FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO ACADÉMICO DE BACHILLERATO EN INGENIERÍA INFORMÁTICA

PROPUESTA DE UN PLAN DE CONTINUIDAD DE LOS SERVICIOS DE BASE DE DATOS SQL, DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA, ALINEADO A LAS NORMAS TÉCNICAS DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

LUIS ALEJANDRO MADRIGAL BENAVIDES

TUTOR: M. SC. ERICK LÓPEZ CHAVARRÍA

I CUATRIMESTRE, 2017

DECLARACIÓN JURADA

Yo Luis Alejandro Madrigal Benavides, mayor de edad, portador de la cédula de identidad número 1-1439-0513 egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Bachillerato en Ingeniería Informática juro solemnemente que mi trabajo de investigación titulado: Propuesta de un Plan de Continuidad de los servicios de bases de datos SQL, de la unidad de Tecnologías de Información y Comunicación del Benemérito Cuerpo de Bomberos de Costa Rica, alineado a las normas técnicas de la Contraloría General de la República., es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público. en fe de lo anterior, firmo en la ciudad de San José, a los 23 días del mes de Enero del año dos mil 17.

Firma del estudiante

Cédula 1-1439-0513

CARTA DEL TUTOR

Heredia, 17 Noviembre del 2016

Destinatario
Carrera
Universidad Hispanoamericana

Estimado señor:

El estudiante LUIS ALEJANDRO MADRIGAL BENAVIDES, cédula de identidad número 114390513, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado ***Propuesta de un plan de continuidad de los servicios de base de datos SQL, de la Unidad de Tecnologías de Información y Comunicación del Benemérito Cuerpo de Bomberos de Costa Rica, alineado a las normas técnicas de la contraloría General de la República.,*** el cual ha elaborado para optar por el grado académico de Bachillerato.
En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	8%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	28%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	18%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20%
	TOTAL		94%

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

Ing. Erick López Chavarría, M.R.I.
Cédula identidad 1-0993-0088

CARTA DE LECTOR

Universidad Hispanoamericana
Sede Heredia
Carrera Ingeniería Informática

Estimado señor

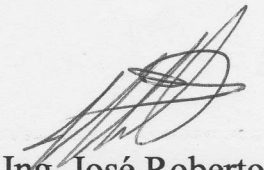
El estudiante Luis Alejandro Madrigal Benavides, cédula de identidad: 1-1439-0513, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado " PROPUESTA DE UN PLAN DE CONTINUIDAD DE LOS SERVICIOS DE BASE DE DATOS SQL, DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA, ALINEADO A LAS NORMAS TÉCNICAS DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA", el cual ha elaborado para obtener su grado de Bachillerato en Ingeniería Informática.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

Firma



Nombre Ing. José Roberto Santamaría Sandoval
Cédula 1-1178-0664
Carnet IE-15830

CARTA DE REVISIÓN DEL FILÓLOGO

San José, 20 de enero del 2017.

Señores

UNIVERSIDAD HISPANOAMERICANA

Estimados señores:

Hago constar que he revisado el trabajo de **PROYECTO DE GRADUACIÓN** del estudiante **LUIS ALEJANDRO MADRIGAL BENAVIDES** denominado **PROPUESTA DE UN PLAN DE CONTINUIDAD DE LOS SERVICIOS DE BASE DE DATOS SQL, DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA, ALINEADO A LAS NORMAS TÉCNICAS DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA,** para optar por el grado académico de **BACHILLERATO EN INGENIERÍA INFORMÁTICA.**

He revisado errores gramaticales, de puntuación, ortográficos y de estilo que se manifiestan en el documento escrito, y he verificado que estos fueron corregidos por el autor.

Con base en lo anterior, se considera que dicho trabajo cumple con los requisitos establecidos por la **UNIVERSIDAD** para ser presentado como requisito final de graduación

Atentamente,

Dr. Bolívar Bolaños Calvo
Carné: 2 949
2-279-320
e-mail: solymsa@racsa.co.cr
Colegio de Licenciados y Profesores

Dedicatoria

A mis padres, quienes desde pequeño me ayudaron a ser la persona que ahora soy, que me ayudaron siempre a salir adelante y que a pesar de todas las cosas siempre estuvieron ahí aconsejándome, ayudándome a no desmayar. Gracias porque sé que sacrificaron muchas cosas en esta etapa para ayudarme a finalizar este proyecto. Que Dios me los bendiga siempre.

A mi hermano menor, como el ejemplo que debe seguir para salir adelante y ser una persona de bien, para que no desaproveche la oportunidad que le dan mis padres para que pueda alcanzar un título universitario, confió plenamente en él y en Dios que así será.

A mi esposa, que fue un apoyo incondicional para poder terminar este trabajo, al igual que mis padres, sé que sacrifico mucho, pero siempre consciente de lo que significaba para mí este trabajo y lo que significa para esa familia que estamos empezando a formar.

A mi primer hijo, la bendición que me mando Dios al final de esta etapa, el obtener la noticia de que iba a ser padre me termino de dar esa fuerza al final del proyecto, pensando siempre en poder darle el mejor ejemplo y deseando darle lo mejor para que nunca le falte nada.

Agradecimiento

Primero agradecer a Dios y a la Virgen de los Ángeles por la vida, por permitirme llevar a cabo este proceso y poder terminarlo de la mejor manera y así cumplir un sueño más en mi vida.

A mis padres, esposa y hermano, por tanto sacrificio que realizaron a lo largo de mis estudios, principalmente a mi padre por tantos consejos y ayudas, por todas esas horas, días explicándome lo que no entendía.

Agradezco al Profesor, Msc. Erick López Chavarría, por su dedicación, conocimientos y experiencia para poder realizar un gran trabajo.

Al Benemérito Cuerpo de Bomberos, por abrirme las puertas y por apoyarme para poder realizar este proyecto en tan prestigiosa institución.

A todos mis familiares, amigos y compañeros que siempre me brindaron palabras de aliento y que cuando necesitaba ayuda siempre estuvieron ahí.

Para todos ellos estaré eternamente agradecido, que Dios los llene de muchas bendiciones.

Tabla de contenido

Contenido

CAPÍTULO I PLANTEAMIENTO DEL PROBLEMA

1.1 Introducción al tema del proyecto

En este documento se estará describiendo las características principales de la Organización, entre ellas las funciones a las que se dedica, como lo es la atención de emergencias que se presentan a nivel nacional, además de cómo está compuesta la Institución en referencia a sus departamentos y funciones. Por otro lado se describirá la justificación de la ejecución de este proyecto, el por qué se llevará a cabo según las necesidades de la institución y la prioridad que tiene el tema para los directores a cargo de la Organización. Se mencionarán los aportes que este trabajo dejará al Cuerpo de Bomberos en el ámbito de la continuidad de los servicios de Tecnologías de Información y Comunicación y también los beneficios que tendrá a nivel global la Institución (empleados, jefaturas, clientes, procesos).La descripción del problema actual ira referenciada en esta primera parte del documento, así como el objetivo general y los específicos dejando claro que se pretende hacer en la ejecución del proyecto, para esto se define el alcance en donde se dejará en evidencia cual es el fin del proyecto, que incluirá y hasta donde se llegará. También se dejarán claras las limitaciones que se tendrán, todas esas cosas que hacen que el proyecto se pueda atrasar o que no se obtengan los resultados que se esperaban.

En la segunda parte de este documento se definirán algunos conceptos técnicos que ayudará a los lectores a entender el desarrollo del trabajo. También se explicarán en qué consisten las metodologías que se utilizarán en la ejecución del proyecto como lo es COBIT, ITIL. Se mencionarán algunas de las empresas o

experiencias semejantes a lo que se pretende y que han sido desarrolladas de manera exitosa.

En el tercer capítulo se hablará sobre el tipo de investigación, su finalidad, dimensión temporal, marco, condición en la que se hace, carácter y naturaleza que tendrá este proyecto. Otra de las cosas que se mencionarán serán los sujetos y fuentes de información, con la descripción de las personas que se consultarán así como los libros, revistas, artículos y documentos que servirán para obtener información importante, las técnicas y herramientas que se manejarán para sustraer la información de la mejor manera posible.

