Elizabeth Beltré** que en difíciles momentos me llevaba a la universidad y aunque sea como sea conmigo es lo más pequeño de la casa y parte de mi vida Te adoro. **Luis Enrique Beltré** uno de mis hermanos mayores y mi ejemplo a seguir porque siempre me ha inspirado a seguir sus mismos pasos**. Jeudy Beltré** porque a pesar de la distancia cada vez que se comunica conmigo me recalca siempre lo que debo hacer. Mis demás Hermanos los que están y los que no están les dedico este gran paso y gracias por todo.

Jorge Luis Beltré Cepeda

A mis Abuelos,

Don Manuel Cepeda y Luz María Marte, (abuelos maternos) por todo el cariño y amor que me han brindado durante mi crecimiento, les agradezco infinitamente por todo y por estar presente en mi vida**, José Remedio Beltré y Ana Rita Tejeda,** (abuelos paternos) aunque nunca los llegue a conocer les dedico este acontecimiento de mi vida y sé que desde el cielo se deben sentir orgullosos.

A mis demás familiares,

(Tíos, Primos, Sobrinos, padrinos) por ser parte de mí y estar presente en muchos momentos de mi vida, les agradezco las veces en que me dieron consejos para bien, muchas gracias por todo los quiero mucho.

A mi novia,

Luz López Pineda, por darme maravillosos momentos en mi vida, por compartir conmigo y estar presente siempre para mí, por estar dispuesta ayudarme y escucharme en todo momento, por aconsejarme y cuidarme, por aguantarme y siempre dispuesta a pasar cualquier obstáculo conmigo, Te Adoro.

A mis Amigos (as),

A los que realmente son mis amigos, los que siempre me apoyaron y ayudaron en cualquier momento, con los que comparto mis alegrías y locuras con los que siempre estoy en comunicación y me han brindado momentos felices, los que me aconsejaron y escucharon en todo momento.

Jorge Luis Beltré Cepeda

Resumen Ejecutivo

Analizando el problema, se verifica que la mayoría de los servicios informáticos se encuentran centralizados en los diferentes servidores de la institución, si alguno de estos presenta una falla, se vería afectado todo el sistema institucional ya que en estos se alojan todas las informaciones de desembolsos de pagos del estado. Cabe destacar que la antigüedad de estos equipos causa una gran deficiencia ante las exigencias informáticas, impidiendo un buen desempeño a la hora de responder a una necesidad. Además, estos equipos presentan una escasa compatibilidad con nuevas tecnologías que podrían ayudar a aprovechar al máximo el espacio y funcionamiento de los mismos.

Una de estas medidas es el uso de equipos en los cuales se replique la información almacenada en los servidores principales de la organización. Esto garantiza la disponibilidad de la información en caso de pérdidas accidentales o fallas en los equipos.

Analizando el caso de estudio, se considera de suma importancia que la Contraloría General de la República adopte este tipo de medidas con el fin de prevenir situaciones que pongan en riesgo la información almacenada en los servidores vigentes.

La pérdida de información vital acarrearía graves problemas en el manejo del control interno del Estado. Por lo tanto, si ocurre un fallo en la infraestructura de la institución, esto puede causar que no se pueda realizar de manera adecuada la revisión de los registros contables de las diferentes entidades y organismos del Estado. En el peor de los escenarios, la perdida de registros contables puede ocasionar que se ponga en

duda las observaciones y/o recomendaciones otorgadas por la Contraloría General de la República, y esto a su vez, puede cuestionar la eficiencia de la gestión del Contralor en función.

Introducción

La Contraloría General de la República está ubicada en Gazcue, av. México #45 edificio de finanzas, en Santo Domingo, República Dominicana es la institución encargada de auditar todas las ordenes de pagos del gobierno dominicano.

El activo más importante que tiene una organización es la información que esta procesa y/o maneja, por lo que es necesario garantizar la disponibilidad e integridad de la misma. Para esto la dirección de tecnología de la información (TI) de cada organización o empresa planifica las medidas de seguridad necesarias para cumplir con este objetivo.

En la actualidad esta entidad no posee ningún mecanismo de redundancia de datos lo que puede ocasionar pérdida de información valiosa para la institución. La redundancia de datos se refiere a la réplica de datos e información en uno o varios equipos diferentes al que se encuentra almacenado.

Con esta investigación se buscara las soluciones a la problemática planteada con fines de que la Contraloría General de la Republica pueda obtener un mayor desenvolvimiento y eficiencia a la hora de tener los datos a la mano, para esto se analizaran cuales mecanismos de redundancia podrían ser útiles para tener una mejora en la institución y a su vez evitar la pérdida de cualquier tipo de información a toda costa.

Por otro lado se pretenden analizar los factores que podrían producir los fallos a favor de la perdida de información para así minimizarlos al punto de que sea evitable que se

produzca alguna ruptura en los servidores que poseen los datos. Es muy importante que la institución tenga mayor control con los usuarios que interactúan con los servicios y con el manejo de la información, se deben obtener reportes de los servidores cada x tiempo periódico para así evitar un mal funcionamiento.

Las bases de datos son un área de la ingeniería que ha recibido bastante atención debido a sus múltiples aplicaciones: automatización de oficinas, ingeniería de software, bibliotecas, diccionarios automatizados y en lo general cualquier sistema orientado a mantenerse y recuperar información importantes de la organizaciones e instituciones y empresa. Su recuperación, actualización y manejo es relativamente sencillo con el uso de cualquier manejador de bases de datos SQL. Cuando hablamos de archivos con estructura nos estamos refiriendo a documentos cuya estructura es declarada de algún modo, asociamos etiquetas a algún elemento de una estructura o mediante sintaxis con la que se escribe el archivo, como se hace en los lenguajes de programación.

Aspectos metodológicos de la investigación

Tipo de estudio

El análisis de esta investigación corresponde al primer nivel del conocimiento, es decir, el tipo de estudio exploratorio o formulativo. Este tipo de estudio permite realizar una investigación precisa de una problemática observada, de esta manera se da lugar a un marco teórico de referencia que sirva de apoyo al desarrollo de la investigación.

Método de investigación

Para este trabajo de investigación se utilizará como guía el método de análisis. Este tipo de método de investigación permite analizar cada una de las partes que caracterizan una realidad problemática, y a partir de esta se desarrolla un análisis de las consecuencias y posibles recomendaciones a fin de dar solución al problema.

Fuentes y técnicas de recolección de información

Para el desarrollo de la unidad de investigación se utilizará como fuente primaria la observación directa por parte de uno de los empleados de la entidad analizada, quien a su vez, es parte del equipo de investigación que sustenta este trabajo.

Además, se considera adecuado emplear el uso de entrevistas al personal del área de informática de la Contraloría General de la República con la finalidad de obtener información detallada de la situación problemática para poder enfocar la investigación a una solución que garantice resultados positivos y permanentes.

Capítulo 1
Antecedente Histórico de la Institución

1.1. Reseña Histórica

Contraloría General de la República Dominicana: Origen y evolución El Sistema Nacional de Control de la República Dominicana descansa en la actualidad en dos pilares fundamentales: Control Externo y Control Interno, teniendo el primero como organismo ejecutor a la Cámara de Cuentas y, el segundo, a la Contraloría General de la República.

Esa primera institución tiene su fundamento legal en la Ley 10-04 mientras que la Contraloría General de la República lo hace a través de la Ley 10-07, no obstante, las ejecuciones de control del Estado aparecen en la primera Constitución de la República, proclamada en San Cristóbal, el 6 de noviembre del 1844. Este ejercicio de control se realizaba a través de un organismo denominado Consejo Administrativo.

El artículo 182 de la referida Constitución dominicana, indica que "la ley organizará un Consejo Administrativo compuesto por funcionarios públicos para verificar anualmente las cuentas generales y hacer un informe de ellas al Congreso, con las observaciones que juzgue oportunas, cuyo encargo será puramente gratuito".

Mediante la Ley No. 42 promulgada el 12 de junio de 1845, se crea la "Contaduría General" como una dependencia de la Secretaría de Estado de Hacienda y Comercio, cuyas funciones, al tenor del numeral 1 del artículo 2 de la mencionada ley, eran las siguientes: "Examinar, verificar, arreglar y centralizar todas las cuentas de la Tesorería General ".

Posteriormente, la Ley 75 del 7 de mayo de 1846 deroga la Ley No.42 y amplía las funciones del Administrador e Inspector General y del Consejo Administrativo, que a la sazón estaba integrado por empleados públicos dirigidos por el Presidente de la República. Es durante la aplicación de esta iniciativa, que se produjeron inexactitudes sobre las funciones de los diferentes servidores públicos, lo que originó la promulgación de una nueva legislación que se detalla en el próximo párrafo.

La Ley 114 del 2 de julio de 1847, modifica y amplía las atribuciones del Contador General, que como administrador e inspector general le atribuía la mencionada Ley No.42, a los fines de solucionar los inconvenientes que se producían en la aplicación de la Ley 75.

La Resolución No. 9 de fecha 10 de abril del 1897, crea el Departamento Examinador de Cuentas, cuya misión principal era inspeccionar y desglosar las cuentas del Estado por parte de los oficiales de la Oficina de Asuntos Insulares (Bureau of Insular Affairs), bajo la dirección del Departamento de Guerra de los Estados Unidos de América.

Mientras, la Orden Ejecutiva No. 563 de fecha 20 de noviembre de 1920, que contenía la Ley de Hacienda y que modifica la Ley 114, es la primera que contempla una diferencia entre Tesorero y Auditor, y reparte las funciones del Contador General entre los ya citados cargos. Por el seguimiento cronológico e histórico se ha podido establecer que las funciones de control siempre se ejercieron aunque bajo diversas denominaciones.

Durante la presidencia de Horacio Vásquez, se promulga el 3 de mayo de 1929, la Ley No.1114 de Contabilidad General que da origen a la "Oficina de Contabilidad General",

independiente de los departamentos administrativos bajo el control y dirección de un Contralor General de la República Dominicana.

Es importante hacer notar, que es a partir de esta ley que la Contraloría adquiere independencia con respecto a su objeto de oficina de control financiero y fiscalización de las operaciones de ingresos y egresos del Estado.

En ese orden, el 9 de agosto del 1954 y mediante Ley 3894, se crea la “Contraloría y Auditoría General de la República”. A la que luego se le modificaría el artículo 1, a través de la Ley No.54 del 1970, sustituyendo la denominación de "Contraloría y Auditoría General de la República por "CONTRALORÍA GENERAL DE LA REPÚBLICA”. Desde este entonces queda establecida la dependencia directa de esta Institución del Poder Ejecutivo en el organigrama del Estado Dominicano:

“Art.1 (Modificado por la Ley No.54 del 13 de noviembre de 1970, G. O. No.9205). La Contraloría General de la República (bajo la dependencia directa del Poder Ejecutivo en virtud a lo dispuesto por el Art. 1 de la Ley No. 54, precitada), y la que estará bajo la dirección de un funcionario que se denominará Contralor General de la República ; también habrá un Sub-Contralor General; tendrá a su cargo la contabilidad general del Estado, fiscalizar el debido ingreso e inversión de los fondos de los diversos departamentos de la Administración Pública, autónomos o no, del Estado y de los municipios; verificar el examen de las que deban rendir las personas o entidades que reciban o manejen fondos o bienes de tales entidades u organismos, así como la inspección contable de las oficinas correspondientes a los mismos”.

El 27 de julio de 2001, como resultado de modificaciones que se habían realizado en el sector financiero nacional, se crea mediante la Ley No. 126-01 la Dirección General de Contabilidad Gubernamental; esta ley asume parte de las funciones que la Ley 3894 le asignaba a la Contraloría General de la República, y que venía ejecutando al amparo de otras legislaciones.

Con la nueva Ley 10-04 del 20 de enero del 2004 a la Cámara de Cuentas se le otorga la potestad de realizar el control externo, sobre las entidades generadoras y ejecutoras del presupuesto nacional, función que también realizaba la Contraloría General de la República desde sus inicios, lo que provocaba una duplicidad de funciones.
En tanto, la Ley 10-07, del 4 de enero de 2007, designa a la Contraloría General de la República como Órgano Rector del Control Interno del Estado.

Cabe resaltar que el modelo del Sistema Nacional de Control establecido en República Dominicana es único debido a que en los demás países existe una sola entidad de control, esto es, o una Contraloría General o un Tribunal de Cuentas, o Cámara de Cuentas.

Ahora que se dispone de una nueva herramienta legal y siguiendo los pasos indicado por su reglamento, se ha desarrollado un proceso tendente a socializarla con todos los miembros de la Contraloría, y concomitantemente con los que integran los distintos organismos generadores y ejecutores del Presupuesto Nacional, a los fines de aplicar con propiedad los mandatos de las presentes normativas.

Partiendo de la dinámica de las sociedades a la que no escapan las instituciones y sus normas, la movilidad evolutiva de estas es eterna, por lo que en cada momento si así lo determinan las circunstancias, esta ley deberá ser modificada para que pueda responder a las exigencias de la época.

1.2. Visión

Ser reconocida como el órgano rector del control interno, agregando valor a la gestión pública para garantizar ejecutorias óptimas y transparentes [7].

1.3. Misión

Somos el órgano rector del sistema nacional de control interno, fiscalizador del debido recaudo, manejo, uso e inversión de los recursos públicos, responsables de autorizar las órdenes de pago, mediante revisiones y consultorías objetivas que generen resultados oportunos, a través de procesos automatizados y estandarizados, recursos humanos idóneos y metodologías basadas en gestión de riesgo; contribuyendo al mejoramiento continuo de las instituciones bajo el ámbito de la ley, creando rentabilidad social [7].

1.4. Valores

Confiabilidad: Gestión basada en altos estándares profesionales, garantizando un desempeño eficiente orientado al logro de resultados.

Legalidad: Aplicamos y supervisamos el cumplimiento de la constitución y las disposiciones legales, reglamentarias y administrativas vigentes.

Probidad: Actuamos de manera íntegra y objetiva, cumpliendo con la ética profesional.

Discreción: Manejamos con prudencia y criterios confidenciales e institucionales, las informaciones y todo recurso bajo nuestro ámbito de responsabilidad.

Respeto a la Diversidad: Valoramos a las personas y sus formas de pensamiento, independientemente de sus condiciones.

Transparencia: Garantizamos el acceso a la información pública, sobre los procesos y los resultados que estos generan [7].

1.5. Organigrama

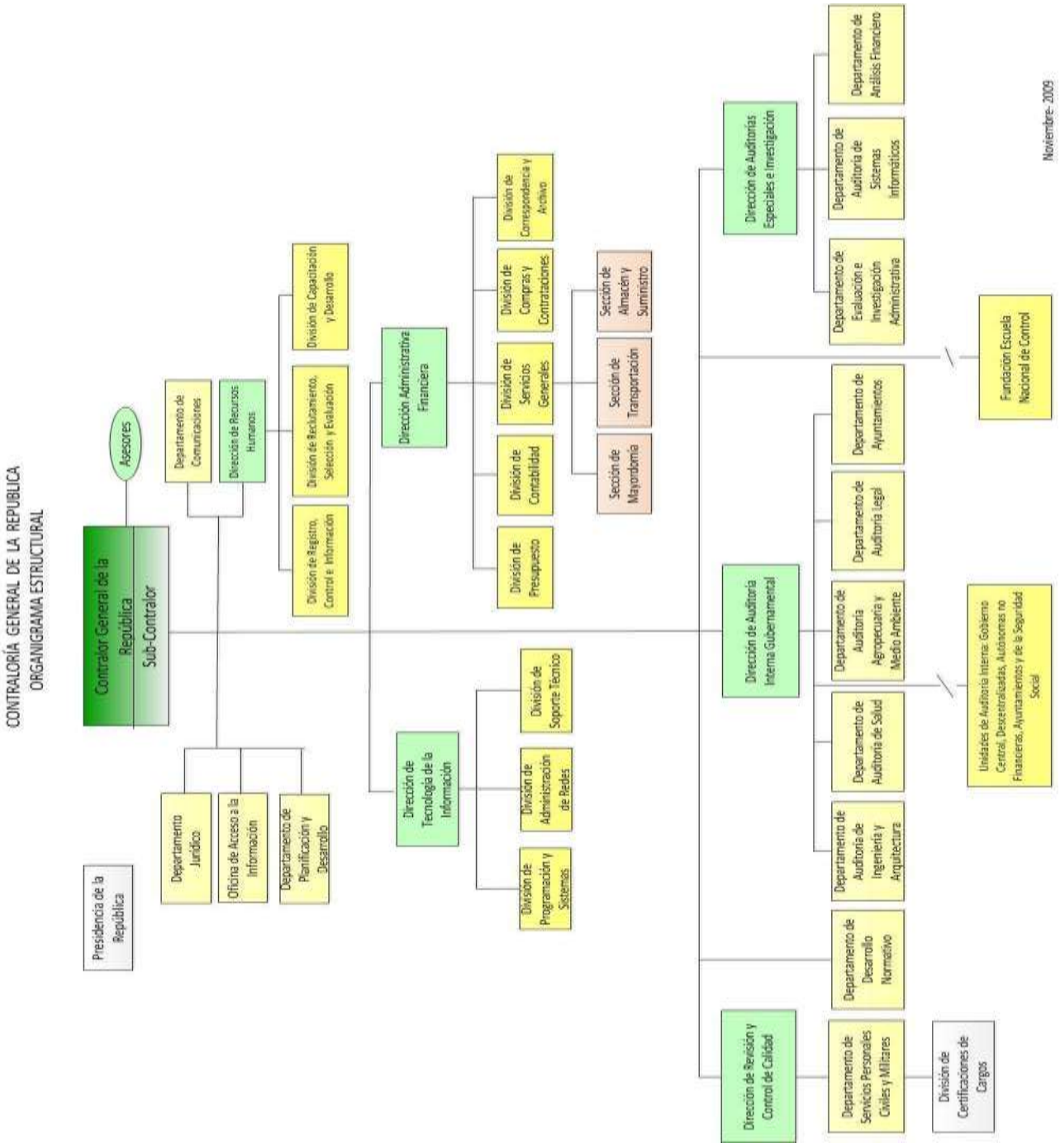

Figura 1.1 Esquema Organizacional Contraloría General Fuente: Contraloría

Capítulo 2
Conceptos de Base de Datos SQL Server

2.1. Características de SQL server

Según Olga Pons, N. M. [15] define el SQL como un lenguaje de acceso a bases de datos que explota la flexibilidad y potencia de los sistemas relacionales y permite así gran variedad de operaciones.