En el cuarto capítulo se realizará un análisis de la situación actual de Benemérito Cuerpo de Bomberos en cuanto al servicio de bases de datos brindado por la Unidad de Tecnologías de Información y Comunicación (TIC). Se estarán realizando diagnósticos tanto a nivel administrativo u operativo, técnico y de percepción, además de establecer las brechas o conclusiones de los diagnósticos realizados.

En la quinta parte se estará proponiendo los aspectos que deben ser creados o modificados para mantener la continuidad del servicio de bases de datos que brinda la unidad de TIC, así como la propuesta de un plan piloto del plan de continuidad el cual contendrá la información requerida para restablecer el servicio ante cualquier desastre, tomando en cuenta recurso humano y tecnológico, todo basado según dictan las normas de la Contraloría General de la República.

1.2 Antecedentes del Contexto de la empresa

1.2.1 Nombre de la empresa

Benemérito Cuerpo de Bomberos de Costa Rica.

1.2.2 Año de fundación

1865.

1.2.3 Estrategia: Misión, Visión

1.2.3.1 Misión

Brindar a la sociedad costarricense protección cuando la vida, los bienes y el medio ambiente se encuentran amenazados por incendios y situaciones de emergencia, basados en los más altos principios humanos y en la búsqueda permanente de la excelencia.

1.2.3.2 Visión

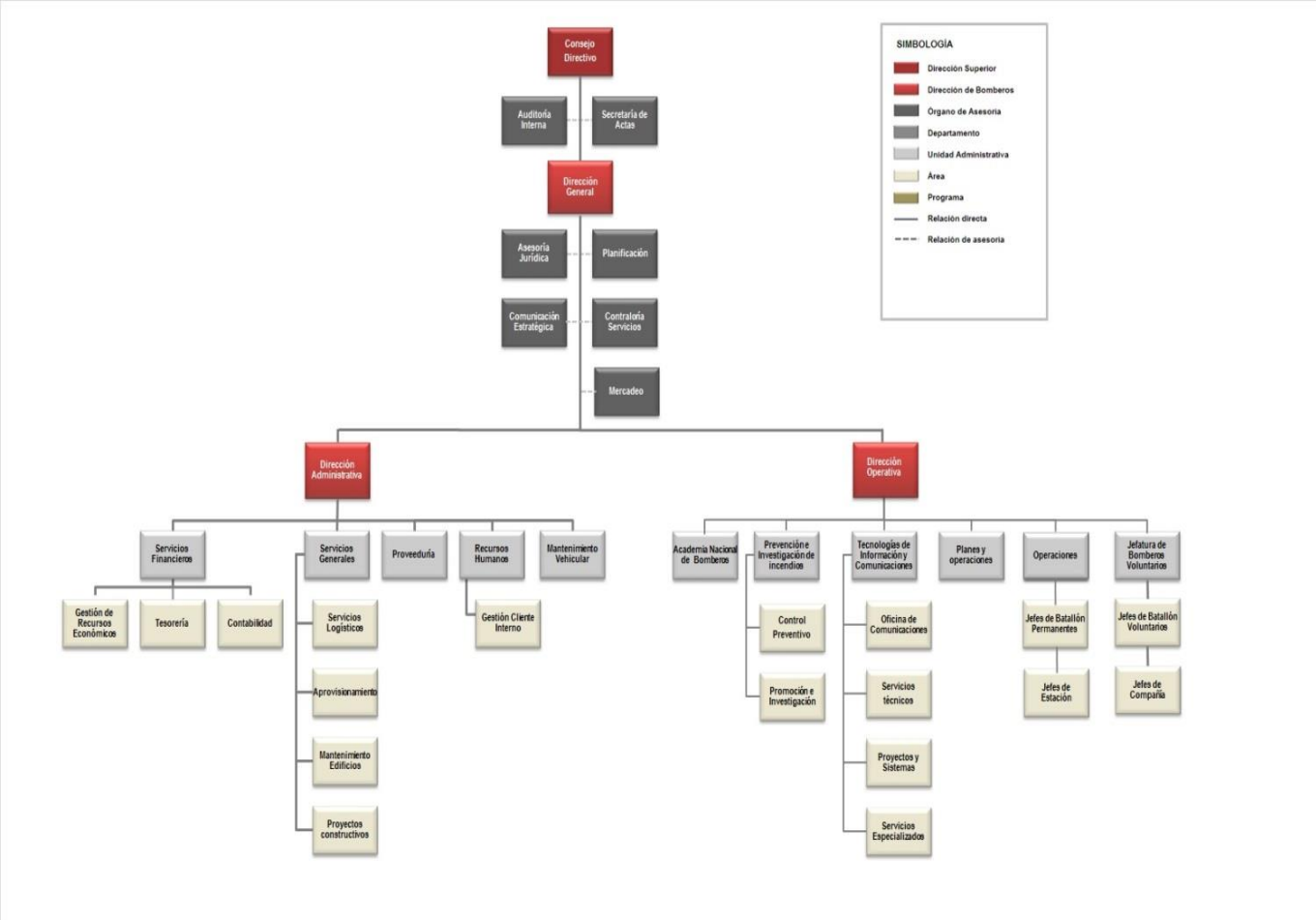
Ser una organización estatal de primera respuesta reconocida por sus altos estándares de calidad, eficacia y eficiencia, al atender las emergencias de su competencia y proveer servicios de prevención de incendios que integralmente, contribuyan al desarrollo del país, mediante la mejora de los índices de protección a la vida, la propiedad y el medio ambiente.

Bomberos.go.cr [Internet]. Costa Rica: Bomberos de Costa Rica [citado 8 jun de 2016]. Disponible en http://www.bomberos.go.cr/mision-y-vision/

1.2.4 Organización

El Benemérito Cuerpo de Bomberos de Costa Rica está compuesto por tres Direcciones: la General, la Operativa y la Administrativa, todas ellas bajo el liderazgo de un Consejo Directivo.

Figura 1: Organigrama Institucional.



Fuente: Tomado de Benemérito Cuerpo de Bomberos de Costa Rica (2016)

1.2.5 Negocio al que se dedica.

El Benemérito Cuerpo de Bomberos de Costa Rica, se dedica brindar servicios de protección, capacitación y prevención de emergencias.

1.2.6 Historia de la organización.

La historia registra que los sucesos ocurridos en San José, el 26 de enero de 1864, a raíz de un voraz incendio en la casa propiedad de don Francisco María Iglesias, indujeron a los costarricenses para formar un cuerpo de bomberos debidamente organizado.

Con la enorme preocupación que dejó entre los vecinos ese siniestro, el 15 de febrero de ese mismo año la Municipalidad de San José acordó iniciar gestiones, para traer de los Estados Unidos una “bomba para incendios”, la cual llegó a la capital el 20 de junio de 1865. Simultáneamente, el Ayuntamiento de San José preparó y presentó al Poder Ejecutivo, el primer Reglamento Oficial del Cuerpo de Bomberos, el cual fue aprobado con fecha 27 de julio de 1865, la cual marca el inicio en Costa Rica de las actividades de una organización de esa índole. Por serias dificultades económicas de la Corporación Municipal, en 1914 los bomberos dejaron de pertenecer a ella y de funcionar como tal. Entonces pasaron a ser dependencia del gobierno y los miembros de la Policía de Orden y Seguridad asumieron la responsabilidad de operar la bomba para incendios, junto con la ayuda espontánea de ciudadanos que acudían en los momentos que cada siniestro ocurría. Bomberos.go.cr [Internet]. Costa Rica: Bomberos de Costa Rica [citado 8 jun de 2016]. Disponible en http://www.bomberos.go.cr/academia-historia/historia-antigua/

El 29 de mayo de 1925, por medio del Decreto Ejecutivo N°4 del entonces presidente de la República el Lic. Ricardo Jiménez Oreamuno, se dispuso que el Cuerpo de Bomberos pasara a ser una dependencia del citado Banco, hoy el Instituto Nacional de Seguros (INS) y que éste fuera el encargado de su administración y dotación.

En marzo del 2002 se promulgó la Ley 8228, Ley del Cuerpo de Bomberos del Instituto Nacional de Seguros, con el propósito de dotar al referido Cuerpo de un marco jurídico que lo respaldara como organización para la atención de situaciones específicas de emergencia y, a la vez, establecer un sistema de financiamiento.