Es un lenguaje declarativo de "alto nivel" o "de no procedimiento" que, gracias a su fuerte base teórica y su orientación al manejo de conjuntos de registros y no a registros individuales permite una alta productividad en codificación y la orientación a objetos. De esta forma, una sola sentencia puede equivaler a uno o más programas que se utilizarían en un lenguaje de bajo nivel orientado a registros. SQL también tiene las siguientes características:

Figura 2.1 SQL Server Fuente: Microsoft

- **Lenguaje de definición de datos:** El LDD de SQL proporciona comandos para la definición de esquemas de relación, borrado de relaciones y modificaciones de los esquemas de relación.
- **Lenguaje interactivo de manipulación de datos:** El LMD de SQL incluye lenguajes de consultas basado tanto en álgebra relacional como en cálculo relacional de tuplas.

- **Integridad:** El LDD de SQL incluye comandos para especificar las restricciones de integridad que deben cumplir los datos almacenados en la base de datos.
- **Definición de vistas:** El LDD incluye comandos para definir las vistas.
- **Control de transacciones:** SQL tiene comandos para especificar el comienzo y el final de una transacción.
- **SQL incorporado y dinámico:** Esto quiere decir que se pueden incorporar instrucciones de SQL en lenguajes de programación como: C++, C, Java, PHP, Cobol, Pascal y Fortran.
- **Autorización:** El LDD incluye comandos para especificar los derechos de acceso a las relaciones y a las vistas.

2.2. Tipos de Datos

Algunos de los tipos de datos básicos de SQL son:

Date: una fecha de calendario que contiene el año (de cuatro cifras), el mes y el día.

Time: La hora del día en horas minutos segundos (el valor predeterminado es 0).

Timestamp: la combinación de Date y Time [5].

2.3. Optimización

Como ya se dijo antes, y suele ser común en los lenguajes de acceso a bases de datos de alto nivel, el SQL es un lenguaje declarativo. O sea, que especifica qué es lo que se quiere y no cómo conseguirlo, por lo que una sentencia no establece explícitamente un orden de ejecución.

El orden de ejecución interno de una sentencia puede afectar seriamente a la eficiencia del SGBD, por lo que se hace necesario que éste lleve a cabo una optimización antes de su ejecución. Muchas veces, el uso de índices acelera una instrucción de consulta, pero ralentiza la actualización de los datos. Dependiendo del uso de la aplicación, se priorizará el acceso indexado o una rápida actualización de la información. La optimización difiere sensiblemente en cada motor de base de datos y depende de muchos factores.

Existe una ampliación de SQL conocida como FSQL (Fuzzy SQL, SQL difuso) que permite el acceso a bases de datos difusas, usando la lógica difusa. Este lenguaje ha sido implementado a nivel experimental y está evolucionando rápidamente [5].

2.4. Definición de SQL

Según Gabillaud, J. [20] define que las aplicaciones en red son cada día más numerosas y versátiles. En muchos casos, el esquema básico de operación es una serie de scripts que rigen el comportamiento de una base de datos.

Debido a la diversidad de lenguajes y de bases de datos existentes, la manera de comunicar entre unos y otras sería realmente complicada a gestionar de no ser por la existencia de estándares que nos permiten el realizar las operaciones básicas de una forma universal.

Es de eso de lo que trata el SQL (Structured Query Language) que no es más que un lenguaje estándar de comunicación con bases de datos. Hablamos por tanto de un lenguaje normalizado que nos permite trabajar con cualquier tipo de lenguaje (ASP o PHP) en combinación con cualquier tipo de base de datos (MS Access, SQL Server, MySQL, entre otros).

El hecho de que sea estándar no quiere decir que sea idéntico para cada base de datos. En efecto, determinadas bases de datos implementan funciones específicas que no tienen necesariamente que funcionar en otras.

Aparte de esta universalidad, el SQL posee otras dos características muy apreciadas. Por una parte, presenta una potencia y versatilidad notables que contrasta, por otra, con su accesibilidad de aprendizaje.

2.5. Reseña Historia de SQL

James R. Groff [28], El concepto de base de datos relacional fue desarrollado originalmente por el Dr. E. F. Codd (“Ted”), un investigador de IBM. En junio de 1970, el Dr. Codd publicó un artículo titulado “Un modelo relacional de datos para grandes bancos de datos compartidos”, que esbozaba una teoría matemática del modo en que se podían almacenar y manipular los datos empleando una estructura tabular.

El artículo de Codd desato un frenesí de investigación en bases de datos relacionales, incluido un importante proyecto de investigación de IBM. El objetivo del proyecto, denominado System/R, era comprobar la operatividad del concepto relacional y proporcionar experiencia en la implementación real de un SGBD relacional.

Por otro lado en la Década de 1950 y principios de la década de 1960. Se desarrollaron las cintas magnéticas para el almacenamiento de datos. Las tareas de procesamiento de datos tales como las nóminas fueron automatizadas, con los datos almacenados en cintas. El procesamiento de datos consistía en leer datos de una o más cintas y escribir datos en una nueva cinta. Los datos también se podían introducir desde paquetes de tarjetas perforadas e impresos en impresoras. Por ejemplo, los aumentos de sueldo se procesaban introduciendo los aumentos en las tarjetas perforadas y leyendo el paquete de cintas perforadas en sincronización con una cinta que contenía los detalles maestros de los salarios. Los registros debían estar igualmente ordenados. Los aumentos de sueldo tenían que añadirse a los sueldos leídos de la cinta maestra, y escribirse en una nueva cinta; esta nueva cinta se convertía en la nueva cinta maestra. Las cintas (y los paquetes de tarjetas perforadas) sólo se podían leer secuencialmente, y los tamaños de datos eran mucho mayores que la memoria principal; así, los

programas de procesamiento de datos tenían que procesar los datos según un determinado orden, leyendo y mezclando datos de cintas y paquetes de tarjetas perforadas.

• Finales de la década de 1960 y la década de 1970.El amplio uso de los discos fijos a finales de la década de 1960 cambió en gran medida el escenario del procesamiento de datos, ya que los discos fijos permitieron el acceso directo a los datos. La ubicación de los datos en disco no era importante, ya que a cualquier posición del disco se podía acceder en sólo decenas de milisegundo. Los datos se liberaron de la tiranía de la secuencialidad. Con los discos pudieron desarrollarse las bases de datos de red y jerárquicas, que permitieron que las estructuras de datos tales como listas y árboles pudieran almacenarse en disco. Los programadores pudieron construir y manipular estas estructuras de datos. Un artículo histórico de Codd [1970] definió el modelo relacional y formas no procedimentales de consultar los datos en el modelo relacional, y nacieron las bases de datos relacionales. La simplicidad del modelo relacional y la posibilidad de ocultar completamente los detalles de implementación al programador fueron realmente atractivas. Codd obtuvo posteriormente el prestigioso premio Turing de la ACM (Association of Computing Machinery, Asociación de Maquinaria Informática) por su trabajo.

Década de 1980.Aunque académicamente interesante, el modelo relacional no se usó inicialmente en la práctica debido a sus inconvenientes por el rendimiento; las bases de datos relacionales no pudieron competir con el rendimiento de las bases de datos de red y jerárquicas existentes. Esta situación cambió con System R, un proyecto innovador en IBM Research que desarrolló técnicas para la construcción de un sistema

de bases de datos relacionales eficiente. En Astrahan et al. [1976] y Chamberlin et al. [1981] se pueden encontrar excelentes visiones generales de System R. El prototipo de System R completamente funcional condujo al primer producto de bases de datos relacionales de IBM: SQL/DS. Los primeros sistemas de bases de datos relacionales, como DB2 de IBM, Oracle, Ingres y Rdb de DEC, jugaron un importante papel en el desarrollo de técnicas para el procesamiento eficiente de consultas declarativas. En los principios de la década de 1980 las bases de datos relacionales llegaron a competir con los sistemas de bases de datos jerárquicas y de red incluso en el área de rendimiento. Las bases de datos relacionales fueron tan sencillas de usar que finalmente reemplazaron a las bases de datos jerárquicas y de red; los programadores que usaban estas bases de datos estaban forzados a tratar muchos detalles de implementación de bajo nivel y tenían que codificar sus consultas de forma procedimental. Aún más importante, debían tener presente el rendimiento durante el diseño de sus programas, lo que implicaba un gran esfuerzo. En cambio, en una base de datos relacional, casi todas estas tareas de bajo nivel se realizan automáticamente por la base de datos, liberando al programador en el nivel lógico. Desde su escalada en el dominio en la década de 1980, el modelo relacional ha conseguido el reinado supremo entre todos los modelos de datos.

La década de 1980 también fue testigo de una gran investigación en las bases de datos paralelas y distribuidas, así como del trabajo inicial en las bases de datos orientadas a objetos.

Principios de la década de 1990.El lenguaje SQL se diseñó fundamentalmente para las aplicaciones de ayuda a la toma de decisiones, que son intensivas en consultas, mientras que el objetivo principal de las bases de datos en la década de 1980 fue las aplicaciones de procesamiento de transacciones, que son intensivas en actualizaciones. La ayuda a la toma de decisiones y las consultas reemergieron como una importante área de aplicación para las bases de datos. Las herramientas para analizar grandes cantidades de datos experimentaron un gran crecimiento de uso. Muchos vendedores de bases de datos introdujeron productos de bases de datos paralelas en este periodo, así como también comenzaron ofrecer bases de datos relacionales orientadas a objeto.

Finales de la década de 1990. El principal acontecimiento fue el crecimiento explosivo de World Wide Web. Las bases de datos se implantaron mucho más extensivamente que nunca antes. Los sistemas de bases de datos tienen ahora soporte para tasas de transacciones muy altas, así como muy alta fiabilidad y disponibilidad 24×7 (disponibilidad 24 horas al día y 7 días a la semana, que significa que no hay tiempos de inactividad debidos a actividades de mantenimiento planificadas). Los sistemas de bases de datos también tuvieron interfaces Web a los datos.

2.6. Lenguaje de SQL (T-SQL)

En la definición de Navathe, R. A. [30] Transact-SQL (T-SQL) es una extensión al SQL de Microsoft y Sybase. SQL, que fundamentalmente se dice que es un Lenguaje de Búsquedas Estructurado, este lenguaje esta estandarizado, fue desarrollado originalmente por IBM para realizar búsquedas, para definir y alterar bases de datos utilizando sentencias declarativas. T-SQL expande el estándar de SQL para incluir programación procedural, variables locales, varias funciones de soporte para procesamiento de strings, procesamiento de fechas, matemáticas, etc. Además cambios a las sentencias DELETE y UPDATE. Estas características adicionales hacen de T-SQL un lenguaje que cumple con las características de un autómata de Turing.

Tabla 2.2 Lenguaje de T-SQL Fuente: Google

2.6.1. Objetos Básicos de SQL

Constante: Una constante, también conocida como valor literal o escalar, es un símbolo que representa un valor de datos específico. El formato de las constantes depende del tipo de datos del valor que representan [30].

2.7. Delimitadores (Triggers)

La coincidencia de delimitadores de Transact-SQL informa de manera inmediata sobre si están escritos correctamente los elementos de sintaxis que deben ir emparejados en el código. El editor de Transact-SQL comprueba si coinciden los delimitadores que identifican los límites de los bloques de código. La concordancia se realiza de la siguiente forma:

- El editor resalta los dos delimitadores de un par cuando se termina de escribir el segundo delimitador del par [31].

2.7.1. Comentarios

Indica texto proporcionado por el usuario. Los comentarios se pueden insertar en una línea independiente, anidada al final de una línea de comandos de Transact-SQL o dentro de una instrucción de Transact-SQL El servidor no evalúa los comentarios [25].

2.7.2. Identificadores

En Transact SQL los identificadores de variables deben comenzar por el carácter @, es decir, el nombre de una variable debe comenzar por @. Para declarar variables en Transact SQL debemos utilizar la palabra clave declare, seguido del identificador y tipo de datos de la variable [33].

2.7.3. Palabras Clave Reservadas

Microsoft SQL Server utiliza palabras clave reservadas para definir, manipular y tener acceso a las bases de datos. Las palabras clave reservadas forman parte de la gramática del lenguaje Transact-SQL que utiliza SQL Server para analizar y comprender las instrucciones y lotes de Transact-SQL. Aunque resulta sintácticamente posible usar palabras clave reservadas de SQL Server como identificador y nombres de objetos en scripts de Transact-SQL, solo se puede hacer usando identificadores delimitados [30].

2.8. Lenguajes de Definición de Datos (DDL)

Abraham Silberschatz (cuarta edición), el lenguaje de definición de datos es un esquema de base de datos se especifica mediante un conjunto de definiciones expresadas mediante un lenguaje especial llamado “lenguaje de definición de datos” (LDD). Por ejemplo, la siguiente instrucción en el lenguaje SQL define la tabla cuenta:

create table cuenta (número-cuenta char(10), saldo integer)

La ejecución de la instrucción LDD anterior crea la tabla cuenta. Además, actualiza un conjunto especial de tablas denominado diccionario de datos o directorio de datos. Un diccionario de datos contiene metadatos, es decir, datos acerca de los datos. El esquema de una tabla es un ejemplo de metadatos. Un sistema de base de datos consulta el diccionario de datos antes de leer o modificar los datos reales. Especificamos el almacenamiento y los métodos de acceso usados por el sistema de bases de datos por un conjunto de instrucciones en un tipo especial de LDD

denominado lenguaje de almacenamiento y definición de datos. Estas instrucciones definen los detalles de implementación de los esquemas de base de datos, que se ocultan usualmente a los usuarios.

2.9. Lenguaje de Manipulación de Datos (DML)

Abraham Silberschatz (cuarta edición), la manipulación de datos es:

• La recuperación de información almacenada en la base de datos.

• La inserción de información nueva en la base de datos.

• El borrado de información de la base de datos.

• La modificación de información almacenada en la base de datos.

Un lenguaje de manipulación de datos (LMD) es un lenguaje que permite a los usuarios acceder o manipular los datos organizados mediante el modelo de datos apropiado. Hay dos tipos básicamente:

• LMDs procedimentales. Requieren que el usuario especifique qué datos se necesitan y cómo obtener esos datos.

• LMDs declarativos (también conocidos como LMDs no procedimentales). Requieren que el usuario especifique qué datos se necesitan sin especificar cómo obtener esos datos. Los LMDs declarativos son más fáciles de aprender y usar que los LMDs procedimentales. Sin embargo, como el usuario no especifica cómo conseguir los datos, el sistema de bases de datos tiene que determinar un medio eficiente de acceder a los datos. El componente LMD del lenguaje SQL es no procedimental.

Una consulta es una instrucción de solicitud para recuperar información. La parte de un LMD que implica recuperación de información se llama lenguaje de consultas. Aunque técnicamente sea incorrecto, en la práctica se usan los términos lenguaje de consultas y lenguaje de manipulación de datos como sinónimos.

2.10. Conceptos Redundancia de datos

La redundancia de datos consiste en el almacenamiento de información idéntica en múltiples archivos. Los mismos datos han sido registrados para más de una aplicación. Almacenar y mantener los mismos datos en 2 archivos en vez de uno, es más costoso ya que requiere doble espacio de almacenamiento y doble cantidad de trabajo. Esto puede llevar a inconsistencia de los datos, es decir, las diversas copias de los mismos datos no concuerdan entre sí. Ejemplo: Registro de Cuentas de Ahorro y de Cuentas Corrientes, información de dirección, teléfono, etc.

Puesto que los archivos que mantienen almacenada la información son creados por diferentes tipos de programas de aplicación existe la posibilidad de que si no se controla detalladamente el almacenamiento, se pueda originar un duplicado de información, es decir que la misma información sea más de una vez en un dispositivo de almacenamiento (Redundancia). Esto aumenta los costos de almacenamiento y acceso a los datos, además de que puede originar la inconsistencia de los datos es decir diversas copias de un mismo dato no concuerdan entre sí, por ejemplo: que se actualiza la dirección de un cliente en un archivo y que en otros archivos permanezca la anterior.

Según las mejores prácticas para la gestión de servicios de TI, señaladas por ITIL (Biblioteca de Infraestructura de Tecnología de la Información), Señala (van Bon, j. 2008) redundancia es una forma de aumentar la disponibilidad y sostenibilidad de sistemas. En un sistema informático existen muchos componentes necesarios para que este funcione, cuantos más componentes se tengan más será la probabilidad de que ocurra un fallo. El grado de redundancia de un sistema dependerá de su importancia y del dinero que puede perderse cuando el sistema no esté disponible debido a un fallo. ITIL define los siguientes tipos de redundancia:

Redundancia activa: Se utiliza para reforzar servicios esenciales que no pueden ser interrumpidos bajo ningún concepto. Con este tipo de redundancia, todas las unidades redundantes están simultáneamente en operación (p. ej. Discos replicados en un servidor).

Redundancia pasiva: Consiste en el uso de activos redundantes que no están operativos hasta que se produce algún fallo (p. ej. Clústeres de sistema).

Redundancia heterogénea: Redundancia con distintos tipos de activos del servicio con capacidades comunes. Se utiliza cuando un fallo se debe a una causa difícil de predecir (p. ej. Uso de distintos medios de almacenamiento, lenguajes de programación o equipos de desarrollo).

Redundancia homogénea: Consiste en el uso de capacidad extra del mismo tipo de activos del servicio. Se utiliza cuando la causa del fallo se conoce con certeza (p. ej. Uso de procesadores idénticos) [39].

Tabla 2.3 Redundancia de Servicio Fuente: Wikipedia

2.11. Definición de Disponibilidad de datos

La Disponibilidad [29] es la cualidad de un sistema para mantenerse operativo principalmente ante contingencias "Cada solicitud (request) eventualmente recibe una respuesta". La Alta Disponibilidad (HA) desde la visión de (Eric Brewer) implica mantener el servicio funcionando ante:

- Caídas y Fallas de discos
- Actualizaciones de Bases de datos
- Actualizaciones de Software
- Actualizaciones de Sistema Operativo
- Cortes de energía
- Cortes en la red
- Movimiento físico del equipo

2.11.1. Transacciones SQL y en bases de datos locales

Para que el sistema de gestión de base de datos reconozca una transacción tenemos que marcar sus límites: cuándo comienza y cuándo termina, además de cómo termina.

Todos los sistemas SQL ofrecen las siguientes instrucciones para marcar el principio y el fin de una transacción:

start transaction commit work rollback work

La primera instrucción señala el principio de una transacción, mientras que las dos últimas marcan el fin de la transacción. La instrucción commit work señala un final exitoso: los cambios se graban definitivamente; rollback work indica la intención del usuario de deshacer todos los cambios realizados desde la llamada a start transaction. Solamente puede activarse una transacción por base de datos en cada sesión. Dos usuarios diferentes, sin embargo, pueden tener concurrentemente transacciones activas.

La implementación de transacciones para tablas locales (dBase y Paradox) es responsabilidad del BDE. Las versiones de 16 bits del BDE no ofrecen esta posibilidad. A partir de la versión 3.0 del BDE que apareció con Delphi 2, se soportan las llamadas transacciones locales. Esta implementación es bastante limitada, pues no permite deshacer operaciones del lenguaje DDL (create table, o drop table, por ejemplo), y la independencia entre transacciones es bastante pobre, como veremos más adelante al estudiar los niveles de aislamiento. Tampoco pueden activarse transacciones sobre tablas de Paradox que no tengan definida una clave primaria. Y hay que tener en cuenta la posibilidad de que al cerrar una tabla no se puedan deshacer posterior-mente los cambios realizados en la misma, aunque aún no se haya confirmado la transacción.

Otra limitación importante tiene que ver con el hecho de que las transacciones sobre bases de datos de escritorio utilizan bloqueos. Paradox solamente admite hasta 255 bloqueos simultáneos sobre una tabla, y dBase es aún más restrictivo, pues sólo permite 100. Por lo tanto, estos son respectivamente los números máximos de registros que pueden ser modificados en una transacción de Paradox y dBase [29].

2.12. Definición de Seguridad en SQL

Según James R. Groff [24] la implementación de un esquema de seguridad y hacer que se cumplan las restricciones de seguridad son responsabilidades del software SGBD. El lenguaje SQL define un marco general para la seguridad de la base de datos, y las instrucciones SQL se utilizan para especificar las restricciones de seguridad. El esquema de seguridad SQL se basa en tres conceptos fundamentales.

Microsoft Señala que SQL Server incluye muchas características que admiten la creación de aplicaciones de base de datos seguras.

Las consideraciones comunes de seguridad, como el robo de datos o el vandalismo, se aplican independientemente de la versión de SQL Server que se use. La integridad de los datos también se debe considerar como un problema de seguridad. Si los datos no están protegidos, es posible que acaben perdiendo su valor si se permite la manipulación de datos y los datos se modifican sin intención o de forma malintencionada con valores incorrectos o bien se eliminan por completo. Además, a menudo existen requisitos legales que se deben cumplir, como el almacenamiento correcto de información confidencial. El almacenamiento de determinados tipos de

datos personales está totalmente prohibido, en función de las leyes que se apliquen en una jurisdicción determinada.

Cada versión de SQL Server incluye diferentes características de seguridad, del mismo modo que las versiones de Windows más recientes mejoran la funcionalidad respecto a las anteriores. Es importante comprender que las características de seguridad no pueden garantizar por sí solas una aplicación de base de datos segura. Cada aplicación de base de datos es única en lo que respecta a los requisitos, el entorno de ejecución, el modelo de implementación, la ubicación física y el rellenado por parte del usuario. Algunas aplicaciones que son locales en cuanto al ámbito pueden necesitar una seguridad mínima, en tanto que otras aplicaciones locales o las aplicaciones implementadas en Internet pueden precisar medidas estrictas de seguridad y supervisión y evaluación continuas.

Los requisitos de seguridad de una aplicación de base de datos de SQL Server se deben tener en cuenta en el tiempo de diseño, no a posteriori. La evaluación de las amenazas en las primeras fases del ciclo de desarrollo permite reducir al mínimo los posibles daños cuando se detecte una vulnerabilidad.

Tabla 2.4 Seguridad en SQL Fuente: Google

2.13. Versiones de SQL Server

Versión	Año
1.0	1989
1.1	1991
4.2	1992
4.21	1994
6.0	1995
6.5	1996
7.0	1998
2000	2000
2005	2005
2008	2008
2008 R2	2010
2012	2012
2014	2014

Tabla 2.1 Versiones de SQL Server Fuente: Autor

2.14. Desencadenadores

Según Dante Cantone [8] Los desencadenadores representan aplicaciones que desarrollamos en lenguaje T-SQL y que se ejecutan, o mejor dicho, se "disparan" cuando sucede algún tipo de evento en una tabla. Los desencadenadores se llaman también disparadores o triggers.

En función del tipo de evento, tenemos los siguientes grupos de desencadenadores:

• Desencadenadores de inserción. Estos desencadenadores se ejecutan cuando se añade un registro o varios.

• Desencadenadores de actualización. Se ejecutan cuando se ha actualizado uno o varios registros.

• Desencadenadores de eliminación.

Con estos desencadenadores aseguramos la lógica de negocio y definimos la integridad de OPERADOR. Antiguamente (versiones anteriores a SQL Server 2000), la integridad referencial en cascada tenía que implementarse mediante desencadenadores que permitiesen la actualización y eliminación en cascada.

2.15. Definición de Clúster

El término cluster se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora. Hoy en día desempeñan un papel importante en la solución de problemas de las ciencias, las ingenierías y del comercio moderno. La tecnología de clusters ha evolucionado en apoyo de actividades que van desde aplicaciones de supercómputo y software de misiones críticas, servidores web y comercio electrónico, hasta bases de datos de alto rendimiento, entre otros usos.

El cómputo con clusters surge como resultado de la convergencia de varias tendencias actuales que incluyen la disponibilidad de microprocesadores económicos de alto rendimiento y redes de alta velocidad, el desarrollo de herramientas de software para cómputo distribuido de alto rendimiento, así como la creciente necesidad de potencia computacional para aplicaciones que la requieran. Simplemente, un cluster es un grupo de múltiples ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador, más potente que los comunes de escritorio. Los clusters son usualmente empleados para mejorar el rendimiento y/o la disponibilidad por encima de la que es provista por un solo computador típicamente siendo más económico que computadores individuales de rapidez y disponibilidad comparables [22].

De un clúster se espera que presente combinaciones de los siguientes servicios:

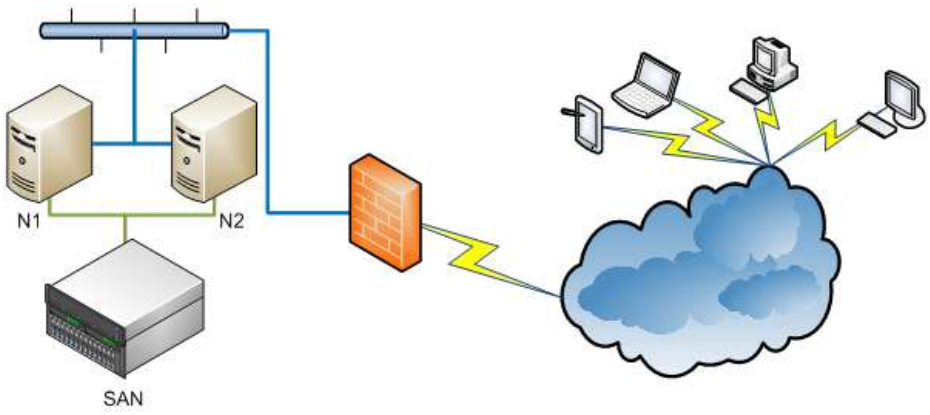

Figura 2.6 Cluster Informáticos Fuente: Autor

1. Alto rendimiento
2. Alta disponibilidad
3. Balanceo de carga
4. Escalabilidad

2.15.1 Alto rendimiento

Un cluster de alto rendimiento: es un conjunto de ordenadores que está diseñado para dar altas prestaciones en cuanto a capacidad de cálculo. Los motivos para utilizar un clúster de alto rendimiento son:

- el tamaño del problema por resolver
- el precio de la máquina necesaria para resolverlo.

Por medio de un cluster se pueden conseguir capacidades de cálculo superiores a las de un ordenador más caro que el costo conjunto de los ordenadores del cluster. Ejemplo de clusters baratísimos son los que se están realizando en algunas universidades con computadoras personales desechados por "anticuados" que consiguen competir en capacidad de cálculo con superordenadores carísimos.

Para garantizar esta capacidad de cálculo, los problemas necesitan ser paralelizables, ya que el método con el que los clusters agilizan el procesamiento es dividir el problema en problemas más pequeños y calcularlos en los nodos, por lo tanto, si el problema no cumple con esta característica, no puede utilizarse el cluster para su cálculo [11].

2.15.2 Alta disponibilidad

Un clúster de alta disponibilidad: es un conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí.

Alta disponibilidad de infraestructura: Si se produce un fallo de hardware en alguna de las máquinas del clúster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios en cualquiera de las otras máquinas del cluster (failover). Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original (failback). Esta capacidad de recuperación automática de servicios nos garantiza la alta disponibilidad de los servicios ofrecidos por el cluster, minimizando así la percepción del fallo por parte de los usuarios.

2.15.3 Balanceo

El balance o balanceo de carga es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles [3].

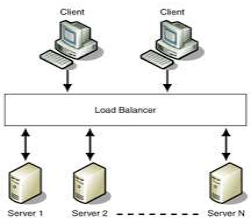

Figura 2.7 Balanceo de Carga Fuente: Google

2.15.4 Escalabilidad

En telecomunicaciones y en ingeniería informática, la escalabilidad es la propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

En general, también se podría definir como la capacidad del sistema informático de cambiar su tamaño o configuración para adaptarse a las circunstancias cambiantes. Por ejemplo, una Universidad que establece una red de usuarios por Internet para un edificio de docentes y no solamente quiere que su sistema informático tenga capacidad para acoger a los actuales clientes que son todos profesores, sino también a los clientes que pueda tener en el futuro dado que hay profesores visitantes que requieren de la red por algunos aplicativos académicos, para esto es necesario implementar soluciones que permitan el crecimiento de la red sin que la posibilidad de su uso y re-uso, disminuya o que pueda cambiar su configuración si es necesario.

2.16. Concepto de Tolerancia a fallos (Failover)

En informática, el concepto de tolerancia a fallos (en inglés: failover) hace referencia a la capacidad de un sistema de acceder a la información, aun en caso de producirse algún fallo o anomalía en el sistema.

Una posibilidad es que el fallo se deba a daños físicos en uno o más componentes de hardware, con la consiguiente pérdida de la información almacenada. La

implementación de la tolerancia a fallos requiere que el sistema de almacenamiento guarde la misma información en más de un soporte físico (redundancia), o en un equipo o dispositivo externo a modo de respaldo. De esta forma, si se produce alguna falla que pueda ocasionar pérdida de datos, el sistema debe ser capaz de restablecer toda la información, recuperando los datos necesarios a partir de algún medio de respaldo disponible [6].

Por lo general, el concepto de tolerancia a fallos se identifica con el sistema de almacenamiento en RAID (Redundant Array of Independent Disks). Los sistemas RAID (a excepción de RAID 0) se basan en la técnica mirroring («en espejo»), que permite la escritura simultánea de los datos en más de un disco del array.

Los sistemas de almacenamiento con tolerancia a fallos son vitales en ambientes donde se trabaje con información crítica, como en el caso de las entidades financieras, gobiernos, corporaciones, etc. El nivel de tolerancia a fallos dependerá de la técnica de almacenamiento utilizada y de la cantidad de veces que la información se encuentre replicada. No obstante, la tolerancia frente a errores nunca es absoluta, puesto que si fallasen todas las réplicas (mirrors) disponibles, incluyendo la copia original, la información quedaría incompleta y corrupta, y lo que es peor: irrecuperable.

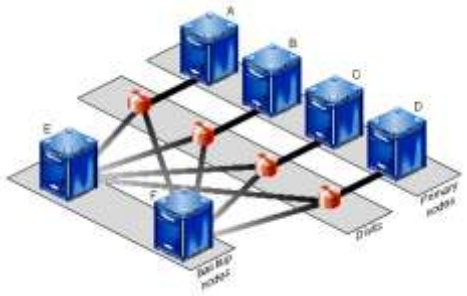

Tabla 2.8 Failover Fuente: Google

2.17. Definición de Espejo (Mirror)

En Internet, un espejo, (del inglés, mirror), es un sitio web que contiene una réplica exacta de otro. Estas réplicas u espejos se suelen crear para facilitar descargas grandes y facilitar el acceso a la información aun cuando haya fallos en el servicio del servidor principal.

Los espejos suelen sincronizarse periódicamente con el servidor principal para mantener la integridad de la información.

Es un concepto muy utilizado en foros cibernéticos donde los usuarios de estos comparten archivos entre sí, ya que en ocasiones algunos de estos no pueden ser descargados adecuadamente, por lo que se informa sobre un espejo para obtenerlo.

En el caso de las redes, «espejo» (o mirror) también hace referencia al modo en el que trabaja un switch, al hacer réplica de todos los paquetes que este conmuta direccionados a un solo puerto a través del cual, con un analizador de tráfico, se puede observar todo el tráfico de la red [11].

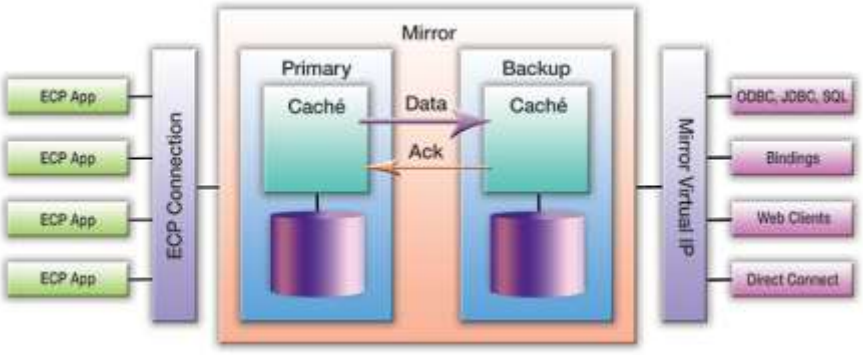

Figura 2.9 Sistema Mirror (Espejo) Fuente: Wikipedia

2.18. Definición de Replicación de Datos

La replicación de datos es mucho más que la simple copia de datos entre varias localidades. Ha sido utilizada, tradicionalmente, como el mecanismo básico para incrementar la disponibilidad y el performance de una BD.

La replicación debería estar acompañada del análisis, diseño, implementación, administración y monitoreo de un servicio que garantice la consistencia de los datos a lo largo de múltiples administradores de recursos en ambientes distribuidos. Por este motivo, un servicio de replicación de datos debería proveer las siguientes funcionalidades:

•Ser escalable. Con respecto a la replicación, la escalabilidad significa la habilidad de replicar volúmenes de datos pequeños o grandes a lo largo de recursos heterogéneos (hardware, redes, sistemas operativos) [29].

•Proveer transformación de datos y mapeo de servicios. Estos servicios permiten que los esquemas de datos diferentes coexistan sin perder su semántica esencial. Por ejemplo, las copias pueden ser idénticas o semánticamente equivalentes. Las copias idénticas podrían tener la misma plataforma, el mismo contenido de información y el mismo tipo de datos, en tanto que copias semánticamente equivalentes podrían tener el mismo contenido de información pero diferentes plataformas y, posiblemente, diferentes tipos de datos.

•Soportar replicación en modo sincrónico (tiempo real) o asincrónico.

•Proveerse un mecanismo que describa los datos y objetos que se van a replicar (diccionario de datos).

•Proveerse un mecanismo para inicializar un nodo, esto es para indicar la recepción de datos replicados.

•Soportar administración end-to-end de seguridad y calidad de servicios. Por ejemplo, el servicio debe garantizar que no puede ocurrir corrupción en los datos durante la proceso de replicación. En otras palabras, los datos pueden cambiar de formato pero no de contenido.

•Proveerse un mecanismo de bitácora que administre cualquier esfuerzo de replicación fallado.

•Proveer un mecanismo de recuperación automático.

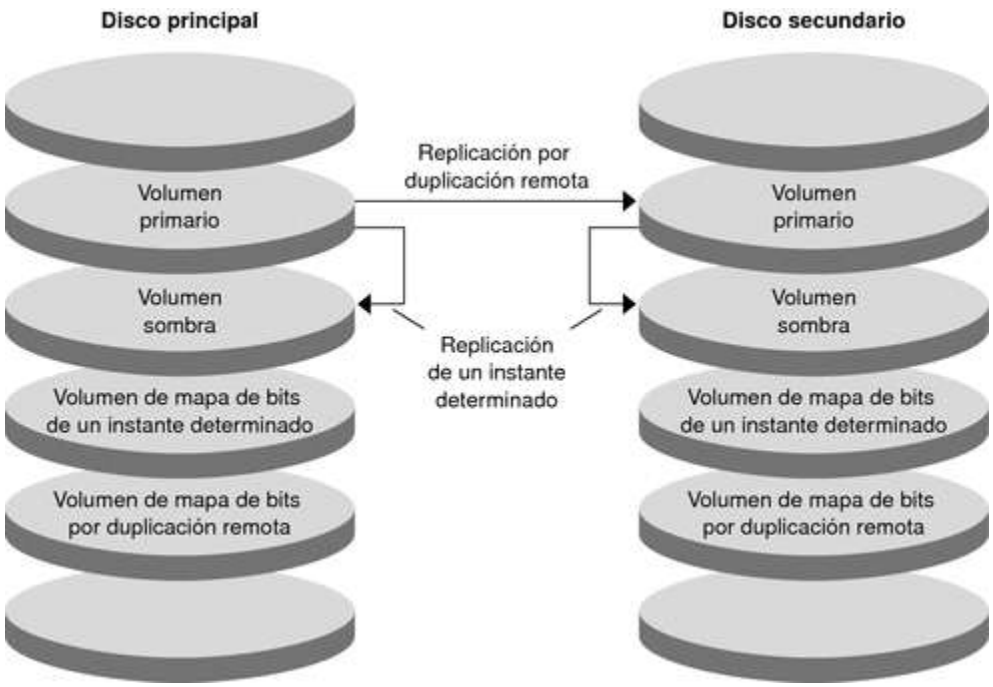

Figura 2.10 Replicación de Datos Fuente: Wikipedia

2.19. Concepto de Balance de carga

El balance o balanceo de carga es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.