Bomberos.go.cr [Internet]. Costa Rica: Bomberos de Costa Rica [citado 8 jun de 2016]. Disponible en http://www.bomberos.go.cr/academia-historia/historia-reciente/

El Benemérito Cuerpo de Bomberos de Costa Rica cuenta con 73 estaciones de bomberos distribuidas a nivel nacional, ubicadas estratégicamente, cuentan con personal altamente capacitado en diversas áreas.

En las estaciones el personal de Bomberos labora un horario denominado 24X24, es decir, que laboran un día completo (24 horas) y descansan el siguiente día las 24 horas. De esta manera un funcionario ingresa a la estación a las 8:00 a.m., sale libre al día siguiente a esa hora y vuelve a ingresar el tercer día a las 8:00 am.

1.3 Justificación del proyecto

El Benemérito Cuerpo de Bomberos de Costa Rica está conformado por unidades operativas, que sus labores son el uso de los sistemas para registrar las emergencias que se presentan (incendios, escapes de gas, enjambres de abejas, rescate de personas, entre otras). Se encuentran las áreas administrativas como Contabilidad, Recursos Humanos, Proveeduría, entre otras; en los cuales los sistemas son parte indispensable del trabajo diario y en donde los datos deben estar en disponibilidad inmediata. También se tienen áreas técnicas como la Unidad de tecnologías de Información y Comunicación, donde se orientará la propuesta de continuidad de la información y servicios de bases de datos. En cada una de estas unidades y en los procesos que se ejecutan día con día, se utilizan diferentes aplicaciones o sistemas informáticos en los cuales se manipulan datos sensibles.

Es por esa razón que la continuidad de los servicios tecnológicos (Sistemas, Gestores de Bases de Datos, Equipo, entre otros), son de suma importancia para mantener sus procesos y servicios operando de manera continua. Por tal razón el Departamento de Tecnologías de la información por una directriz administrativa, quiere estar a derecho con la ley y cumplir con las normas de continuidad de los servicios establecida y dictada por la contraloría General de la República, que en cumplimiento del numeral 1.4 de las referidas Normas Técnicas, esta Contraloría General emitió en 2007 y 2012, las directrices D.5.2007-CO-DDI y D-1-2012-DC-UTI con el propósito de documentar e implementar una política de seguridad de la información y los procedimientos correspondientes; asignar los recursos necesarios

para lograr los niveles de seguridad requeridos y considerar lo que establece la normativa en mención.

Para el benemérito Cuerpo de Bomberos la propuesta elaborada en este proyecto brindará mejores controles de acuerdo a los planes de continuidad de servicios que se desarrollaran y se recomendarán en este trabajo. Debido a la falta de un plan de contingencia es conveniente desarrollar la implementación de lo propuesto en este trabajo en beneficio de toda la institución, especialmente evitar pérdidas no solamente de datos si no evitar pérdidas económicas. La actualización de los procesos y planes de contingencia que aquí se mencionan traerán el beneficio de estar al día con las propuestas gubernamentales y evitando así posibles sanciones administrativas que traerían más problemas a los ya identificados.

Según oficio **CBCR-021280-2015-DGB-00716** enviado por el Director General el 20 de Agosto del 2015, se hace referencia a la importancia para la organización definir las directrices de continuidad de las operaciones del Cuerpo de Bomberos cuyo propósito principal indica textualmente lo siguiente: **“Definir las directrices a seguir antes, durante y después de una interrupción de las operaciones del Cuerpo de Bomberos, que respondan oportunamente ante eventos que afecten las operaciones y servicios brindados por la organización, así como gestionar la continuidad y recuperación de los procesos, con el menor impacto de las operaciones.”**

Este proyecto de forma específica dará un beneficio a las personas encargadas de mantener día a día los datos disponibles y los sistemas a la mano para desarrollar de mejor forma el trabajo de la institución; específicamente los

administradores de bases de datos, los desarrolladores de sistemas, quienes tendrán accesible la o las herramientas disponibles para la debida continuidad de los servicios informáticos. Por lo tanto el desarrollo de este proyecto llenará un vacío existente de planes de contingencia con respecto a la manipulación de datos y el correcto manejo y uso de los mismos.

El proyecto en sí se justificará apoyado en normas establecidas por la contraloría general de la república y la directriz anteriormente mencionada. Estas normas son prácticamente de uso y conocimiento de las áreas involucradas. La implementación de este proyecto traerá resultados específicos a las eventualidades que se presenten para la continuidad de los servicios; un valor agregado será la capacitación obligatoria a los funcionarios involucrados en el proyecto. En este momento llenará el vacío existente, contribuyendo así a establecer de forma correcta las normas mencionadas y el análisis de problemas eventuales o reales con que carece el Cuerpo de Bomberos en este momento.

Según indica ITIL v3 entre las ventajas de la administración de la continuidad de servicios se destacan las siguientes:

1. Manejo y mitigación de riesgos.
2. Reducción de periodos de interrupción no planificados de los servicios de TI.
3. Se fortalece la confianza en la calidad del servicio por parte de usuarios y clientes.

4. Se constituyen en el apoyo confiable que requiere el proceso en la continuidad de las operaciones del negocio.

1.4 Definición del Problema

La Unidad de Tecnologías de Información y Comunicación del Benemérito Cuerpo de Bomberos de Costa Rica, se encuentra desde el año 2009 en un proceso de mejoramiento administrativo; para que las políticas y normas de atención de los servicios en general sean acorde a lo establecido por la ley de Costa Rica en cuanto a la Gestión de la Seguridad de la Información y de la Continuidad de los servicios informáticos. Por esta causa se revisan los procedimientos establecidos para que la continuidad y disponibilidad de los servicios y de la información estén de forma inmediata a disposición de quien los necesite.

¿Cuál es la situación actual del proceso de base de datos en la unidad de Tecnologías de Información y Comunicación?

Se han identificado incumplimientos de normas; como la normativa de Gestión de la Seguridad de la Información, en su apartado de la continuidad de los servicios de Tecnología de Información (TI) según la Contraloría General de la República[1]. Estas normas establecen como se deben administrar las Tecnologías de Información en las instituciones públicas para asegurar que mantengan a TI funcionando de la manera adecuada; poder medir el costo/beneficio de las inversiones que esta área de la organización realice, brindar servicios más

1 Contraloría General de la República, Normas Técnicas para la gestión y el control de las Tecnologías de Información, proceso 1.4 Gestión de la seguridad de la información, apartado 1.4.7 Continuidad de los servicios de TI.

confiables, mayor trasparencia en los procesos que se ejecuten, capacidad de respuesta de TI con el negocio y mayor retorno de la inversión.

¿Cuáles son las principales vulnerabilidades que tiene el proceso de continuidad de base de datos?

La aplicación de Normas técnicas, permitirá que los servicios de Tecnologías de Información y Comunicación (TIC) mediante adecuados modelos de Gestión de Seguridad Informática, mejoren prácticas que presentan lineamientos inadecuados con respecto a la funcionalidad y la asistencia necesaria en caso de emergencia. Debido a que la Organización debe velar por la disponibilidad para la cual debe tener la información requerida en el momento que se necesite, confidencialidad donde la información debe ser accesible a sus destinatarios predeterminados (usuarios) e integridad donde la información debe ser correcta y completa, protegiéndola de manipulaciones que puedan causar daño, pérdida, o modificaciones no autorizadas.

La problemática enfocada a las causas y efectos se podría explicar en la siguiente manera:

- La inexistencia de un plan de continuidad de los servicios de la Unidad de Tecnologías de Información y Comunicación, podría generar un efecto en la interrupción de los servicios brindados, afectando la atención oportuna en casos de desastres naturales o de fallas humanas y técnicas, lo que significaría la no obtención de la información en el momento. Esto entrabaría el proceso normal y el día a día del manejo de los datos.

- Actualmente contar con un modelo de gestión de los Servicios de Tecnologías de Información, no alineado a las mejores prácticas establecidas legalmente, hace que estas no se ajusten a lo que la Contraloría estipula en su proceso 1.4 y apartado 1.4.7. que textualmente dice: **"La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica en forma efectiva y oportuna las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización"** (Aguilar Montoya, 2007, pág. 5)**,** pudiendo generar gran impacto en los costos de la organización al no contar con las acciones preventivas y correctivas en caso de algún incidente, ya sea humano o natural.