El balance de carga se mantiene gracias a un algoritmo que divide de la manera más equitativa posible el trabajo, para evitar los así denominados cuellos de botella [23].

2.20. Almacenamiento SAN (Storage Area Network)

Una SAN (Storage Area Network) es una red de área de almacenamiento, es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman. Una SAN proporciona almacenamiento (discos duros) en fibra a los distintos servidores de la organización, tanto servidores con sistemas operativos Windows como GNU Linux [5].

Figura 2.11 SAN Fuente: Google

Figura 2.12 Esquema SAN Simple Fuente: Wikipedia

2.21. Arreglos (RAID)

En informática, el acrónimo RAID (del inglés Redundant Array of Independent Disks), traducido como «conjunto redundante de discos independientes», hace referencia a un sistema de almacenamiento de datos que usa múltiples unidades de almacenamiento de datos (discos duros o SSD) entre los que se distribuyen o replican los datos. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor throughput (rendimiento) y mayor capacidad. En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto [30].

Figura 2.13 RAID Fuente: Google

En el nivel más simple, un RAID combina varios discos duros en una sola unidad lógica. Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAIDs suelen usarse en servidores y normalmente (aunque no es necesario) se implementan con unidades de disco de la misma capacidad. Debido al descenso en el precio de los discos duros y la mayor disponibilidad de las opciones RAID incluidas en los chipsets de las placas base, los RAIDs se encuentran también como opción en las computadoras personales más avanzadas. Esto es especialmente frecuente en las computadoras dedicadas a tareas intensivas y que requiera asegurar la integridad de los datos en caso de fallo del sistema. Esta característica no está obviamente disponible en los sistemas RAID por software, que suelen presentar por tanto el problema de reconstruir el conjunto de discos cuando el sistema es reiniciado tras un fallo para asegurar la integridad de los datos. Por el contrario, los sistemas basados en software son mucho más flexibles (permitiendo, por ejemplo, construir RAID de particiones en lugar de discos completos y agrupar en un mismo RAID discos conectados en varias controladoras) y los basados en hardware añaden un punto de fallo más al sistema (la controladora RAID).

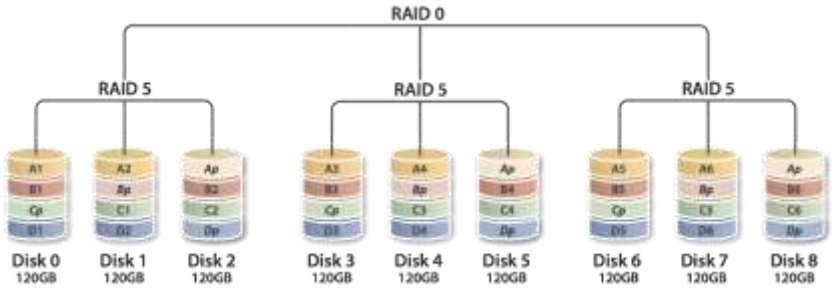

Figura 2.14 Esquema de RAID Fuente: Wikipedia

Capítulo 3
Seguridad de Red y Servidores

3.1. Concepto de seguridad

Aguilera López [1] En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

3.2. Ataques de negación de servicios. (Denial of Service Attacks)

Los ataques de negación de servicio o Denial of Service Attacks (DoS) son ataques que le impiden a un sistema de tratamiento responder a solicitudes legítimas de tráfico o solicitudes de recursos y objetos. La forma más común de estos ataques se da cuando se están transmitiendo muchos paquetes de datos a un servidor, el cual no puede procesarlos todos a la vez. Otras formas de negación de los ataques de servicios se centran en la explotación de un conocido fallo o vulnerabilidad en un sistema operativo, servicio o aplicación. La explotación de la falla a menudo resulta en la caída del sistema o el 100 por ciento de uso de CPU [32].

No importa en qué consista un ataque actual, cualquier ataque que hace que su víctima no pueda realizar las actividades normales puede considerarse como un ataque de negación de servicios. Los ataques de negación de servicio pueden resultar de accidentes en el sistema, reinicios del sistema, corrupción de datos, bloqueo de los servicios, y más.

Una forma de prevenir estos ataques, seria aumentando el número de conexiones que un servidor pueda soportar. Sin embargo, esto generalmente requiere recursos de hardware adicionales (memoria, CPU, y así sucesivamente) y puede no ser posible para todos los sistemas operativos o de red soportar dicho aumento [2].

3.3. Principales Elementos y Equipos de Protección

3.3.1. Concepto de Hub

Los Hubs tienen varios puertos físicos utilizados para proporcionar conectividad básica a varios equipos. Hubs suelen tener entre cuatro y treinta y dos puertos físicos. En una red Ethernet, el centro tendría puertos utilizados para conectar a NIC en las computadoras host utilizando un cable de par trenzado múltiple RJ-45. La mayoría de los centros están activos, lo que significa que tienen el poder y amplificarán la salida a un nivel establecido [36].

Los hubs no tienen inteligencia. Lo que va en un puerto sale a todos los puertos en el concentrador. Esto presenta un riesgo de seguridad, ya que si un atacante instala un analizador de protocolos (sniffer) en cualquier computadora conectada al hub, el sniffer capturará todo el tráfico que pasa a través del hub. Como se mencionó anteriormente, cualquier tráfico enviado a través del cable en texto claro está sujeto a oler ataques con un analizador de protocolos. Una forma de proteger contra esto es mediante la encriptación de los datos. Otra forma de proteger contra los ataques de sniffer es reemplazar todos los hubs con switches para limitar la cantidad de tráfico que llega a cualquier ordenador. Muchas empresas restringen específicamente el uso de concentradores en sus redes para reducir el riesgo de rastreadores de captura de tráfico [2].

3.3.2. Definición de Switch

Los switch tiene la capacidad de aprender qué equipos están unidos a cada uno de sus puertos físicos. El mismo utiliza este conocimiento para crear conexiones conmutadas internas cuando dos computadoras se comunican entre sí.

- La comparación de Puertos Físico y Puertos Lógicos

Hay que tener en cuenta que un puerto físico utilizado por un switch es completamente diferente de los puertos lógicos discutidos previamente. Se conecta cables a un puerto físico. El puerto lógico es un número incrustado en un paquete e identifica los servicios y protocolos.

Figura 3.1 Switch Fuente: Consentry

3.3.3. Definición de Routers

Los routers conectan varios segmentos de red juntos en una sola red y enrutan el tráfico entre los segmentos. Como ejemplo, la Internet es efectivamente una sola red de alojamiento miles de millones de ordenadores. Los routers rutean el tráfico de un segmento a otro.

Dado que los routers no pasan transmisiones, reducen eficazmente el tráfico en cualquier segmento individual. Los segmentos separados por routers se refieren a veces como dominios de difusión. Si una red tiene demasiados equipos en un solo segmento, las emisiones pueden dar lugar a colisiones excesivas y reducir el rendimiento de la red.

Mover equipos a un segmento diferente separados por un router puede mejorar significativamente el rendimiento general. Los routers de Cisco son muy populares, pero existen muchas otras marcas. La mayoría de los routers son dispositivos físicos, y los routers físicos son los más eficientes. Sin embargo, también es posible añadir enrutamiento software en equipos con más de una NIC. Por ejemplo, los productos de servidor de Windows (como Windows Server 2008 y 2008 R2) pueden funcionar como routers añadiendo servicios adicionales [4].

Figura 3.2 Router Fuente: Cisco

3.4. Concepto de Firewall

Según Vieites, A. G. [40] el cortafuego o firewall filtran el tráfico entre las redes y puede filtrar tanto tráfico de entrada como de salida. En otras palabras, un firewall puede asegurar que sólo determinados tipos de tráfico están permitidos en su red y se les permite salir de su red sólo a determinados tipos de tráfico. El propósito de un firewall es similar a un servidor de seguridad en un coche. El servidor de seguridad en un coche se encuentra entre el motor y el habitáculo. Si se inicia un incendio en el compartimiento del motor, el servidor de seguridad proporcionará una capa de protección de los pasajeros en la cabina de pasajeros. Del mismo modo, un firewall en una red intentará mantener el mal tráfico (a menudo en forma de atacantes) fuera de la red. Por supuesto, un motor tiene una gran cantidad de piezas móviles que pueden hacer daño a nosotros si llegamos accidentalmente en él mientras se está ejecutando. El servidor de seguridad en un coche protege a los pasajeros de tocar cualquiera de las partes en movimiento. Del mismo modo, una red también puede impedir que los usuarios accedan a lugares que un administrador considere peligroso. Por ejemplo, los usuarios sin educación podrían descargar inadvertidamente archivos dañinos, pero muchos firewalls pueden bloquear descargas potencialmente maliciosas. Los firewalls comienzan con una capacidad de enrutamiento básico para el filtrado de paquetes. Por otra parte los firewalls más avanzados van más allá de filtrado de paquetes simples e incluyen el filtrado de contenido proporcionado por muchos Gateway de seguridad web y electrodomésticos. Un firewall puede ser basado en host o basada en la red.

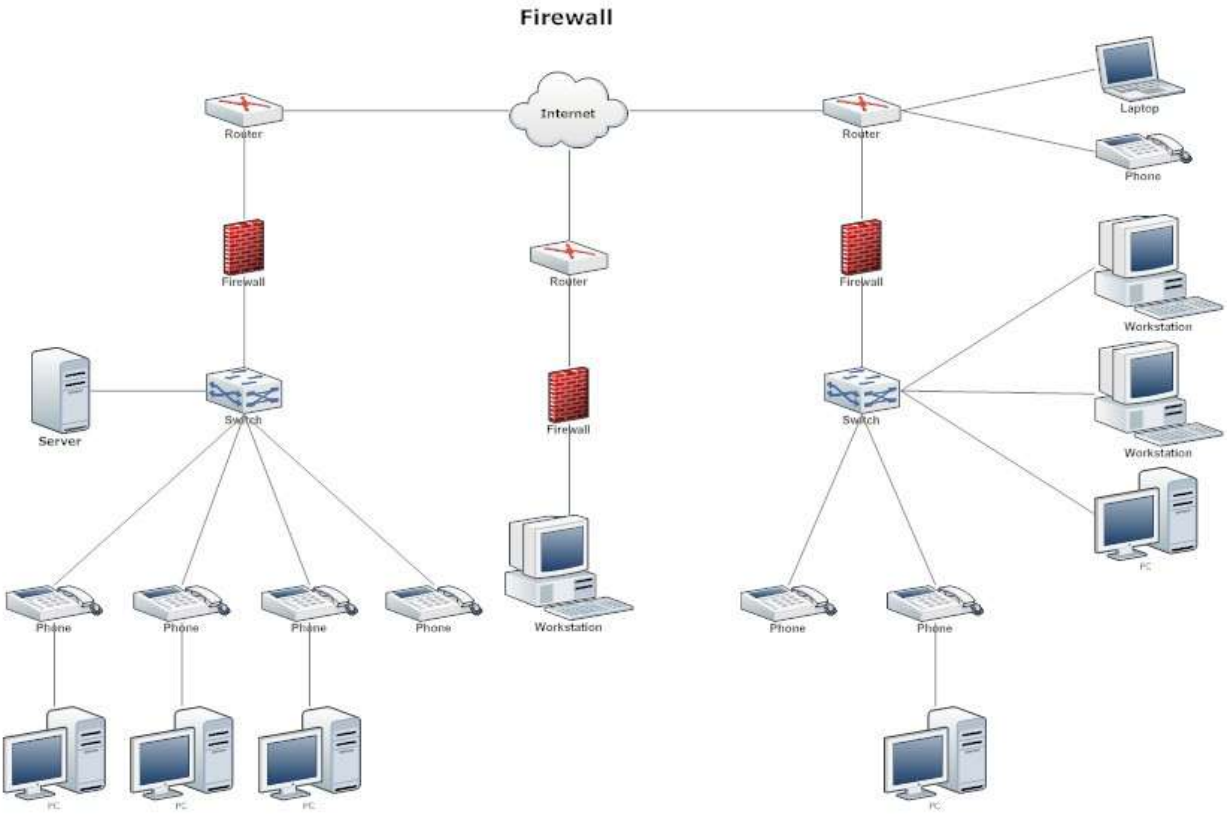

Figura 3.3 Ejemplo Esquema Firewall Fuente: Autor

3.5. Sistema de detención de intruso (IDS)

Emmett Dulaney, M. J. [12] Sistemas de detección de intrusiones (IDS) ayudan a detectar ataques a los sistemas y redes. Los sistemas de prevención de intrusiones (IPS) detienen los ataques en curso detectando y bloqueando ataques a los sistemas y redes. Mientras que algunos IDS activos, también puede tomar medidas para bloquear los ataques, no todos los IDS son activos.

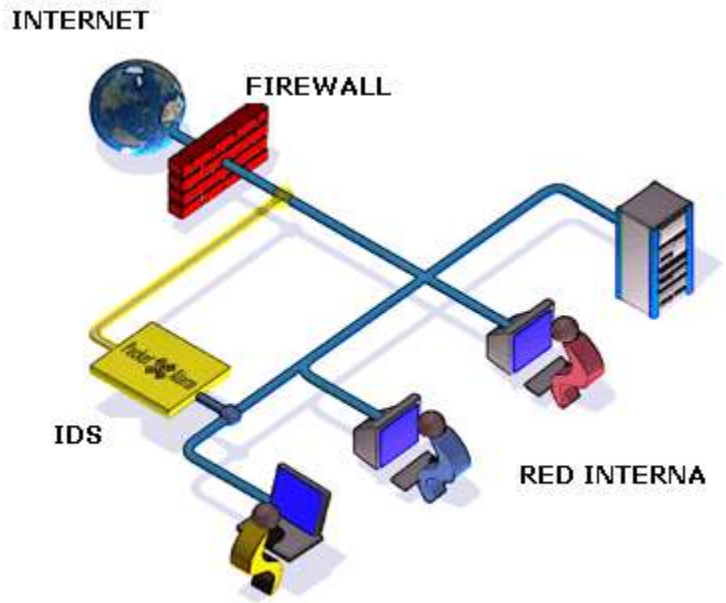

Figura 3.4 IDS Fuente: Google

3.5.1. IDS Pasivos

Los IDS pasivos registrarán el ataque y también pueden generar una alerta para notificar a alguien. La mayoría de los IDS son pasivos por defecto. La notificación puede venir en muchas formas, incluyendo:

- Una ventana pop-up. Un cuadro de diálogo puede aparecer y notificar al usuario del evento.
- Un monitor central. Algunas organizaciones grandes utilizan monitores centrales para mostrar los eventos de interés.
- Un e-mail. El IDS puede enviar un e-mail a un usuario o grupo. Muchos sistemas de correo electrónico pueden transmitir a dispositivos portátiles, tales como los dispositivos Smartphone o tabletas.
- Un mensaje de página o texto. Muchos servidores de correo electrónico pueden aceptar e-mail y enviarlos a un sistema de teléfono para enviar un mensaje de página o texto.

3.5.2. IDS Activos

Un IDS activo registrará y notificará al personal de la misma manera que un IDS pasivo, además también pueden cambiar el entorno para impedir o bloquear el ataque. Los IDS activos pueden:

- Modificar ACL (Lista de Control de Acceso) en servidores de seguridad para bloquear el tráfico ofensivo.

- Cerrar los procesos en un sistema que fueron causadas por el ataque.

- Desviar el ataque a un ambiente seguro.

- Considere el ataque de inundación SYN, donde un ataque inunda un sistema con paquetes SYN, pero nunca completa el enlace de tres vías de TCP con el paquete ACK.
- El ataque es a menudo proviene de una dirección IP específica. El IDS puede modificar las listas de control de acceso en un router o firewall para bloquear todo el tráfico desde esta dirección IP. Las sesiones TCP atacante iniciado consumen recursos en el servidor hasta que se cierran. Los IDS activos pueden cerrar todas estas sesiones para liberar recursos.
- También es posible desviar el ataque a un honeypot o red trampa.

3.6. Sistema de detención de intruso en la red (NIDS)

Un sistema de detección de intrusiones basado en red (NIDS) monitorea la actividad en la red. Un administrador instala sensores NIDS en dispositivos de red tales como routers y firewalls. Estos sensores recogen información y el informe a un servidor central de monitoreo anfitrión de una consola de NIDS.

Un NIDS no es capaz de detectar anomalías en sistemas individuales o estaciones de trabajo a menos que la anomalía provocara una diferencia significativa en el tráfico de red. Además, un NIDS no es capaz de descifrar el tráfico cifrado. En otras palabras, sólo puede monitorear y evaluar las amenazas en la red del tráfico enviado en texto plano o el tráfico no cifrado [9].

La figura 3.5 muestra un ejemplo de una configuración de NIDS. En la figura, los sensores están situados antes del firewall, después de que el servidor de seguridad, y en los routers. Estos sensores monitorean el tráfico de red en subredes dentro de la red e informar a la consola de NIDS. Si un atacante lanzó un ataque a la red, el NIDS lo detectará.

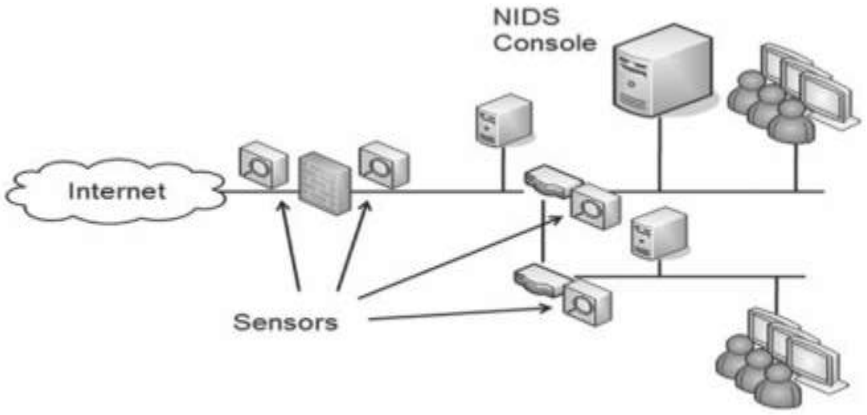

Figura 3.5 sensores NIDS Fuente: Autor

3.7. Sistema de detención de intruso en dispositivos (HIDS)

Un sistema de detección de intrusos basado en host (HIDS) es un software adicional instalado en una estación de trabajo o servidor. Proporciona protección al host individual y puede proteger los archivos críticos del sistema operativo. El objetivo principal de cualquier IDS es para monitorear el tráfico. Para un HIDS, este tráfico pasa a través de la tarjeta de interfaz de red (NIC).

Muchos IDS basados en host se han expandido para supervisar la actividad de aplicación en el sistema. Como ejemplo, se puede instalar un HIDS en diferentes servidores expuestos a Internet, como servidores web, servidores de correo y

servidores de bases de datos. Además de monitorear el tráfico de red de gran alcance de los servidores, el HIDS también puede controlar las aplicaciones de servidor [13].

3.8. Manejador de eventos e incidentes de seguridad (SIEM)

Información y administración de eventos de seguridad (SIEM) es un término para los productos de software y servicios que combinan la gestión de información de seguridad (SIM) y la gestión de eventos de seguridad (SEM). Tecnología SIEM ofrece análisis en tiempo real de alertas de seguridad generados por el hardware y las aplicaciones de red. SIEM se vende como software, aparatos o servicios gestionados, y también se utilizan para registrar los datos de seguridad y generar informes para fines de cumplimiento.

Las siglas SEM, SIM y SIEM se han usado a veces segmento intercambiables. El segmento de gestión de la seguridad se ocupa del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola que se conoce comúnmente como la gestión de eventos de seguridad (SEM). La segunda área proporciona almacenamiento a largo plazo, el análisis y la comunicación de los datos de registro y se conoce como gestión de la información de seguridad (SIM). Al igual que con muchos significados y definiciones de las capacidades nuevas necesidades moldear continuamente derivados de SIEM categorías de productos. La necesidad de una voz visibilidad céntrica o vSIEM (información de seguridad de voz y gestión de eventos) es un ejemplo reciente de esta evolución [15].

La gestión de eventos de seguridad de la información (SIEM), acuñado por Mark Nicolett y Amrit Williams de Gartner en 2005, describe las capacidades de los productos de la recolección, análisis y presentación de información de los dispositivos de red y de seguridad; aplicaciones de gestión de identidad y acceso; herramientas de gestión de vulnerabilidades y cumplimiento de políticas; sistema operativo, registros de bases de datos y aplicaciones; y datos de amenazas externas. Un punto clave es monitorear y ayudar a gestionar usuarios y servicios privilegiados, servicios de directorio y otros cambios en la configuración del sistema; así como proporcionar la auditoría de registro y revisión y respuesta a incidentes.

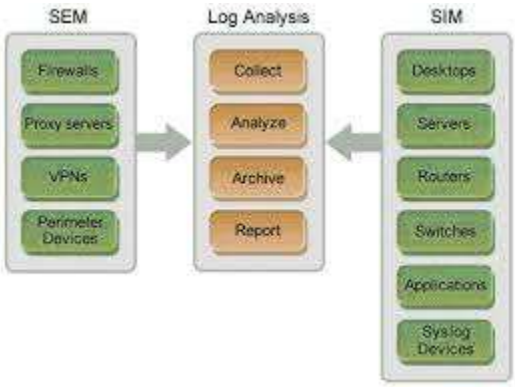

Figura 3.6 Esquema SIEM Fuente: Google

3.9. Seguridad de Puertos

La seguridad de los puertos limita a los ordenadores que se pueden conectar a través de los puertos en un switch. Incluye restringir los dispositivos que se conectan en función de su dirección MAC, y deshabilitar los puertos inactivos. Los Puerto de seguridad incluye la restricción de lo que las computadoras pueden conectarse a cualquier puerto físico basado en la dirección MAC y deshabilitar puertos inactivos.

En una implementación simple de la seguridad portuaria, el interruptor se acuerda de las primeras una o dos direcciones MAC que se conectan al puerto. Cualesquiera otras direcciones MAC asociadas a este puerto se bloquean. Muchos switches también soportan la configuración manual de cada puerto con una dirección MAC específica. Esto limita la conectividad de cada puerto a un dispositivo específico utilizando esta dirección MAC. Esto requiere mucho más trabajo, pero ofrece un mayor nivel de seguridad.

Si no se utilizan los puertos físicos, puede desactivarse en el interruptor para apoyar la seguridad del puerto base. Esto evita que alguien pueda conectar un ordenador portátil a un enchufe de pared abierta con un RJ-45, que conecta con el interruptor, y el acceso a su red.

También puede utilizar un servidor IEEE 802.1X para la autenticación basada en el puerto. IEEE 802.1X restringe a los clientes no autorizados que se conecten a la red hasta que se autentican a través del servidor 802.1X [19].

3.10. Concepto de Malware

Los Malware, constituyen los diferentes programas que pueden afectar al computador y que deben ser conocidos por los investigadores al momento de recabar información en un equipo determinado [32].

Figura 3.7 Tipos de Malware Fuente: Google

3.11. Definición de Virus

Los virus informáticos son creados con mala intención y enviados por los atacantes. Un virus se une a pequeños trozos de código de computadora, de software o documentos. El virus se ejecuta cuando el software se ejecuta en un ordenador. Si el virus se propaga a otros equipos, los equipos podrían seguir propagando el virus (David Afinson, 2010).

Un virus se transfiere a otro ordenador a través del correo electrónico, transferencia de archivos y mensajería instantánea. Los virus se esconden uniéndose a un archivo en el ordenador. Cuando se accede al archivo, el virus se ejecuta e infecta el ordenador. Un virus tiene el potencial de dañar o borrar archivos en el equipo, utilizando su dirección de correo electrónico para propagarse a otros equipos o incluso borrar su disco duro.

Algunos virus pueden ser excepcionalmente peligrosos. El tipo más dañino de virus se utiliza para registrar las pulsaciones de teclado. Los atacantes pueden usar estos virus para recoger información sensible, como contraseñas y números de tarjetas de crédito. Los virus pueden incluso alterar o destruir la información en una computadora [34].

3.12. Concepto de Gusanos

Un gusano es un programa de auto replicado que es perjudicial para las redes. Un gusano utiliza la red para duplicar su código en las máquinas de esta, y esto lo hace sin la intervención del usuario. Es diferente de un virus debido a que un gusano no necesita estar adjuntado a un programa para infectar un anfitrión o una computadora destino.

Aunque el gusano no daña los datos o aplicaciones en los ordenadores que infecta, perjudica las redes porque consume ancho de banda de toda la red. David Afinson (2010).

3.13. Ataques de fuerza bruta y de diccionario.

El ataque de Fuerza Bruta es un intento de descubrir las contraseñas de cuentas de usuario intentando sistemáticamente todas las posibles combinaciones de letras, números y símbolos. Con la velocidad de las computadoras modernas y la capacidad de emplear la computación distribuida, los ataques de fuerza bruta tienen éxito incluso en contra de contraseñas seguras. Con el tiempo suficiente, todas las contraseñas pueden ser descubiertas con un ataque de fuerza bruta.

Para prevenir dichos ataques se hace necesario utilizar métodos de prevención, uno recomendable, pero no infalible es utilizar una contraseña con caracteres alfanuméricos y saber que cuanto más larga sea una contraseña más difícil será lograr efectividad a través de un ataque de Fuerza Bruta [35].

3.14. Los despidos de energía

El poder es una utilidad fundamental tener en cuenta en la revisión de cualquier plan de preparación para desastres. Para sistemas muy críticos, puede utilizar fuentes de alimentación ininterrumpida y generadores para proporcionar tolerancia a fallos y alta disponibilidad [38].

3.14.1 UPS

Un sistema de alimentación ininterrumpida (UPS) es una batería o banco de baterías utilizadas como respaldo en caso de falla de energía primaria. El UPS se conecta a la pared y recibe energía de la fuente comercial, como se muestra en la Figura 9.2. El poder comercial mantiene las baterías cargadas y la electrónica dentro del sistema UPS proporciona energía a sistemas externos.

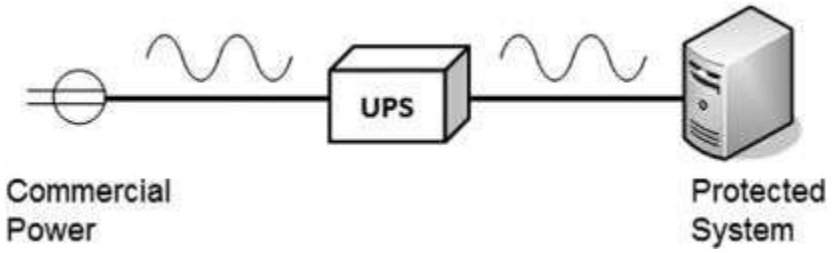

Figura 3.8 UPS Fuente: Wikipedia

Capítulo 4
Propuesta para la Contraloría General de la República

4.1. Situación Actual de la CGRD

En la actualidad esta entidad no posee ningún mecanismo de redundancia de datos lo que puede ocasionar pérdida de información valiosa para la institución. La redundancia de datos se refiere a la réplica de datos e información en uno o varios equipos diferentes al que se encuentra almacenado.

Analizando el problema, se verifica que la mayoría de los servicios informáticos se encuentran centralizados en los diferentes servidores de la institución, si alguno de estos presenta una falla, se vería afectado todo el sistema institucional ya que en estos se alojan todas las informaciones de desembolsos de pagos del estado. Cabe destacar que la antigüedad de estos equipos causa una gran deficiencia ante las exigencias informáticas, impidiendo un buen desempeño a la hora de responder a una necesidad. Además, estos equipos presentan una escasa compatibilidad con nuevas tecnologías que podrían ayudar a aprovechar al máximo el espacio y funcionamiento de los mismos.

Por otra parte, el esquema de red actual no garantiza la continuidad de los servicios y disponibilidad de la información ya que en caso de presentarse una falla en alguno de los puntos, la carencia de enlaces redundantes causaría una pérdida de información impidiendo la recuperación de la misma. Además no existe una política de seguridad de red implementada, lo que presenta un alto riesgo para la institución por los posibles ataques a la información.

4.2. Análisis Foda para la Contraloría

Fortaleza: constamos con el apoyo de la gerencia y el personal humano lo que nos permite el crecimiento de la infraestructura para tener una mejor plataforma para los equipos y la red.

Se consta con un personal capacitado preparado para implementar estos procesos y equipo para la restructuración de la red.

Oportunidades: Entre las oportunidades que tenemos de crecimiento están la adquisición de nuevos equipos de infraestructura y la implementación de nuevas capas de seguridad, también la capacitación del personal para los manejos de los nuevos equipos. La plataforma tecnología permitirá incorporación fácilmente nuevos sistemas.

Se implementara un modelo que colocara a la Contraloría General en una de las instituciones del estado más moderna en infraestructura y seguridad informática.

Debilidades: Que la parte financiera puede ver que la inversión en los nuevos equipos como un gasto y no como una inversión que asegure la fluidez del proceso de negocio.

Que la información esta vulnerable ya que los servicio no consta de tecnología que ofrezcan alta disponibilidad.

Amenazas: que si se presenta alguna falla pueda comprometer la información en nuestros servidores y estar expuesto a ataques cibernéticos por la falta de seguridad, además que esto podría afectar en el engranaje de todo el estado Dominicano.

4.3. Esquema de la Red Actual CGRD

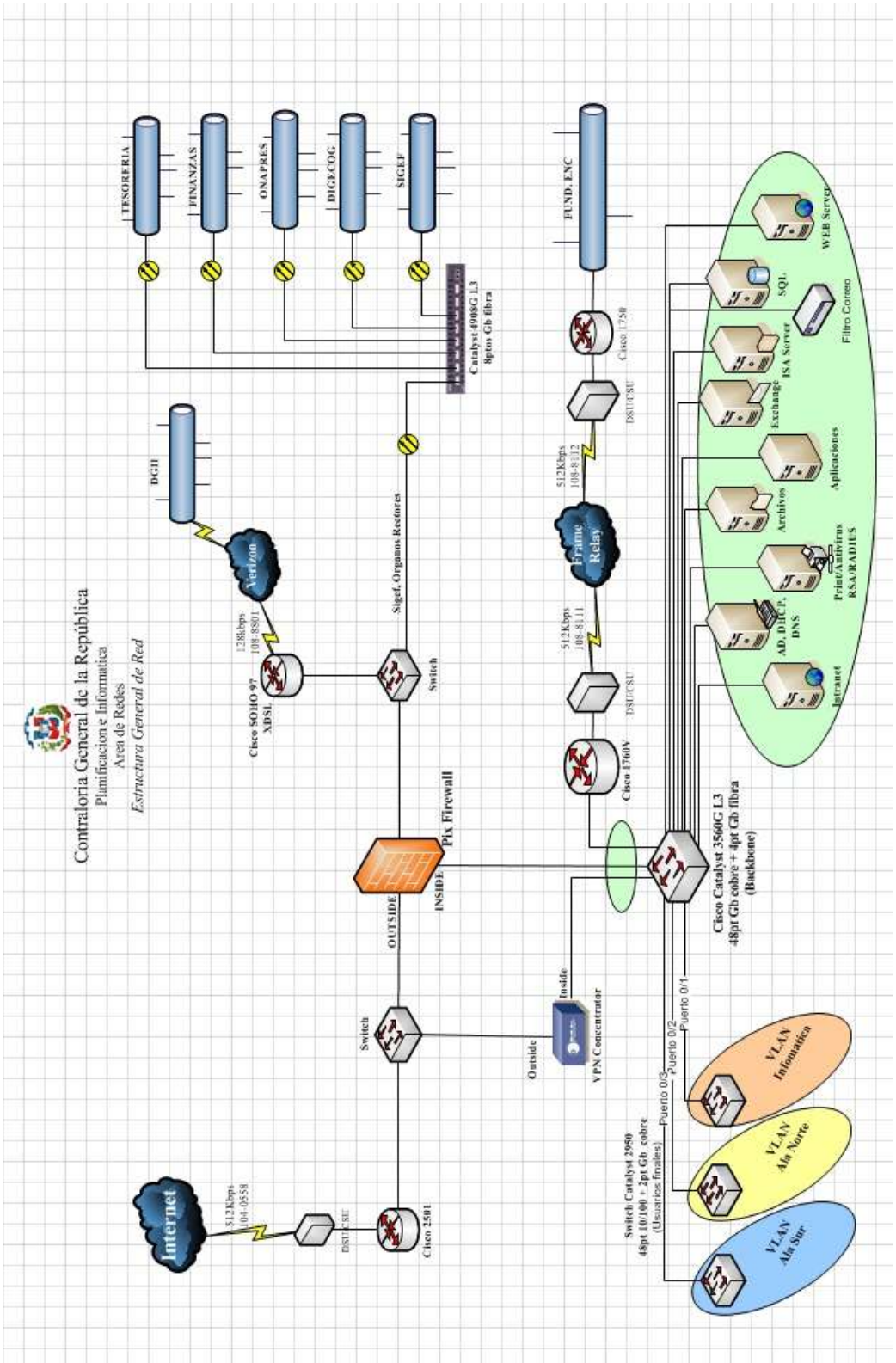

Figura 4.1 Esquema de Red Actual Fuente: Contraloría

4.4. Servidores e Infraestructura de la Contraloría

Entre los servidores que tenemos se encuentra un servidor de archivo, un servidor de dominio, un servidor web para las aplicaciones en las nubes, un servidor de impresión, un servidor de aplicaciones, un servidor SQL y un servidor correo.

En cuanto a la infraestructura de la red tenemos 5 switch en cascada y 2 switch capa 3 dos router cisco 2900 para el manejo de tráfico, un Ips y un concentrador de VPN además de una línea de internet para los servicios de la web.

4.5. Propuesta para la CGRD

Después de analizar el caso de estudio entendiendo que la Contraloría General de la Republica es eje central de todos el engranaje del estados Dominicano entendemos que el mejor esquema de red y de infraestructura es el siguiente, los servicios de (ISP) ósea internet estén redundantes los cuales irán a un switch que estará conectado a dos balanceadores en clúster para manejo de toda carga, proponemos dos firewall y un ISP el ips para el censado de toda la infraestructura y los firewall trabajado como clústeres de alta disponibilidad que irían conectados a dos router que se encargan del manejo de todo el tráfico de la red, además de 10 switch los cuales estarán distribuido de la siguiente manera dos capa 3 trabajando como server 4 switch de distribución y 4 de acceso para albergar todos los host de la institución.

En cuanto los servidores tendremos los servicios virtualizados en cuatro servidores físico que estarán en failover clúster si uno de esto servidores falla las maquinas serán migradas a uno que esté disponible, en cuanto al servidores de base de datos estarán

en (Sql Server) los tendremos en dos servidores físicos en clúster activo - pasivo que si se presenta alguna falla el otro entre de unas vez los cuales aseguran la disponibilidad de los servicios. Constaremos además de dos SAN (store área network) en clúster por lo que recomendamos dos switch fibre channel con conexión gigabit a los servidores físicos y donde se alojara los discos virtuales y la data de la Contraloría.

En cuanto a la electricidad tendremos dos ups redundante para evitar cualquier falla eléctrica, lo cual garantiza la disponibilidad las 24 horas los 7 días de la semana.

Los cambios permiten aislar los problemas que se puedan presentar en la red en el futuro, también reducirá el tiempo para la solución de los mismos, pues ya los usuarios, servidores y demás equipos no quedan al mismo nivel ni en el mismo segmento. La nueva estructura también permite aplicar políticas de control de acceso para los usuarios, de tal forma que es posible restringir el acceso a dispositivos en específicos (P.ej.: servidores o Firewall de Internet). Anteriormente no existía control sobre quienes se conectaban remotamente a la red vía las instituciones externas. Por un lado, las instituciones externas protegían su acceso desde afuera pero no había restricción para conectarse hacia la Contraloría. Con los nuevos cambios, solo las conexiones remotas explícitamente configuradas tendrán permiso para entrar a la red.