- De acuerdo a lo estipulado por la Contraloría General de República en su norma de la seguridad y continuidad de los servicios, indica el apartado: "…**que se debe documentar y poner en práctica acciones preventivas y correctivas**…" (Aguilar Montoya, 2007, pág. 5), siendo la capacitación una de esas prácticas preventivas, se necesita de un proceso de inducción al personal a cargo de las funciones propias en caso de una eventualidad, que interrumpa los servicios y/o la disponibilidad de la información requerida. El no contar con este proceso de inducción que dé el conocimiento adecuado a los funcionarios, podrían afectar la secuencia operativa y la integridad de datos[2] y recuperación de los mismos. La capacitación es una inversión y debe realizarse en el tiempo adecuado, para que

2 Se refiere a los valores reales que se almacenan y se utilizan en las estructuras de bases de datos.

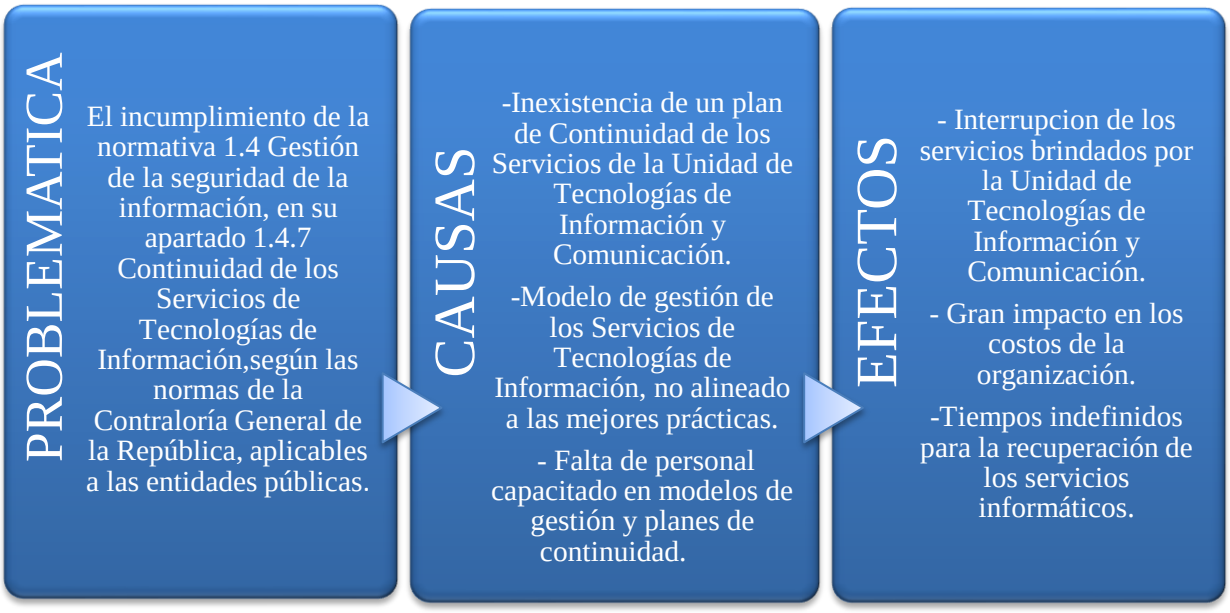
tampoco afecte el proceso normal de atención al usuario y los servicios, por lo que deben planificarse escogiendo quienes van a capacitar y a quienes se capacitará, identificando y separando las áreas involucradas.

- Al no existir un plan como el que se propone, los tiempos para la recuperación de servicios y de información serán indefinidos. Ocasionando el atraso en la obtención de la información que se requiere por parte de los usuarios internos del departamento, con un debido tratamiento a los problemas identificados y mediante la capacitación continua de los involucrados (usuarios, técnicos, entre otros.), estos tiempos y costos serán minimizados y corregidos de la manera adecuada.

¿Qué criterios técnicos se deben tomar en cuenta para diseñar el plan de bases de datos?

Esta propuesta es necesaria no solamente para cumplir con dicha norma, sino porque por no tener planes de continuidad de servicios informáticos, puede tener el riesgo de contar con incidentes imprevistos, con que puedan tener los procesos, que están relacionados, por ejemplo, a la parte operativa y que podrían generar inconsistencias o la no disponibilidad en la información de las emergencias atendidas, repercutiendo en procesos legales y viéndose afectada la imagen de Bomberos. De la misma manera las unidades financieras podrían caer en grandes errores en el presupuesto disponible, al no contar con la información real en cuanto al proceso financiero de la Institución y por consiguiente, no se cumpla con los objetivos organizacionales, provocando pérdidas económicas de consideración.

Figura 2: Diagrama Causa-Efecto



Fuente: Elaboración propia (2016)

1.5 Objetivos

1.5.1 Objetivo general

Proponer un Plan de Continuidad a los Servicios de Base de Datos brindados por la Unidad de Tecnologías de Información y Comunicación del Benemérito Cuerpo de Bomberos de Costa Rica, alineados a las normas técnicas de la Contraloría General de la República, durante el II semestre del 2016.

1.5.2 Objetivos específicos

- **Diagnosticar** la situación actual del proceso de continuidad de base de datos en la Unidad de Tecnologías de Información y Comunicación.
- **Analizar** las principales vulnerabilidades del proceso de continuidad de base de datos detectadas en el diagnóstico, en relación con las buenas prácticas propuestas por las normas técnicas de la Contraloría General de la República y el DS4 de Cobit v4.1.
- **Diseñar** el plan de continuidad de base de datos para la Unidad de Tecnologías de Información y Comunicación basado en las normas técnicas de la Contraloría General de la República.
- Proponer un plan piloto para la **implementación** del proyecto de continuidad de base de datos para la Unidad de Tecnologías de Información y Comunicación.

1.6 Alcance

El **primer entregable** será, un documento que contenga los puntos vulnerables en caso de la interrupción de los servicios de la base de datos. En este entregable se analizarán los procesos de recuperación actuales (si existen) y poderlos comparar con las recomendaciones establecidas por la Normativa de la Contraloría General de la República, en cuanto a la continuidad de los servicios.

El **segundo entregable** será, un documento que identifique puntualmente las vulnerabilidades y como estas debe diseñarse o ajustarse con el análisis realizado.

El **tercer entregable** será un documento que contenga el detalle del plan de continuidad de base de datos, basado en los resultados obtenidos en el primer y segundo entregable.

El **cuarto entregable** será un documento con el plan piloto de la implementación del plan de continuidad de base de datos. Este entregable tendrá como fin establecer las correcciones administrativas y técnicas, así como la capacitación técnica que incluye la parte normativa que dicta la contraloría General de la República, respecto a los planes y procedimientos de prevención y recuperación. Además de la inducción correspondiente, según los puestos del personal involucrado, tanto a nivel de sistemas informáticos como bases de datos, sin dejar de lado a los usuarios que utilizan esos sistemas.