4.6. Esquema Propuesto para CGRD

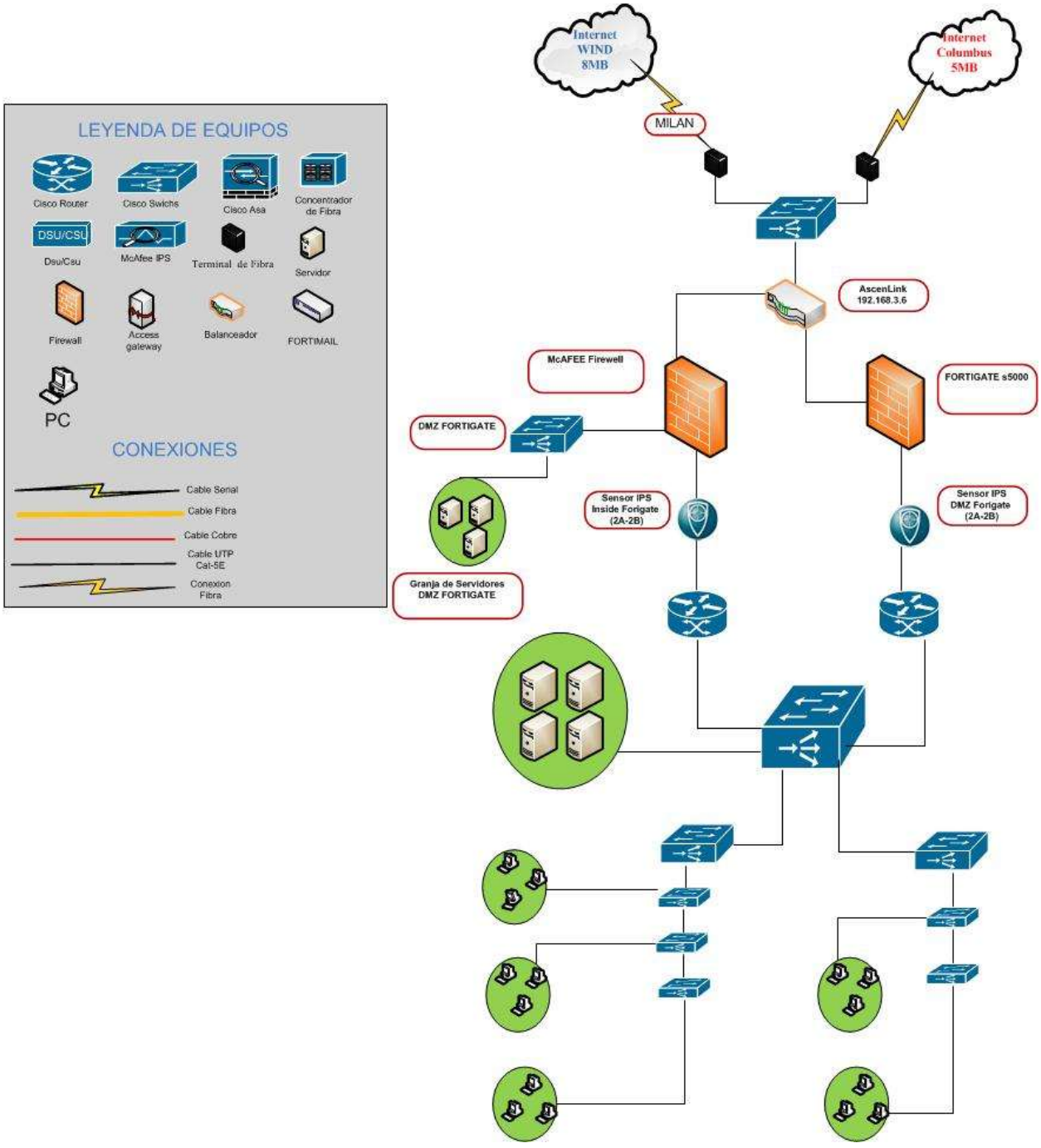

Figura 4.2 Esquema de Red Propuesto Fuente: Autor

Diagrama Alto Nivel Propuesto

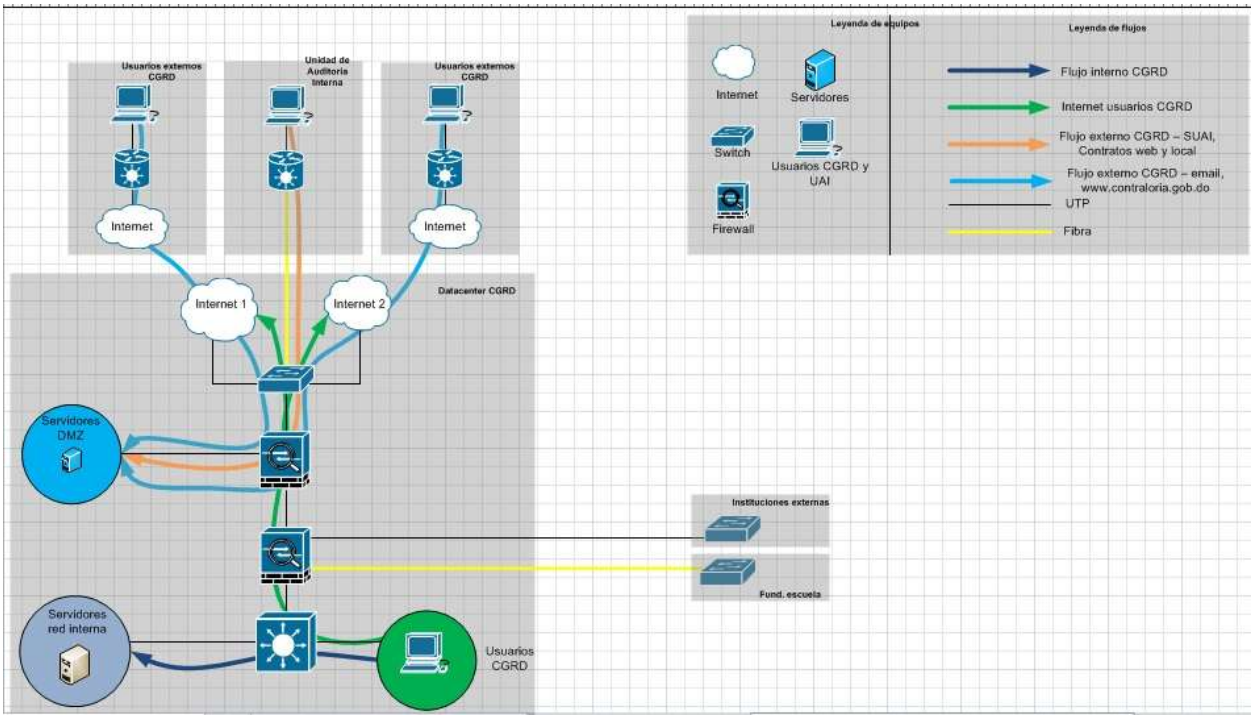

Figura 4.3 Esquema de Alto Nivel Fuente: Autor

4.7. Cotización de los Nuevos Equipo y Presupuesto

• Dos Firewall Marca FortiGate Serie 5000

• Un Router 3800 Cisco

• Dos Consola de almacenamiento SAN (Storage Área Network)

• UPS Uninterrupted Power supply three/3 phase online

• Dos Fibre Channel Switch 24ts Cisco

• Servidor Dell Poweredge 1950

• 4 Cisco Catalyst 2960 48 Power over Ethernet (PoE) Switch

4.8. Presupuesto del proyecto

La mayoría de los equipos utilizados en la implementación del proyecto, se cotizaron en moneda americana (USD), por eso fue necesario utilizar una tasa de referencia para el cambio de monedas, considerando el precio actual del dólar americano en nuestro país, la tasa es 43.80 x 1.

A partir de la cotizaciones de todo lo necesario, Firewall, Switch, Routers, Ups, Sam, Servidores, instalación, configuración y demás. Se presupuestó el proyecto en

RD$ 2, 237,356.00 detallado en la tabla de la siguiente página.

En el mismo se destaca la inversión mayor que es la adquisición de los 2 Servidores requeridos, el monto asciende a RD$ 880,000.00 El segundo mayor Monto que tiene el presupuesto es la adquisición de los firewall que haciende a RD$ $660,000.

La Parte del cableado y configuración los técnicos de la institución la cubrirán con los materiales y la puesta en marcha del proyecto.

4.9. Presupuesto Del Proyecto

Descripción	Cantidad	Precio Unitario US$	Precio Unitario RD$	Total RD$
FortiGate S 5000	**2**	**$7500**	**$330000**	**$660000**
Router Cisco 3800	**1**	**$185**	**$8140**	**$8140**
Storage area network	**2**	**$1150**	**$50600**	**$101200**
Ups	**1**	**$2500**	**$110000**	**$110000**
Fibre Channel Switch	**2**	**$1250**	**$55000**	**$110000**
Dell Poweredge1950	**2**	**$10000**	**$440000**	**$880000**
Cisco Catalyst 2960	**4**	**$2716**	**$119504**	**$478016**
			Total RD$	**$2237356**

Tabla 4.1 Tabla de Presupuesto Fuente: Autor

4.10. Propuesta Para Adquisición de Equipo

Estos equipos se contemplaran en el presupuesto del año y serán financiados por organismo internacionales que aportan para el crecimientos de la CGRD.

4.11. Retorno de Inversión (Roi)

La contraloría general como órgano rector de todo el sistema financiero está obligada a garantizar los procesos y auditorias que se elaboran en el estado, facilitando todas las órdenes de pagos. Como se sabe las direcciones de tecnología están obligadas a garantizar y a automatizar todos los procesos para que los clientes tengan una mejor facilidad para acceder a las informaciones que solicitan a esta entidad.

Con la puesta en marcha de este proyecto se garantiza que las auditorias tendrán una mejor fluidez y que los pagos se registren en tiempos record también se podrá garantizar que las personas no estén cobrando en varias instituciones y con esta medida se proyecta que el estado tenga una partida millonaria para el presupuesto anual.

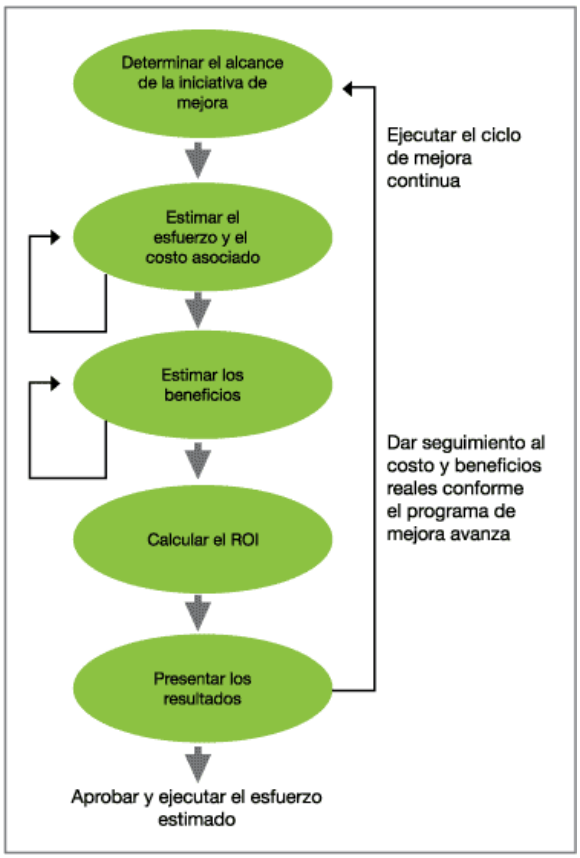

Figura 4.3 Procedimiento para el análisis del ROI Fuente: Alfredo Calvo

Calcular el ROI

El cálculo del ROI, se realiza dividiendo la estimación de los beneficios estimados entre los costos asociados con el programa. Si consideramos una inversión de

RD$ 2, 237,356.00 un beneficio esperado RD$8, 450,000.00 al año tenemos:

ROI = 8, 450,000 / 2, 237,356 = 3.77

El retorno de la inversión está garantizado en el primer año de ejecución ya que se estimas unas ganancias para el estado superior a los 3, 000,000.00 de pesos por la reducción que presentara el presupuesto anual del estado.

4.12. Costo del Proyecto

Se proyecta una inversión de RD$2, 237,356.00 de pesos.

4.13. Cronograma de actividades

El diseño e implantación del proyecto se desarrollara en 45 días Laborable teniendo en cuanta que cualquier imprevisto que pueda surgí, tal y como se detalla en el cronograma de actividades más abajo. Empezando con el análisis de la situación actual, donde también se hizo un levantamiento de los requerimientos y necesidades de la Institución.

Luego de evaluar la situación actual y conocer los requerimientos con que debe cumplir el proyecto, se diseñaron dos diferentes propuestas, las cuales necesitaron de 5 días de trabajo.

Para la presentación de las diferentes propuestas se necesitaron cotizar todos los equipos requeridos, para que con la información técnica y económica se tomara la decisión por una de las dos opciones.

Figura 4.4 Cronograma de Implementación Fuente: Autor

Recomendación

Según la investigación realizada, podemos recomendar:

- Implementar nuevas normas para el acceso a la Red fuera de la Institución, que solo el personal previamente autorizado pueda acceder.
- Enseñar la importancia y eficiencia de la Redundancia de datos a los empleados de TI.
- Crear un plan de Capacitación para los empleados de TI de la Contraloría General de la Republica Dominicana.
- Crear DMZ para los servicios que se accederán de la nube.
- Suplir con equipos de última tecnología, para poder maximizar la eficiencia y calidad de vida de los equipos.
- Los servidores deben conectarse a tomas provenientes de distintas regletas o fuentes, para contar con redundancia en caso de fallo eléctrico.

Estas recomendaciones pretenden ayudar a utilizar eficazmente los recursos de los Servidores y Base de Datos con los que cuenta el centro de datos de la Contraloría General de la Republica Dominicana. Es importante tener en mente que estas capacidades son limitadas y su uso debe realizarse con criterios de eficiencia energética.

Conclusión

Como resultado de la investigación realizada se ha podido comprobar la importancia, eficiencia y eficacia de la Redundancia de Datos, las cuales proporcionan tolerancia a fallos, lo que permite que el sistema continúe la operación total o parcial, si una parte del sistema falla debido a la pérdida o corrupción de datos o energía eléctrica. Dicha redundancia se produce automáticamente en algunos conjuntos de discos y ups, lo que permite recuperar datos en caso de fallo del mismo.

Cabe recordar que la Redundancia de datos es la copia (o re-escritura) de los datos, que se produce cuando algunas piezas o porciones de datos se almacenan dos veces. Esta da como resultado una reducción de la capacidad de almacenamiento, dado que la implementación de dicha redundancia requiere la duplicación de la totalidad de los conjuntos de datos o las colecciones de los datos relacionados almacenados en tablas. Tales duplicaciones ocupan una cantidad significativa de espacio de almacenamiento.

La redundancia de datos brinda un eficiente desempeño del sistema de Base de Datos, puesto que permite controlar la ejecución de transacciones que operan en paralelo, accesando a información compartida y, por lo tanto, interfiriendo potencialmente unas con otras. Permitiendo mejorar el rendimiento en las consultas a las bases de datos.

En conclusión se evidencia la necesidad de tener sistemas redundantes en los negocios los cuales garantiza la continuidad de los mismos.

Bibliografía

1. Aguilera Lopez, P. (2010). *Seguridad Informatica.* Madrid, España: Editorial Editex, S.A. .
2. Anonimo. (n.d.). *Linux Maxima Seguridad.* Prentice Hall.
3. (2004 [4ta Edicion]). *Sistemas de Bases de Datos.* Addison-Wesley. ISBN: 84-782-9075-3.
4. Brewer, E. (2000). *http://www.cs.berkeley.edu/~brewer/cs262b-2004/PODC-keynote.pdf.* Retrieved from Toward Robust Distributed Systems.
5. C., R. P. (2004). *Sistemas de Bases de Datos: Diseño, Implemetnacion y Administracion.* Mexico: International Thomson Editores, S.A.
6. Computadoras, C. y. (2004). *Stallings, W.* Madrid.
7. *contraloria.gob.do/Sitecontraloria/index.php/home/mision-y-vision*. (n.d.).
8. Dante Cantone, m. (2011). *Administrador de Storage y Backups.* Ra-Ma, 1ra Edicion.
9. David Afinson, K. Q. (2010). *IT Essentials: PC Hardware and Software Companion .* Indianapolis, Indiana: Third Edition, Cisco Press.
10. Dordoigne, J. (n.d.). *Redes Informaticas: Nociones Fundamentales (Protocolos, Arquitecturas, Redes Inalambricas, Virtualizacion, Seguridad, IP v6, ...).* Eni Ediciones 5ta Edicio.
11. edición., D. ".-V. (n.d.). *http://lema.rae.es/drae/?val=disponibilidad*.
12. Emmett Dulaney, M. J. (2011). *Seguridad Informatica.* Anaya Multimedia-Anaya Interactiva 1ra. Edicion.
13. Fernandez-Sanguino, J. F. (n.d.). *El sistema Operativo GNU/Linux y sus Herramientas libres en el mundo de la seguridad.*
14. Gabillaud, J. (2009). *SQL Server 2008 - SQL, Transact SQL: Diseño y creación de una base de datos.*
15. garcia-cervigon. (2011). *seguridad de informacion.* España: ediciones paraninfo, sa.
16. Garcia-Cervigon, A. &. (2011). *Seguridad Informatica.* Madrid, España: Ediciones Paraninfo, SA.
17. Gibson, D. (2011). *SECURITY +.*
18. Gonzalo Alvarez Marañon, P. P. (n.d.). *Seguridad Informatica Para empresas y Particulares.* McGraw-Hill.
19. Gottschalck, P. (2010). *Policing Cyber Crime.* Petter Gottschalck & Ventus .
20. Gudiño, P. F. (n.d.). *redundancia.*
21. Henry F. Korth, A. S. (2006 [5ta Edicion]). *Fundamentos de Base de Datos.* McGraw-Hill. ISBN: 84-481-4644-1.

22. *http://wwwclusterinformatica.blogspot.com/2011/05/cluster-informatica.html*. (n.d.).