1.6.1 Exclusiones

Como exclusiones en este proyecto, estarían las bases de datos Oracle, ya que en un corto/mediano plazo todo lo referente a bases de datos se estará unificando en bases de datos Microsoft SQL Server 2014 Enterprise. Otras de las exclusiones son los demás servicios que brinda la unidad de Tecnologías de Información y Comunicación del Cuerpo de Bomberos, como lo son:

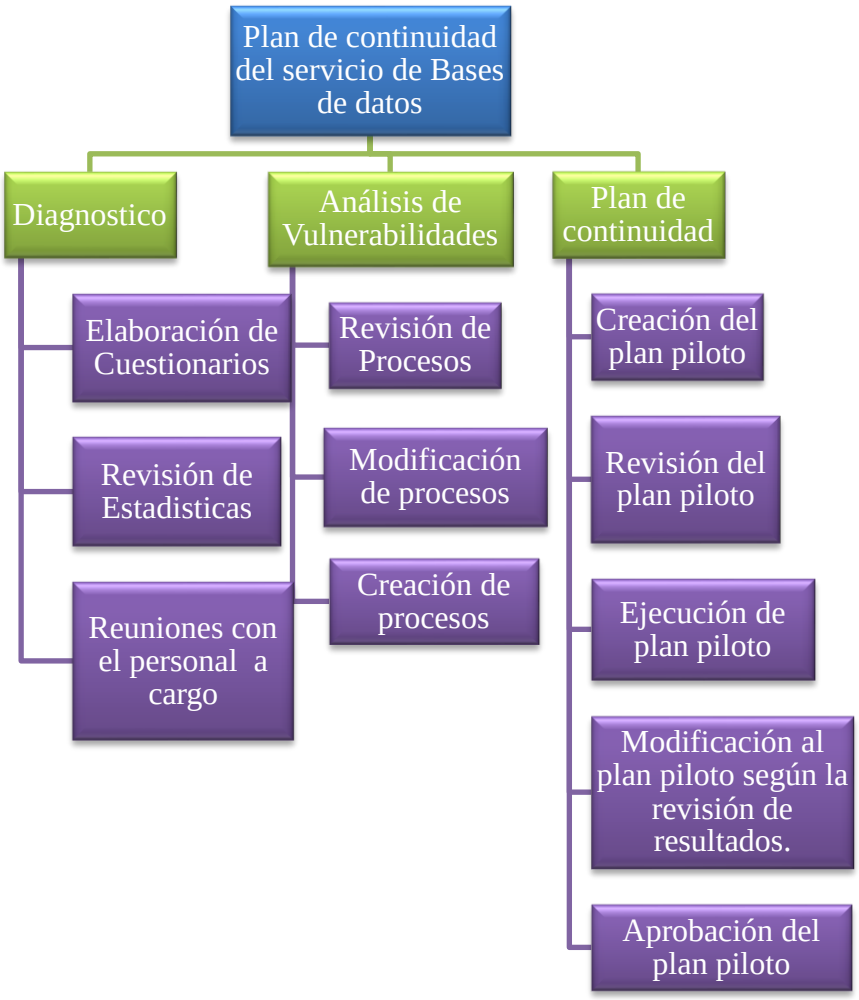
- Gestión de la Plataforma Tecnológica.
- Soporte Técnico de la plataforma Tecnológica.
- Gestión de las Telecomunicaciones
- Gestión de Despacho de Recursos para la atención de emergencias
- Gestión de Mensajería electrónica
- Gestión de Software Colaborativo
- Gestión de Aplicaciones
- Gestión Estadística
- Gestión de Cartografía Digital

1.7 Limitaciones

A raíz de lo mencionado, se podría topar en el proceso, la necesidad de crear o modificar alguna política o procedimiento institucional y esto podría generar un atraso en el desarrollo del proyecto, por cuanto puede ser necesaria una aprobación del consejo directivo y se generarían atrasos hasta que estos cambios sean aprobados.

1.8 EDT

Figura 3: Diagrama EDT



Fuente: Elaboración propia (2016)

CAPÍTULO II MARCO TEÓRICO

2.1 Marco conceptual general.

2.1.1 Los procesos de Continuidad de las Bases de Datos en TI.

En diferentes áreas de trabajo de las empresas, se habla de procesos como una serie de pasos que se deben seguir de forma lógica, para cumplir con objetivos. Itilv3 define proceso como **"Un conjunto de actividades interrelacionadas orientadas a cumplir un objetivo específico."**(http://itilv3.osiatis.es/estrategia_servicios_TI.php, Osiatis S.A, Itilv3, recuperado el 2-6-16 a las 09:44pm). Para las empresas sea cual sea su misión es importante definir sus procesos tanto administrativos, estratégicos, operativos entre otros, pues estos traerán grandes ventajas porque son cuantificables y se basan en el rendimiento, tienen resultados específicos, tienen un propósito claro y se pueden identificar tiempos, recursos y responsables. Haciendo que con esta información se puedan tomar decisiones para la mejora continua de los procesos aplicados y así mejoras al servicio que se brinda.

En la mayoría de las empresas, hoy en día, se utilizan diferentes sistemas informáticos para gestionar la información de los procesos que se ejecutan; la información se encuentra almacenada en bases de datos, las cuales se pueden definir como **"un almacén que permite guardar grandes cantidades de información de forma organizada para que luego se pueda encontrar y utilizar fácilmente".** (http://www.maestrosdelweb.com/que-son-las-bases-de-datos/, Pérez, 2007, recuperado el 5/6/2016 a las 12:00 pm). En las bases de datos se pueden almacenar grandes cantidades de información, como por ejemplo, clientes,

productos, ventas, cuentas bancarias, inventarios, entre otras. Mucha de esta información es de gran relevancia y es por que las bases de datos son un pilar importante en las grandes empresas.

Las bases de datos sirven para tener la información disponible cuando se desee, además de mantenerla ordenada y lo menos redundante posible. Por medio de los sistemas gestores de bases de datos se puede brindar accesos específicos a los usuarios y así velar por la seguridad de la información que se encuentra almacenada.

Por esto las empresas luchan por tener procesos de continuidad de bases de datos, que faciliten y ayuden a mejorar las consultas de la información y asegurar la disponibilidad de la misma. Debido a lo importante que es para el negocio esta disponibilidad, muchas organizaciones establecen en sus políticas y procesos que la información debe estar disponible 24 horas los 365 días del año.

2.1.2 Las vulnerabilidades del proceso de continuidad de base de datos y las buenas prácticas para evitarlas.

En todos los procesos que tienen las organizaciones, existen vulnerabilidades que no se pueden controlar por completo, sin embargo, las empresas luchan por disminuir su impacto y la probabilidad de que suceda. La vulnerabilidad se define como "**La probabilidad de que, debido a la intensidad de un evento externo y a la fragilidad de los elementos expuestos, ocurran daños en la economía, la vida humana y el ambiente**". (http://www.cepal.org/publicaciones/xml/3/8283/jjgomez.pdf, Zapata, 2000, recuperado el 2/6/2016 a la 07:05 pm). Es difícil predecir cuándo se

enfrentará con una vulnerabilidad, pero las empresas deben estar preparadas para cuando suceda. Una vulnerabilidad en bases de datos va desde una persona mal intencionada que ingrese a los sistemas y manipule la información del negocio, hasta un desastre natural que impida el buen funcionamiento de los equipos y sea imposible obtener la información que se requiera en ese momento. A raíz de esto, es la importancia de las empresas de contar con procesos que ayuden a identificar estas vulnerabilidades para así tomar medidas de prevención con el fin de estar preparados para cualquier eventualidad.

Para poder asumir estos riegos, existen mejores prácticas que ayudan a mejorar el control de las vulnerabilidades que se presenten en cada proceso de la empresa, ya que estas aconsejan como gestionar estos procesos. La Universidad Internacional de Valencia, define buenas prácticas como **"Todas aquellas experiencias que se guían por principios, objetivos y procedimientos apropiados o por pautas aconsejables que se adecuan a una normativa determinada o a una serie de parámetros consensuados".** (http://www.viu.es/concepto-y-utilidad-de-las-buenas-practicas-en-la-ensenanza/, Universidad Internacional de Valencia, Recuperado el 2/6/2016 a las 07:40pm). Como bien se cita anteriormente, las buenas prácticas nacen de estudios e investigaciones realizadas a procesos o actividades que se presentaron en algún momento y que ayudaron a obtener mejores resultados en estos procesos. Por tal razón es importante aplicar buenas prácticas que ayuden a disminuir las vulnerabilidades que se presenten en los servicios que brinda la empresa, en especial a los servicios de TI, permitiendo mejorar estos servicios en eficiencia y

eficacia. Al implementar mejores prácticas las empresas se benefician en aumentar la calidad del servicio y la satisfacción de los usuarios; facilita la toma de decisiones, reducción de costos, reducción de riesgos y el impacto en los cambios, ayuda a utilizar de una mejor manera los recursos tecnológicos y favorece a disminuir los tiempos de respuesta ante cualquier eventualidad.