23. J, D. C. (n.d.). *Introduccion a los Sistemas de Base de Datos.* Prentice Hall 7ma. Edicion.

24. James R. Groff, P. N. (n.d.). *Manual de Referencia SQL.* McGraw-Hill.

25. Jose Maria Alonso, A. G. (2012). *Ataques a Bases de Datos: SQL Injection.* UOC.

26. Korth, A. S. (n.d.). *Fundamentos de Base de Datos.* McGraw-Hill 4ta Edicion.

27. M., C. (2010). *200 Repuestas: Seguridad.* Lomas de Zamora, Argentina: Fox Andina.

28. Mannino, M. V. (n.d.). *Administracion de Bases de Datos: Diseño y Desarrollo de Aplicaciones.* McGraw-Hill 3ra. Edicion .

29. Marcos, G. (2011, Abril 03). *http://www.compuchannel.net/2011/04/03/redundancia-contingencia-continuidad-resiliencia/*.

30. Navathe, R. A. (2007 [5ta Edicion]). *Fundamentos de Sistemas de Base de Datos.* Addison-Wesley. ISBN 84-782-9085-0.

31. Olga Pons, N. M. (2005). *Introduccion a las Bases de Datos: Modelos Relacional.* Paraninfo. ISBN:8497323963.

32. Prowse, D. L. (2012). *Authorized Cert Guide Security SY0-301.* Indianapolis, Indiana: Second Edition, Pearson.

33. Rivero E., G. C. (2004). *Base de Datos relacionales: Diseño Fisico.* Madrid, España: R.B. Servicios Editoriales S.L.

34. Stewart, J. M. (2011). *CISSP. Certified Information Systems Security Professional.* USA: Fifth Edition Wiley Publishing, INC. .

35. Technology, C. (2010). *Computer Forensics, Investigating Network Intrusions & Cyber Crime.* Usa: Cengage Learning.

36. Technology., C. (2010). *Computer Forensics, Investigating Hard Disks, File & Operating Systems.* Volume 2. USA: Cengage Learning.

37. Vacca, J. R. (2005). *Computer Forensic. Computer Crime Scene Investigation.* Boston, Massachusetts: Charless River Media.

38. Valenzuala, F. D. (n.d.). *Seguridad Informatica en la Empresa: Teorias y Practica de Seguridad para empleados y Gerentes no tecnicos.*

39. Van Bon, J. (2008). *Fundamentos de la Gestion de Servicios de TI basada en ITIL.* Amersfoot, Holanda: Van Haren Publishing, Zaltbommel.

40. Vieites, A. G. (2011). *Enciclopedia de la Seguridad Informatica.* Ra-Ma Editorial, S.A. 2da Edicion.

Glosario

Alta disponibilidad de infraestructura: Si se produce un fallo de hardware en alguna de las máquinas del clúster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios en cualquiera de las otras máquinas del clúster.

Alta disponibilidad: es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado. Disponibilidad se refiere a la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos.

Archivo o **fichero informático:** Es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene.

Balance o balanceo de carga: Es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos.

Base de Datos Relacional: Es una base de datos que cumple con el modelo relacional, el cual es el modelo más utilizado en la actualidad para implementar bases de datos ya planificadas. Permiten establecer interconexiones (relaciones) entre los datos (que están guardados en tablas), y a través de dichas conexiones relacionar los datos de ambas tablas, de ahí proviene su nombre**:** "Modelo Relacional".

Base de datos o **banco de datos:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Cinta magnética: Es un tipo de medio o soporte de almacenamiento de datos que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro o algún cromato.

Clúster de alta disponibilidad: Es un conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí.

Clúster de alto rendimiento: Es un conjunto de ordenadores que está diseñado para dar altas prestaciones en cuanto a capacidad de cálculo.

Clúster: El término se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de hardwares comunes y que se comportan como si fuesen una única computadora.

Computador u ordenador: Es una máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil.

Contraloría: Entidad gubernamental destinada a la vigilancia y control de los gastos de la administración pública.

Datos: es una representación simbólica de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la

información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

DBASE: fue el primer sistema de gestión de base de datos usado ampliamente para microcomputadoras, publicado por Ashton Tate para CP/M, y más tarde para Apple II, Apple Macintosh, UNIX, VMS, e IBM PC bajo DOS donde con su legendaria versión III Plus se convirtió en uno de los títulos de software más vendidos durante un buen número de años.

Escalabilidad: Es la propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

Estructura de datos: Es una forma de organizar un conjunto de datos elementales con el objetivo de facilitar su manipulación. Un dato elemental es la mínima información que se tiene en un sistema.

Índice de una base de datos: Es una estructura de datos que mejora la velocidad de las operaciones, por medio de identificador único de cada fila de una tabla, permitiendo un rápido acceso a los registros de una tabla en una base de datos. Al aumentar drásticamente la velocidad de acceso, se suelen usar, sobre aquellos campos sobre los cuales se hacen frecuentes búsquedas.

Infraestructura: Es el conjunto de elementos o servicios que están considerados como necesarios para que una organización pueda funcionar o bien para que una actividad se desarrolle efectivamente**.**

Integridad de datos se refiere a la corrección y complementación de los datos en una base de datos.

Lenguaje de programación: Es un lenguaje formal diseñado para expresar procesos que pueden ser llevados a cabo por máquinas como las computadoras.

Metadatos: Literalmente «sobre datos», son datos que describen otros datos.

Multiprocesamiento o **multiproceso:** Es tradicionalmente conocido como el uso de múltiples procesos concurrentes en un sistema en lugar de un único proceso en un instante determinado.

Paradox: Es una base de datos relacional para entornos MS Windows, anteriormente disponible para MS-DOS y Linux, desarrollada actualmente por Corel e incluida en la suite ofimática WordPerfect Office.

Raid: Es un sistema de almacenamiento de datos que usa múltiples unidades de almacenamiento de datos (discos duros o SSD) entre los que se distribuyen o replican los datos.

Redundancia de datos: Es la copia (o re-escritura) de los datos, que se produce cuando algunas piezas o porciones de datos se almacenan dos veces. La redundancia de datos también tiene lugar si ciertos datos se pueden derivar directamente de otros.

Registro: representa un objeto único de datos implícitamente estructurados en una tabla. En términos simples, una tabla de una base de datos puede imaginarse formada de *filas* y *columnas* o campos.

SAN (Storage Area Network): Es una red de área de almacenamiento, es una red concebida para conectar servidores, matrices de discos y librerías de soporte.

Servidores: En informática, un servidor es un nodo que, formando parte de una red, provee servicios a otros nodos denominados clientes.

Sistema de gestión de bases de datos (**SGBD**): Es un conjunto de programas que permiten el almacenamiento, modificación y extracción de la información en una base de datos, además de proporcionar herramientas para añadir, borrar, modificar y analizar los datos.

SQL o lenguaje de consulta estructurado: Es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar de forma sencilla información de interés de bases de datos, así como hacer cambios en ellas.

Tabla en las bases de datos: se refiere al tipo de modelado de datos, donde se guardan los datos recogidos por un programa. Su estructura general se asemeja a la vista general de un programa de hoja de cálculo.

Anexos o Apéndice

Grupo Focal (Focus Group)

Es un tipo de técnica de estudio empleada en las ciencias sociales y en trabajos comerciales que permite conocer y estudiar las opiniones y actitudes de un público determinado.

Entrevistas Realizadas al Personal de TI.

Delwil Morillo

1- **Como defines la continuidad de negocios?**
   Que los servicios se mantenga disponible a la hora que los clientes lo requieran, para esto debe de existir DRP.

2- **Que sabe de redundancia de datos?**
   Es tener un servidor de acopio para alojar una copia de la base de datos, en caso de que el principal salga de servicio el segundo entre en operación, esto se hace poniendo el servidor de base de datos en espejo..

3- **Porque se recomiendan sistemas Seguros?**
   Esto evita la perdida de información por ataques de falso positivos e usuarios mal intencionado.

4- **Cuales motores de base de datos conoces?**
   Sql, Mysql, Oracol Data Centel.

5- **Cuál es la mejor forma para preservar los datos?**
   La mejor forma es haciendo backup periódicamente y almenarlos tanto en disco como en cintas.
6- **De qué depende la seguridad en TI?**
   La seguridad en TI depende de la robustecida y escalabilidad que esté formada su estructura de red y base de datos.

Jelinson Zapata

7- **Como defines la continuidad de negocios?**
Este concepto se enfoca en un plan de respuestas oportunas en caso de la materialización de algún riesgo que pueda interrumpir la operatividad de la entidad.

8- Que sabe de redundancia de datos?
Es un la técnica de crear un espejo de la información ya sea a través de arreglos de discos, replicación en servidores interno o e fuera (Site alternos), siendo así podemos garantizar la disponibilidad de los mismos.

9- Porque se recomiendan sistemas Seguros?
Se recomiendan por estos nos permiten mayor capacidad de aseguramiento, integridad y disponibilidad de la información.

10- Cuales motores de base de datos conoces?
Sql (Microsoft), My Sql, Oracle.

11- Cuál es la mejor forma para preservar los datos?
Mediante políticas de backup eficaces.

12- De qué depende la seguridad en TI?
Depende de la implementación de controles, mejores prácticas, cultura, etc. Alineados a la necesidades del negocio. Nota: La medidas de seguridad no deben interrumpir la operatividad del negocio.

Jesusito Luciano

1- **Como defines la continuidad de negocios?**
   Es como una empresa o negocio se prepara para situaciones de incidente que lo pueden poner en peligro su funcionamiento. Estos peligros van desde incendios hasta terremotos.

2- **Que sabe de redundancia de datos?**
   Esto es cuando los mismos datos se guardan varias veces en diferentes lugares.

3- **Porque se recomiendan sistemas Seguros?**
   Porque es una de la parte más importante para el mantenimiento de nuestro datos e informaciones a salvo.

4- **Cuales motores de base de datos conoces?**
   Mysql y sql server

5- **Cuál es la mejor forma para preservar los datos?**
   El consejo más importante que podemos ofrecer a cualquier, colectivo o individuo es que siempre mantenga a salvo las informaciones más importante.

6- **De qué depende la seguridad en TI?**
   Va a depender especialmente de un firewall y de un antivirus, además de aspecto físico y administrativos.

Thomas Tavera

1- **Como defines la continuidad de negocios?**

Diría que es la capacidad que tiene un negocio de ser rentable y continuar en operación.

2- **Qué sabe de redundancia de datos?**

Entiendo por redundancia de datos a la replicación de la data dentro de la base de datos que por razones de performance y de tiempo de respuesta se hace. Un ejemplo es la base de datos de Twitter, cuando realizas un tweet este es replicado en múltiples servidores repartidos estratégicamente en el mundo para asegurar la velocidad a la hora de acceder al mismo.

3- **Porque se recomiendan sistemas Seguros?**

Recomendaría sistemas seguros siempre y cuando maneje algún tipo de información personal, por ejemplo, cualquier sistema que necesite credenciales para identificar un usuario.

4- **Cuales motores de base de datos conoces?**

Oracle, Microsoft SQL Server, PostgreSQL, MongoDB, SQLite, Cassandra, Dynamo DB. Hasta ahora solo he utilizado Microsoft SQL y DynamoDB.

5- **Cuál es la mejor forma para preservar los datos?**

Aplicando las medidas de infraestructura y seguridad correspondientes.

6- **De qué depende la seguridad en TI?**

El cybersecurity es toda una rama de la tecnología en constante desarrollo, existen factores de seguridad que van desde la infraestructura hasta los protocolos de comunicación internos dentro de los sistemas.

DECANATO DE INGENIERIAS E INFORMATICA

Anteproyecto de Tesis

Asesor

Freddy Jiménez

Tema:

Diseño e implementación de un plan de redundancia y alta disponibilidad mediante un sistema de base de datos (SQL Server) para la Contraloría General de la República, en Santo Domingo, en el periodo Septiembre – Diciembre 2014.

Fecha

11/06/2014

Sustantes:

Saúl Espinosa 2006-2201

Luis Santos 2009-2058

Jorge Luis Beltre 2010-0599

Santo Domingo, Rep. Dom.

Tema

Diseño e implementación de un plan de redundancia y alta disponibilidad mediante un sistema de base de datos (SQL Server) para la contraloría general de la república, en santo domingo, en el periodo septiembre – diciembre 2014.

Introducción

La Contraloría General de la República está ubicada en Gazcue, av. México #45 edificio de finanzas, en Santo Domingo, República Dominicana es la institución encargada de auditar todas las ordenes de pagos del gobierno dominicano.

La data que se maneja en la institución es el activo más importante.

En la actualidad esta entidad no posee ningún mecanismo de redundancia de datos lo que puede ocasionar pérdida de información valiosa para la institución. La redundancia de datos se refiere a la réplica de datos e información en uno o varios equipos diferentes al que se encuentra almacenado.

Con esta investigación se buscara las soluciones a la problemática planteada con fines de que la Contraloría General de la Republica pueda obtener un mayor desenvolvimiento y eficiencia a la hora de tener los datos a la mano, para esto se analizaran cuales mecanismos de redundancia podrían ser útiles para tener una mejora en la institución y a su vez evitar la pérdida de cualquier tipo de información a toda costa.

Por otro lado se pretenden analizar los factores que podrían producir los fallos a favor de la perdida de información para así minimizarlos al punto de que sea evitable que se produzca alguna ruptura en los servidores que poseen los datos. Es muy importante

que la institución tenga mayor control con los usuarios que interactúan con los servicios y con el manejo de la información, se deben obtener reportes de los servidores cada x tiempo periódico para así evitar un mal funcionamiento.

Las bases de datos son un área de la ingeniería que ha recibido bastante atención debido a sus múltiples aplicaciones: automatización de oficinas, ingeniería de software, bibliotecas, diccionarios automatizados y en lo general cualquier sistema orientado a mantenerse y recuperar información importantes de la organizaciones e instituciones y empresa. Su recuperación, actualización y manejo es relativamente sencillo con el uso de cualquier manejador de bases de datos SQL. Cuando hablamos de archivos con estructura nos estamos refiriendo a documentos cuya estructura es declarada de algún modo, asociamos etiquetas a algún elemento de una estructura o mediante sintaxis con la que se escribe el archivo, como se hace en los lenguajes de programación.

Justificación e Importancia

El activo más importante que tiene una organización es la información que esta procesa y/o maneja, por lo que es necesario garantizar la disponibilidad e integridad de la misma. Para esto la dirección de tecnología de la información (TI) de cada organización o empresa planifica las medidas de seguridad necesarias para cumplir con este objetivo.

Una de estas medidas es el uso de equipos en los cuales se replique la información almacenada en los servidores principales de la organización. Esto garantiza la disponibilidad de la información en caso de pérdidas accidentales o fallas en los equipos.

Analizando el caso de estudio, se considera de suma importancia que la Contraloría General de la República adopte este tipo de medidas con el fin de prevenir situaciones que pongan en riesgo la información almacenada en los servidores vigentes.

La pérdida de información vital acarrearía graves problemas en el manejo del control interno del Estado. Por lo tanto, si ocurre un fallo en la infraestructura de la institución, esto puede causar que no se pueda realizar de manera adecuada la revisión de los registros contables de las diferentes entidades y organismos del Estado. En el peor de los escenarios, la perdida de registros contables puede ocasionar que se ponga en duda las observaciones y/o recomendaciones otorgadas por la Contraloría General de la República, y esto a su vez, puede cuestionar la eficiencia de la gestión del Contralor en función.

Planteamiento del Problema

Descripción del Problema

La Contraloría General de la República es una dependencia de la Presidencia de la República Dominicana que tiene como función realizar auditorías especiales y revisiones de los registros de contabilidad de las entidades y organismos del Gobierno central, ayuntamientos, entidades descentralizadas y autónomas, y de cualquier persona física o jurídica que administre o maneje fondos y bienes públicos. Es decir, esta entidad vela por el control interno del Estado dominicano.

En la actualidad esta entidad no posee ningún mecanismo de redundancia de datos lo que puede ocasionar pérdida de información valiosa para la institución. La redundancia de datos se refiere a la réplica de datos e información en uno o varios equipos diferentes al que se encuentra almacenado.1 En esta propuesta se analizará algunos mecanismos de redundancia que podrían mejorar la situación actual de la entidad.

Analizando el problema, se verifica que la mayoría de los servicios informáticos se encuentran centralizados en los diferentes servidores de la institución, si alguno de estos presenta una falla, se vería afectado todo el sistema institucional ya que en estos se alojan todas las informaciones de desembolsos de pagos del estado. Cabe destacar que la antigüedad de estos equipos causa una gran deficiencia ante las exigencias informáticas, impidiendo un buen desempeño a la hora de responder a una necesidad. Además, estos equipos presentan una escasa compatibilidad con nuevas tecnologías

[1] García-Cervigón, A. & Alegre Ramos, M. (2011). Seguridad Informática. Madrid, España: Ediciones Paraninfo, SA

que podrían ayudar a aprovechar al máximo el espacio y funcionamiento de los mismos.

Por otra parte, el esquema de red actual no garantiza la continuidad de los servicios y disponibilidad de la información ya que en caso de presentarse una falla en alguno de los puntos, la carencia de enlaces redundantes causaría una pérdida de información impidiendo la recuperación de la misma. Además no existe una política de seguridad de red implementada, lo que presenta un alto riesgo para la institución por los posibles ataques a la información.

Los cambios permiten aislar los problemas que se puedan presentar en la red en el futuro, también reducirá el tiempo para la solución de los mismos, pues ya los usuarios, servidores y demás equipos no quedan al mismo nivel ni en el mismo segmento. La nueva estructura también permite aplicar políticas de control de acceso para los usuarios, de tal forma que es posible restringir el acceso a dispositivos en específicos (P.ej.: servidores o Firewall de Internet).

Anteriormente no existía control sobre quienes se conectaban remotamente a la red vía las instituciones externas. Por un lado, las instituciones externas protegían su acceso desde afuera pero no había restricción para conectarse hacia la Contraloría. Con los nuevos cambios, solo las conexiones remotas explícitamente configuradas tendrán permiso para entrar a la red.

Formulación del problema

¿Cuáles mecanismos de redundancia y alta disponibilidad de datos se podrían aplicar en la Contraloría General de la República?

Sistematización del problema

¿Cuáles son los principales problemas que afectan actualmente a los servidores de almacenamiento de información ubicados en el data center de la institución?

¿Cuáles métodos de redundancia de datos permitirían asegurar la disponibilidad de la información y continuidad del negocio en caso de alguna falla?

¿Cuál topología de red debería implementarse a fin de asegurar la comunicación entre los distintos puntos de acceso de la institución?