2.1.3 Las normas técnicas de la Contraloría General de la República

En Costa Rica, las empresas públicas son regidas por la Contraloría General de la República, estas dictaminan como deben trabajar estas entidades de gobierno para vigilar el uso de los recursos públicos como por ejemplo los tecnológicos y esto se enjuicia en las llamadas Normas Técnicas para la gestión y el control de las tecnologías de información, las cuales esta entidad define como **"Los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado".** (http://www.ocu.ucr.ac.cr/Leyes/Nuevas%20normas%20de%20TI%20-CGR%20N-2-2007-CO-DFOE.pdf, Contraloría General de la República, 2007, Recuperado el 4/6/2016 a las 8:10 am). Estas normas sirven para que las entidades públicas de Costa Rica, velen por el buen uso de los presupuestos asignados ya que este dinero es tomado de fondos públicos y sus gastos deben ser reportados a esta entidad. También para regular de una mejor manera la administración de los recursos

tecnológicos y mantener una continuidad razonable de los servicios que se brindan y certificar que la interrupción de los mismos no afecten significativamente a los usuarios. Estas normas se dividen en 5 capítulos, los cuales se mencionan a continuación:

- Capítulo I Normas de aplicación general
- Capítulo II Planificación y organización
- Capítulo III Implementación de tecnologías de información
- Capítulo IV Prestación de servicios y mantenimiento
- Capítulo V Seguimiento

2.1.4 Plan piloto para la implementación

El término "implementar" es usado en muchas empresas cuando desean desarrollar proyectos con el fin de mejorar o crear algún proceso, y está relacionado a términos como investigación, análisis, evaluación entre otros. Según la real academia española el termino implementar se refiere a: **"Poner en funcionamiento o aplicar métodos, medidas, para llevar algo a cabo".** (http://dle.rae.es/?id=L4eKVkR, Real Academia Española, 2016, recuperado el 4/6/2016 a las 10:25 am). Esta definición ayuda a entender el por qué en la mayoría de las empresas les gusta hablar de la implementación, ya que al implementar, las organizaciones se aseguran de que se estará llevando a cabo un proyecto el cual dependerá de investigaciones previas, análisis y pruebas, asegurándose de alcanzar de una mejor manera sus objetivos. Muchas de estas implementaciones

son de planes estratégicos, planes de continuidad operativa, planes de control de calidad de productos y servicios.

Es importante mencionar que la implementación se da también para planes pilotos, que utilizan las empresas para asegurar que el proyecto que se ejecutara será beneficioso para el negocio y en la mayoría estos planes son aprobados por las juntas directivas o personal de peso que respalde lo que se ejecutara en ese plan. Se define como plan piloto, **"…una herramienta científica estándar para una investigación "suave", lo que permite que los científicos lleven a cabo un análisis preliminar antes de iniciar un experimento o estudio a gran escala**."(https://explorable.com/es/estudio-piloto , recuperado el 4/6/16 a las 11:40). Este plan piloto los encargados del proyecto pueden observar todas la variables que existen, ventajas y desventajas de implementarlo ya como un proyecto final, en esta etapa se está a tiempo de corregir y evaluar situaciones que no se hayan contemplado al inicio y asegurar que el plan final va a traer grandes beneficios al negocio.

2.1.5 Planes de contingencia para la continuidad de los servicios de bases de datos

Las empresas hoy en día sea cual sea su misión, están expuestas a ser perjudicadas por diversos factores o riesgos que afectan su funcionamiento y el alcance de sus objetivos, paralizando las procesos diarios que en esta se realizan, es por esto que las empresas deben contar con planes de contingencia para poder continuar con las operaciones, se define este plan como, "**Un conjunto de**

procedimientos alternativos a la operatividad normal de cada institución. Su finalidad es la de permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización." (http://www.forodeseguridad.com/artic/discipl/4132.htm, recuperado el 21/8/2016 a las 02:00 pm)**.** Contar con estos planes actualizados, ayuda a las instituciones a levantarse de una forma más rápida, eficaz y eficiente en caso de alguna caída de los servicios, garantizando la continuidad de los mismos. En las instituciones públicas, la creación de estos planes debe estar acorde a las normas y procedimientos establecidos por la Contraloría General de la República.

2.2 Marco de la gestión del proyecto

2.2.1 COBIT

Por sus siglas en ingles Control Objetives for Information and related Technology (Objetos de control para tecnología de la Información y relacionada), es un modelo para el gobierno de las Tecnologías de Información desarrollado por la Information System Audit and Control Association (ISACA) y el IT Governance Institute (ITGI). Según este último, COBIT, **"brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógicas. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien."** (IT Governance Institute, 2007, p. 5. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf).Estas buenas prácticas

ayudarán a las organizaciones a mantener una Unidad de Tecnologías de Información y Comunicación (TIC) funcionando adecuadamente y permitiendo el avance de la Institución en busca de cumplir los objetivos del negocio. COBIT trabaja sobre 4 dominios que son: planear y organizar, adquirir e implantar, entregar y dar soporte, monitorear y evaluar. Esto sobre procesos que TIC ejecuta diariamente y ello permitirá asegurar, que la información de la Organización está segura y que se le da el trato correspondiente para evitar sustracción de datos, perdida de información o que la misma sea inconsistente. La disponibilidad es otro factor muy importante que COBIT toma en cuenta, esto por cuanto los datos deben estar disponibles todo el tiempo para cualquier tipo de Organización.

2.2.1.1 DS1 Definir y administrar los niveles de servicio

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los interesados sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados. (COBIT 4.1, IT Governance Institute, 2007, p.101).

2.2.1.2 DS2 Administrar los servicios de terceros

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de

administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los Servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada. (COBIT 4.1, IT Governance Institute, 2007, p.105).

2.2.1.3 DS3 Administrar el desempeño y la calidad

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua. (COBIT 4.1, IT Governance Institute, 2007, p.109).

2.2.1.4 DS4 Garantizar la continuidad del servicio

La continuidad de los servicios es un punto muy crítico para las Organizaciones; pues deben garantizar a sus clientes o usuarios que la información siempre va a estar accesible pase lo que pase y es por esta razón se debe estar preparado para cualquier eventualidad. COBIT en su dominio DS4, ayuda a las empresas a garantizar la continuidad del servicio, como se indica en su manual COBIT 4.1 **“La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los**

planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio." (COBIT 4.1, IT Governance Institute, 2007, p.113. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf)**.** Con esto se asegura el mínimo impacto al negocio en caso de alguna interrupción de los servicios de TI. Entre las características más importantes del DS4 están; entrega de valor, administración de riesgos, administración de recursos, medición del desempeño y alineación estratégica. Cabe mencionar que la propuesta estará basada en su mayoría en este domino.

2.2.1.5 DS5 Garantizar la seguridad de los sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad. (COBIT 4.1, IT Governance Institute, 2007, p.117).

2.2.1.6 DS6 Identificar y asignar costos

La necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación de un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios. Un sistema equitativo de costos permite al negocio tomar decisiones más informadas respectos al uso de los servicios de TI. (COBIT 4.1, IT Governance Institute, 2007, p.121).

2.2.1.7 DS7 Educar y entrenar a los usuarios

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios. (COBIT 4.1, IT Governance Institute, 2007, p.125).

2.2.1.8 DS8 Administrar la mesa de servicio y los incidentes

Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de

una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo. (COBIT 4.1, IT Governance Institute, 2007, p.129).

2.2.1.9 DS9 Administrar la configuración

Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoria de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido. (COBIT 4.1, IT Governance Institute, 2007, p.133).

2.2.1.10 DS10 Administración de Problemas

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y

mejora la conveniencia y satisfacción del usuario. (COBIT 4.1, IT Governance Institute, 2007, p.137).

2.2.1.11 DS11 Administración de Datos

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio. (COBIT 4.1, IT Governance Institute, 2007, p.141).

2.2.1.12 DS12 Administración del Ambiente Físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal. (COBIT 4.1, IT Governance Institute, 2007, p.145).

2.2.1.13 DS13 Administración de Operaciones

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de

operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo del hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI. (COBIT 4.1, IT Governance Institute, 2007, p.149).

2.2.2 ITIL

Cuando se habla de Gestión de TI, existen muchas metodologías o buenas prácticas que ayudan a los gerentes de TI a brindarle la tranquilidad al negocio con respecto a este tema, una de estas metodologías es ITIL (IT Infrastructure Library, biblioteca de infraestructura de TI) la cual se puede definir como "**Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.**"(Héctor Acevedo, ITIL ¿Qué es y para qué sirve?, Magazcitum[Internet],2010, [citado el 10 Jun 2016], disponible en http://www.magazcitum.com.mx/?p=50) .Este paquete de mejores prácticas ayudarán en conjunto con otras metodologías como COBIT, a mejor los procesos relacionados con la gestión de servicios de las Instituciones Públicas, básicamente algunos de los temas importantes de ITIL es poder promover una gestión por procesos y especificar cuáles son los indicadores que podrían utilizar las empresas para administrar los servicios de TI, implementar roles y responsabilidad a sus colaboradores y promover una alineación con resto de la organización. Por su nivel

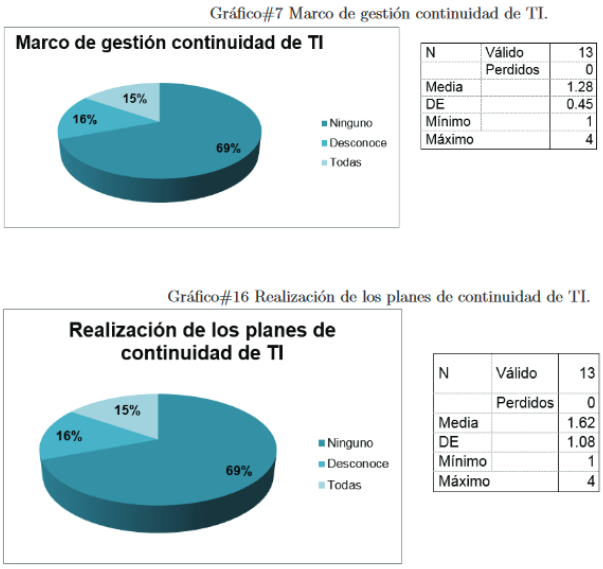
de empleo en otras Organizaciones a nivel Internacional ITIL se ha vuelto un estándar a nivel mundial.

2.3 Antecedentes de teorías o proyectos o de experiencias semejantes

En Costa Rica existen gran cantidad de Empresas Públicas que al igual que el Cuerpo de Bomberos, deben cumplir con las leyes del estado. En materia de las tecnologías de Información y en referencia al cumplimiento de las Normas Técnicas de la Contraloría General de la República; algunas de estas Instituciones ya realizaron o se encuentran ejecutando el proceso de continuidad y seguridad de la información que dictan estas normas. Una de ellas es el Ministerio de trabajo y seguridad Social de Costa Rica, según documento elaborado por Mora y Vargas que deja en evidencia la ejecución de este proceso y como resultados textualmente indican: "**Se realizó una encuesta para conocer sobre el plan de continuidad del departamento de TI en el MTSS, con el fin de conocer las políticas y procedimientos para soportar la continuidad de TI en sus servicios brindados a la institución y si utilizan el COBIT como requisito que tiene por parte del gobierno el MTSS; el estudio en el departamento de TI del MTSS, donde su mayoría es integrada por personal con un grado profesional técnico"** (Mora y Vargas, 2016, Continuidad de Servicio de TI en el Ministerio de Trabajo y Seguridad Social de Costa Rica, recuperado de http://bb9.ulacit.ac.cr/tesinas/publicaciones/041861.pdf , el 11/6/2016 a las 05:36

pm)**.** Un ejemplo de los resultados obtenidos en esta encuesta se adjunta a continuación de manera gráfica:

Figura 4 Resultados Obtenidos



Fuente: Tomado de Mora y Vargas (2016)

Otra de las entidades que han ejecutado este proceso es la Refinadora Costarricense de Petróleo (Recope), según su Política de Continuidad de Negocio y Seguridad de la Información, la misma aprobada por la junta directiva el 29 de Abril del 2015 cuyo objetivo indica: **"Establecer la posición de RECOPE frente a la disponibilidad, integridad y confidencialidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales."** (Recope, 2015, Política de Continuidad del negocio y Política de Seguridad de la Información, recuperado de https://www.recope.go.cr/wp-

content/uploads/2015/05/Politicas_de_continuidad_y_seguridad_de_la_Informacion2.pdf, el 11/6/2016 a las 06: 20 pm). Con esta política RECOPE se compromete a que todos los procesos críticos del negocio operen de manera ininterrumpida, reconociendo su valor estratégico en la gestión del negocio.

La Universidad de Costa Rica (UCR), es otra de las entidades públicas que no se ha quedado atrás con la ejecución de normativas para la seguridad y continuidad de la información pues, en el 2015 se publica la resolución de las Directrices de seguridad de la Información de la Universidad de Costa Rica, cuya solicitud de aprobación fue enviada a la rectoría por el comité de Gerencial de Informática. En esta directriz se indica: **"…la Institución reconoce la importancia de adoptar un conjunto de directrices técnicas de seguridad de información, que además de tener como premisa básica la protección de la información perteneciente a la Universidad en su custodia, constituye el fundamento de la cultura que en materia de seguridad de la información desea establecer, reforzar, implementar e incorporar en su diario quehacer, con miras no sólo a lograr un manejo eficiente de sus recursos informáticos, acorde con el interés público y en estricta concordancia con el ordenamiento jurídico costarricense, sino, sobre todo, a propiciar la eficiencia en las labores y el mejoramiento constante de los servicios que le dan fundamento a la Institución."** (Universidad de Costa Rica, la Gaceta Universitaria. Directrices de seguridad de la información de la Universidad de Costa Rica. Recuperado de http://www.cu.ucr.ac.cr/uploads/tx_ucruniversitycouncildatabases/officialgazette/2015/a07-2015.pdf, el 11/6/2016 a las 07: 03 pm) Es por esto que queda claro que el

tema de la seguridad y continuidad de los servicios de TI son de aplicación obligatoria y que las entidades públicas, están trabajando por cumplir estas normativas y estar a derecho con las leyes dictadas por el Gobierno de Costa Rica; además de asegurarse para ellas la continuidad del negocio al que se dedican.

CAPÍTULO III MARCO METODOLÓGICO

3.1 Tipo de investigación:

3.1.1 Finalidad

La finalidad de este proyecto es aplicada, ya que lo que se pretende es crear un plan de continuidad de servicios para así cumplir con las normas establecidas por el gobierno y evitar sanciones a la organización o pérdidas económicas importantes. Con este plan de continuidad se pretende reducir el impacto del riesgo de la pérdida del servicio de bases de datos ofrecido por la Institución.

3.1.2 Dimensión Temporal

Este proyecto es longitudinal, ya que se deben ejecutar varios pasos para poder cumplir el objetivo del mismo. Entre ellos se debe realizar el diagnóstico de los procesos críticos de bases de datos, estos deben ser analizados para encontrar puntos de mejora y así poder crear el plan de continuidad. Proponer luego la ejecución del plan piloto, ya que esto es un proceso continúo de mejora donde las políticas y controles establecidos para la continuidad del servicio de bases de datos deben ser revisados periódicamente y que los riesgos sean mínimos.

3.1.3 Marco

Este proyecto se llevará a cabo en la Unidad de Tecnologías de Información y Comunicación del Benemérito Cuerpo de Bomberos de Costa Rica, en el área de Servicios técnicos donde son administradas las bases de datos, específicamente en el proceso de Continuidad y Seguridad del servicio de base de datos que brinda esta unidad.

3.1.4 Condición en la que se hace

La investigación de este proyecto será de campo, ya que el diagnóstico de la situación actual se realizará en la empresa, departamento y proceso en el cual se desea desarrollar el proyecto.

3.1.5 Carácter

Este proyecto tiene diferentes tipos de carácter entre ellos:

- Causal: Debido a que existen causas como inexistencia de un plan de continuidad, modelos de gestión de servicios no alineados a las mejores prácticas y falta de personal capacitado para realizar estos procesos. Además esto genera efectos negativos como la interrupción de los servicios, impacto en los costos de la organización y tiempos indefinidos para la recuperación de los servicios.
- Exploratorio: Este es un proyecto nuevo en el tema de continuidad de servicios tecnológicos para el Cuerpo de Bomberos, pues no se encuentra implementado un plan de continuidad y debido a una serie de normativas que deben cumplirse es necesaria su implementación.
- Prospectivo: Con la ayuda de este proyecto los jerarcas pueden tomar decisiones como cambios en políticas, manuales y procesos que ayuden en un futuro a evitar interrupciones en los servicios o a disminuir los tiempos de recuperación, evitando consecuencias de tipo tecnológico, económico, entre otros, a la institución.