Objetivos

Objetivos generales

Determinar los mecanismos de redundancia y alta disponibilidad de datos para la Contraloría General de la República.

Objetivos específicos

Identificar mecanismos de redundancia de datos que se adapten a las necesidades de la Contraloría General de la República.

Proponer una topología de red que garantice la continuidad del negocio y la disponibilidad de los datos.

Determinar políticas de seguridad de la información que contribuyan a mejorar la protección de los datos e integridad de los mismos.

Evaluar la capacidad de los equipos existentes y determinar las mejoras o cambios que puedan mejorar la situación actual.

Marco de referencia

Marco teórico

Entre los aspectos considerados por la seguridad de la información se encuentra el evitar el acceso no autorizado a la información y robo o fraude de datos. Por otro lado también se consideran otros aspectos importantes como el control de acceso físico y la continuidad del servicio.

Para obtener continuidad del servicio, tanto la arquitectura de las aplicaciones como la infraestructura de recursos de hardware deben diseñarse para obtener tal objetivo. Dentro de las estrategias utilizadas por una dirección de TI se encuentra la redundancia de datos. Debido a esto, este trabajo se enfoca en la importancia que subraya el autor Enrique Rivero Cornelio, del cual se cita lo siguiente:

“Mencionaremos la importancia de diseñar la arquitectura del sistema con redundancia, para que el fallo de un componente no afecte el nivel de servicio. Para ello hay que estudiar la presencia de posibles puntos aislados de fallo y evitarlos con la duplicidad o redundancia de recursos. Debe subrayarse también la importancia de no olvidar en el estudio las paradas planificadas para mantenimiento, bien sea correctivo o bien preventivo, el cual es necesario para disminuir la probabilidad de fallos futuros o para satisfacer necesidades de crecimiento.”2

Dado que la Contraloría General de la República trabaja con sistemas críticos que deben estar funcionando las 24 horas al día, los 365 días del año, se considera necesario minimizar los fallos que pueden afectar el funcionamiento normal del

[2] Rivero, E., Guardia, C. & Reig, J. (2004). Base de datos relacionales: Diseño físico. Madrid, España: R.B. Servicios Editoriales S.L.

sistema. Existen técnicas y configuraciones que ayudan a tener sistemas redundantes, sin que esto afecte al funcionamiento de los mismos.

Según las mejores prácticas para la gestión de servicios de TI, señaladas por ITIL (Biblioteca de Infraestructura de Tecnología de la Información), la redundancia es una forma de aumentar la disponibilidad y sostenibilidad de sistemas.3 En un sistema informático existen muchos componentes necesarios para que este funcione, cuantos más componentes se tengan más será la probabilidad de que ocurra un fallo. El grado de redundancia de un sistema dependerá de su importancia y del dinero que puede perderse cuando el sistema no esté disponible debido a un fallo. ITIL define los siguientes tipos de redundancia:4

Redundancia activa: Se utiliza para reforzar servicios esenciales que no pueden ser interrumpidos bajo ningún concepto. Con este tipo de redundancia, todas las unidades redundantes están simultáneamente en operación (p. ej. Discos replicados en un servidor).

Redundancia pasiva: Consiste en el uso de activos redundantes que no están operativos hasta que se produce algún fallo (p. ej. Clústeres de sistema).

Redundancia heterogénea: Redundancia con distintos tipos de activos del servicio con capacidades comunes. Se utiliza cuando un fallo se debe a una causa difícil de

[3] Van Bon, J. (2008). Fundamentos de la Gestión de Servicios de TI basada en ITIL. Amersfoort, Holanda: Van Haren Publishing, Zaltbommel.
[4] Van Bon, J. (2008). Fundamentos de la Gestión de Servicios de TI basada en ITIL. Amersfoort, Holanda: Van Haren Publishing, Zaltbommel.

predecir (p. ej. Uso de distintos medios de almacenamiento, lenguajes de programación o equipos de desarrollo).

Redundancia homogénea: Consiste en el uso de capacidad extra del mismo tipo de activos del servicio. Se utiliza cuando la causa del fallo se conoce con certeza (p. ej. Uso de procesadores idénticos).

En el desarrollo de este trabajo de investigación se indicaran los tipos de redundancia que pueden mejorar y/o solucionar la situación actual de la Contraloría General de la República.

Origen Histórico

Contraloría General de la República Dominicana: Origen y evolución

El Sistema Nacional de Control de la República Dominicana descansa en la actualidad en dos pilares fundamentales: Control Externo y Control Interno, teniendo el primero como organismo ejecutor a la Cámara de Cuentas y, el segundo, a la Contraloría General de la República.

Esa primera institución tiene su fundamento legal en la Ley 10-04 mientras que la Contraloría General de la República lo hace a través de la Ley 10-07, no obstante, las ejecuciones de control del Estado aparecen en la primera Constitución de la República, proclamada en San Cristóbal, el 6 de noviembre del 1844. Este ejercicio de control se realizaba a través de un organismo denominado Consejo Administrativo.

El artículo 182 de la referida Constitución dominicana, indica que "la ley organizará un Consejo Administrativo compuesto por funcionarios públicos para verificar anualmente las cuentas generales y hacer un informe de ellas al Congreso, con las observaciones que juzgue oportunas, cuyo encargo será puramente gratuito".

Mediante la Ley No. 42 promulgada el 12 de junio de 1845, se crea la "Contaduría General" como una dependencia de la Secretaría de Estado de Hacienda y Comercio, cuyas funciones, al tenor del numeral 1 del artículo 2 de la mencionada ley, eran las siguientes: "Examinar, verificar, arreglar y centralizar todas las cuentas de la Tesorería General ".

Posteriormente, la Ley 75 del 7 de mayo de 1846 deroga la Ley No.42 y amplía las funciones del Administrador e Inspector General y del Consejo Administrativo, que a la

sazón estaba integrado por empleados públicos dirigidos por el Presidente de la República. Es durante la aplicación de esta iniciativa, que se produjeron inexactitudes sobre las funciones de los diferentes servidores públicos, lo que originó la promulgación de una nueva legislación que se detalla en el próximo párrafo.

La Ley 114 del 2 de julio de 1847, modifica y amplía las atribuciones del Contador General, que como administrador e inspector general le atribuía la mencionada Ley No.42, a los fines de solucionar los inconvenientes que se producían en la aplicación de la Ley 75.

La Resolución No. 9 de fecha 10 de abril del 1897, crea el Departamento Examinador de Cuentas, cuya misión principal era inspeccionar y desglosar las cuentas del Estado por parte de los oficiales de la Oficina de Asuntos Insulares (Bureau of Insular Affairs), bajo la dirección del Departamento de Guerra de los Estados Unidos de América.

Mientras, la Orden Ejecutiva No. 563 de fecha 20 de noviembre de 1920, que contenía la Ley de Hacienda y que modifica la Ley 114, es la primera que contempla una diferencia entre Tesorero y Auditor , y reparte las funciones del Contador General entre los ya citados cargos. Por el seguimiento cronológico e histórico se ha podido establecer que las funciones de control siempre se ejercieron aunque bajo diversas denominaciones.

Durante la presidencia de Horacio Vásquez, se promulga el 3 de mayo de 1929, la Ley No.1114 de Contabilidad General que da origen a la "Oficina de Contabilidad General",

independiente de los departamentos administrativos bajo el control y dirección de un Contralor General de la República Dominicana.

Es importante hacer notar, que es a partir de esta ley que la Contraloría adquiere independencia con respecto a su objeto de oficina de control financiero y fiscalización de las operaciones de ingresos y egresos del Estado.

En ese orden, el 9 de agosto del 1954 y mediante Ley 3894, se crea la “Contraloría y Auditoría General de la República”. A la que luego se le modificaría el artículo 1, a través de la Ley No.54 del 1970, sustituyendo la denominación de "Contraloría y Auditoría General de la República por "CONTRALORÍA GENERAL DE LA REPÚBLICA”. Desde este entonces queda establecida la dependencia directa de esta Institución del Poder Ejecutivo en el organigrama del Estado dominicano:

“Art.1 (Modificado por la Ley No.54 del 13 de noviembre de 1970, G. O. No.9205). La Contraloría General de la República (bajo la dependencia directa del Poder Ejecutivo en virtud a lo dispuesto por el Art. 1 de la Ley No. 54, precitada), y la que estará bajo la dirección de un funcionario que se denominará Contralor General de la República ; también habrá un Sub-Contralor General; tendrá a su cargo la contabilidad general del Estado, fiscalizar el debido ingreso e inversión de los fondos de los diversos departamentos de la Administración Pública, autónomos o no, del Estado y de los municipios; verificar el examen de las que deban rendir las personas o entidades que reciban o manejen fondos o bienes de tales entidades u organismos, así como la inspección contable de las oficinas correspondientes a los mismos”.

El 27 de julio de 2001, como resultado de modificaciones que se habían realizado en el sector financiero nacional, se crea mediante la Ley No. 126-01 la Dirección General de Contabilidad Gubernamental; esta ley asume parte de las funciones que la Ley 3894 le asignaba a la Contraloría General de la República, y que venía ejecutando al amparo de otras legislaciones.

Con la nueva Ley 10-04 del 20 de enero del 2004 a la Cámara de Cuentas se le otorga la potestad de realizar el control externo, sobre las entidades generadoras y ejecutoras del presupuesto nacional, función que también realizaba la Contraloría General de la República desde sus inicios, lo que provocaba una duplicidad de funciones.

En tanto, la Ley 10-07, del 4 de enero de 2007, designa a la Contraloría General de la República como Órgano Rector del Control Interno del Estado.

Cabe resaltar que el modelo del Sistema Nacional de Control establecido en República Dominicana es único debido a que en los demás países existe una sola entidad de control, esto es, o una Contraloría General o un Tribunal de Cuentas, o Cámara de Cuentas.

Ahora que se dispone de una nueva herramienta legal y siguiendo los pasos indicado por su reglamento, se ha desarrollado un proceso tendente a socializarla con todos los miembros de la Contraloría, y concomitantemente con los que integran los distintos organismos generadores y ejecutores del Presupuesto Nacional, a los fines de aplicar con propiedad los mandatos de las presentes normativas.

Partiendo de la dinámica de las sociedades a la que no escapan las instituciones y sus normas, la movilidad evolutiva de estas es eterna, por lo que en cada momento si así lo

determinan las circunstancias, esta ley deberá ser modificada para que pueda responder a las exigencias de la época[5].

[5] http://contraloria.gob.do/Sitecontraloria/index.php/home/origen-historico

Visión

Ser reconocida como el órgano rector del control interno, agregando valor a la gestión pública para garantizar ejecutorias optimas y transparentes.

Misión

Somos el órgano rector del sistema nacional de control interno, fiscalizador del debido recaudo, manejo, uso e inversión de los recursos públicos, responsables de autorizar las órdenes de pago, mediante revisiones y consultorías objetivas que generen resultados oportunos, a través de procesos automatizados y estandarizados, recursos humanos idóneos y metodologías basadas en gestión de riesgo; contribuyendo al mejoramiento continuo de las instituciones bajo el ámbito de la ley, creando rentabilidad social.

Valores

Confiabilidad: Gestión basada en altos estándares profesionales, garantizando un desempeño eficiente orientado al logro de resultados.

Legalidad: Aplicamos y supervisamos el cumplimiento de la Constitución y las disposiciones legales, reglamentarias y administrativas vigentes.

Probidad: Actuamos de manera íntegra y objetiva, cumpliendo con la ética profesional.

Discreción: Manejamos con prudencia y criterios confidenciales e institucionales, las informaciones y todo recurso bajo nuestro ámbito de responsabilidad.

Respeto a la Diversidad: Valoramos a las personas y sus formas de pensamiento, independientemente de sus condiciones.

Transparencia: Garantizamos el acceso a la información pública, sobre los procesos y los resultados que estos generan[6].

[6] http://contraloria.gob.do/Sitecontraloria/index.php/home/mision-y-vision

Marco conceptual

A continuación se definen los conceptos claves que el lector debe entender para poder comprender la finalidad de este trabajo de investigación.

Redundancia de datos: Como se indicó anteriormente, se refiere a la réplica de datos e información en uno o varios equipos diferentes al que se encuentra almacenado.

Disponibilidad de datos: Garantiza que la información y recursos del sistema estén disponibles en el momento en que los usuarios los necesiten.7

Riesgo: En seguridad informática, se considera un riesgo a la posibilidad de que se materialice una amenaza debido a una vulnerabilidad presente.8

Topología de red: Es la manera en como los datos se transmiten a través de la red.

Política de seguridad: Agrupa un conjunto de normas y procedimientos que ayudan a mantener un nivel de seguridad adecuado en un sistema informático.9

Marco espacial

La formulación del problema, la investigación que se desarrollará en base a esta y las posibles soluciones que serán analizadas se circunscriben a La Contraloría General de la República Dominicana, específicamente a su Sede principal ubicada en la ciudad de Santo Domingo.

[7] Cerra, M. (2010). 200 Respuestas: Seguridad. Lomas de Zamora, Argentina: Fox Andina
[8] Aguilera López, P. (2010). Seguridad informática. Madrid, España: Editorial Editex, S.A.
[9] García-Cervigón, A. & Alegre Ramos, M. (2011). Seguridad Informática. Madrid, España: Ediciones Paraninfo, SA

Marco temporal

La delimitación temporal de esta investigación se centra en el año 2014.

Aspectos metodológicos de la investigación

Tipo de estudio

El análisis de esta investigación corresponde al primer nivel del conocimiento, es decir, el tipo de estudio exploratorio o formulativo. Este tipo de estudio permite realizar una investigación precisa de una problemática observada, de esta manera se da lugar a un marco teórico de referencia que sirva de apoyo al desarrollo de la investigación.

Método de investigación

Para este trabajo de investigación se utilizará como guía el método de análisis. Este tipo de método de investigación permite analizar cada una de las partes que caracterizan una realidad problemática, y a partir de esta se desarrolla un análisis de las consecuencias y posibles recomendaciones a fin de dar solución al problema.

Fuentes y técnicas de recolección de información

Para el desarrollo de la unidad de investigación se utilizará como fuente primaria la observación directa por parte de uno de los empleados de la entidad analizada, quien a su vez, es parte del equipo de investigación que sustenta este trabajo.

Además, se considera adecuado emplear el uso de entrevistas al personal del área de informática de la Contraloría General de la República con la finalidad de obtener

información detallada de la situación problemática para poder enfocar la investigación a una solución que garantice resultados positivos y permanentes.

Bibliografía

García-Cervigón, A. & Alegre Ramos, M. (2011). Seguridad Informática. Madrid, España: Ediciones Paraninfo, SA

Rivero, E., Guardia, C. & Reig, J. (2004). Base de datos relacionales: Diseño físico. Madrid, España: R.B. Servicios Editoriales S.L.

Van Bon, J. (2008). Fundamentos de la Gestión de Servicios de TI basada en ITIL. Amersfoort, Holanda: Van Haren Publishing, Zaltbommel.

Van Bon, J. (2008). Fundamentos de la Gestión de Servicios de TI basada en ITIL. Amersfoort, Holanda: Van Haren Publishing, Zaltbommel.

Cerra, M. (2010). 200 Respuestas: Seguridad. Lomas de Zamora, Argentina: Fox Andina

Aguilera López, P. (2010). Seguridad informática. Madrid, España: Editorial Editex, S.A.

Rob, P. & Coronel C. (2004). Sistemas de Base de Datos. Diseño, Implementación y Administración. México: International Thomson Editores, S.A.

García-Cervigón, A. & Alegre Ramos, M. (2011). Seguridad Informática. Madrid, España: Ediciones Paraninfo, SA

Oficina Presidencial de Tecnologias de la Informacion y Comunicaciones. (2014). norma general sobre el uso e implementacion de las tecnologias de la informacion y comunicacion en el estado dominicano. Santo domingo: Optic.

contraloria.gob.do/Sitecontraloria/index.php/home/mision-y-vision

contraloria.gob.do/Sitecontraloria/index.php/home/origen-historico

Ramez A. Elmasri & Shamkant B. Navathe: “Fundamentos de Sistema de bases de datos”. Addison-Wesley, 2007 [5ta edición]. ISBN 84-782-9085-0.

Olga Pons, Nicolás Marín, Juan Miguel Medina, Silvia Acid & Ma Amparo Vila: “Introducción a las Bases de Datos: Modelos relacional”. Paraninfo, 2005. ISBN 8497323963.

Anónimo “Linux Máxima Seguridad”
Prentice Hall.

Jorge Ferrer y Javier Fernandez-Sanguino “El Sistema Operativo GNU/Linux y sus herramientas libres en el mundo de la seguridad” .

Thomas M. Connolly & Carolyn E. Begg:
“Sistemas de bases de datos”Addison-Wesley, 2005 [4ta edición]. ISBN 84-782-9075-3.

Henry F. Korth, Abraham Silberschatz & S. Sudarshan:
“Fundamentos de bases de datos”.McGraw-Hill, 2006 [5ta ed]. ISBN 84-481-4644-1.

Tabla de contenido

Fuentes y técnicas de recolección de información

Muestra

Tipo de Muestra

Tamaño de la Muestra

Capítulo 1 Contraloría General De la Republica

- Introducción
- Historia
- Organigrama
- Filosofía
- Misión
- Visión
- Valores

Capítulo 2 Técnicas Base de Datos (SQL Server)

- Características Generales de SQL
- Redundancia de datos
- Disponibilidad de datos
- Lenguajes de Definición de Datos
- Lenguaje de Manipulación de Datos
- Recuperación de Clave

Capítulo 3 Seguridad de Red y Servidores

- Firewall
- IDS (Intrusion Detection System)
- NIDS (Network Intrusion Detection System)
- HIDS (Host Intrusion Detection System)
- SIEM (Security Incident And Event Management)
- Vlan
- Seguridad de Puertos

Capítulo 4 Situación Actual de la Institución y Propuesta

- Situación
- Esquema de Red
- Servidores e Infraestructura
- Propuesta
- Cotización de los Nuevos Equipo y Presupuesto
- Propuesta Para Adquisición de Equipo
- Tiempo de Retorno de Inversión
- Costo del Proyecto
- Cronograma de Implementación
- Consideraciones Finales

Conclusión

Recomendación

Bibliografía

Glosario

Anexos o Apéndices