- Participativos: Se necesita de un conjunto de personas para poder llevar a cabo parte de este proyecto como por ejemplo la capacitación encargados del proceso de continuidad de los servicios de bases de datos.
- Descriptivo-analítico: En este proyecto se deberá analizar la normativa que dicta la Contraloría General de la República, así como los procesos y políticas que rigen en la institución, para sí determinar que se debe cambiar, ajustar o implementar.

3.1.6 Naturaleza

La naturaleza de este proyecto es mixta, pues se analizarán datos tanto cualitativos como cuantitativos. A nivel cualitativo se estará analizando la información de procesos, procedimientos, estado actual, vulnerabilidades entre otras. A nivel cuantitativo se analizarán datos como tiempos de recuperación, tiempos de aceptación del negocio de estar sin el servicio, además de analizar y calcular espacio en disco de servidores para Bases de datos.

3.2 Sujetos y fuentes de información:

3.2.1 Sujetos

Para este trabajo se pretende consultar a 3 personas de la institución, las cuales conocen muy bien diferentes procesos de bases de datos, que estarán involucrados directamente en este proyecto. El administrador de bases de datos que cuenta con el conocimiento de cómo está el negocio en materia de Bases de Datos y los procesos que se realizan, la encargada de control interno de TIC, que cuenta con

el conocimiento y la capacitación sobre la implementación de normas técnicas, la creación de procedimientos y políticas para esta unidad, la directora de la unidad de TIC, a ella se le estará consultando, porque conoce de primera mano la situación actual del negocio, en referencia a las tecnologías y es la encargada de velar por que la unidad cumpla con las normativas dictadas por la Contraloría General de la República.

3.2.2 Fuentes

Para el desarrollo de este proyecto se consultaran varias fuentes de información, entre ellas; las Normas Técnicas de la Contraloría General de la República, ya que estas son de acatamiento obligatorio y mencionan que se debe hacer para gestionar de una forma adecuada las Tecnologías de Información de las entidades públicas. Otro de los documentos son los manuales de COBIT 4.1 e ITIL en su versión 3, estos manuales indican como debe hacerse para mantener una buena gestión de las tecnologías, así como las mejores prácticas que deben adaptarse a los procesos para la continuidad de los servicios. El Marco SEVRI es un documento muy importante a tomar en cuenta, pues se refiere al Sistema Específico de Valoración de Riesgos Institucionales; cuyo objetivo es encontrar información que ayude a tomar decisiones, para buscar niveles de riesgo aceptables y así cumplir con los objetivos de la Institución.

3.3 Técnicas y Herramientas

3.3.1 Técnicas de consulta

Una de las herramientas utilizadas que se aplicará para realizar consultas en este proyecto, es la entrevista, esta tiene como definición "**acto de comunicación oral que se establece entre dos o más personas (el entrevistador y el entrevistado o los entrevistados) con el fin de obtener una información o una opinión, o bien para conocer la personalidad de alguien."**(Romeo y Domenech, Materiales de lengua y literatura, http://www.materialesdelengua.org/EXPERIENCIAS/PRENSA/f_entrevista_web.pdf, recuperado el 18/6/2016 a las 3:18 pm).

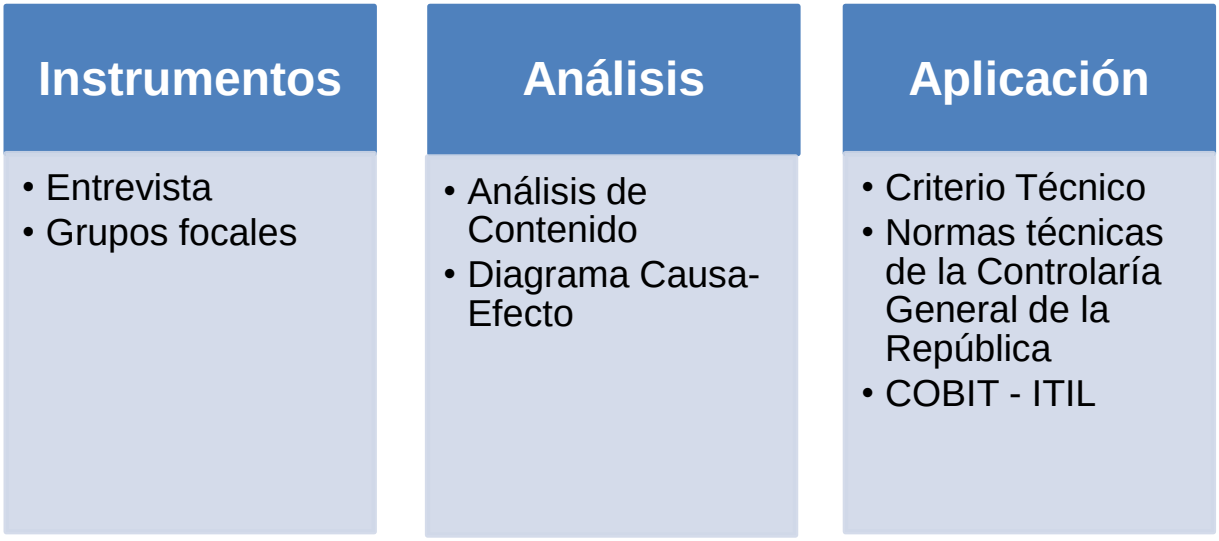
Para las entrevistas que se realicen en este proyecto se definirán una serie de preguntas abiertas, las cuales irán relacionadas al tema que se desea abordar con el entrevistado. También se estará utilizando los grupos focales para obtener información que ayude a cumplir con el objetivo de este proyecto. Un grupo focal se define **" entrevistas de grupo, donde un moderador guía una entrevista colectiva durante la cual un pequeño grupo de personas discute en torno a las características y las dimensiones del tema propuesto para la discusión."** (http://biblioteca.uahurtado.cl/ujah/856/txtcompleto/txt105091.pdf, Grupos focales, técnicas de Investigación cualitativa, Mella, 2000). Esta técnica ayudará a aclarar información sobre la continuidad del servicio de bases de datos, ya que al estar discutiendo varias personas sobre el tema, se podrán tomar decisiones importantes que ayuden con el avance de la investigación y cumplir con el objetivo final.

3.3.2 Técnicas de análisis

Para este trabajo se utilizará el análisis de contenido, debido a que se tomarán las entrevistas y se analizará la información recolectada referente al proceso de continuidad de los servicios de bases de datos y tener un panorama más amplio de la ejecución del mismo en la unidad de TIC. Esto ayudará a generar criterio para la toma de decisiones y diseñar el plan de continuidad de bases de datos de la forma más adecuada, guiado a las normas técnicas y a las mejores prácticas.

3.4 Diseño de Investigación

Figura 5 Diseño de Investigación



Fuente: Elaboración Propia (2016)

- **Instrumentos:** Se utilizarán la entrevista y grupos focales, con dichos instrumentos se recolectará la información de la problemática existente con respecto a la continuidad de los servicios de bases datos SQL del Benemérito Cuerpo de Bomberos de Costa Rica.
- **Análisis:** Se ejecutará un análisis de contenido el cual ayudará al estudio de la información recolectada en las entrevistas y los grupos focales, además el diagrama causa–efecto detallará las vulnerabilidades encontradas en la problemática así como las consecuencias.
- **Aplicación:** Con el análisis realizado y el criterio técnico, se desarrollará el plan de continuidad de bases de datos, según lo establecido en las Normas Técnicas de la Controlaría General de la República, así como la normalización de las mejores prácticas COBIT e ITIL.

CAPÍTULO IV DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

En este capítulo se enfocará en describir el estado actual de los procesos de las operaciones de recuperación de la información de las bases de datos del BCBCR en una eventual suspensión del servicio; para esto y de acuerdo a lo diagnosticado se propondrán estrategias correctivas basándose en los conceptos de administración de la continuidad del negocio, establecida por las buenas prácticas existentes (ITIL, COBIT) y el marco legal establecido por la Contraloría General de la República.

Como primer paso del diagnóstico se realizó una entrevista al encargado de las bases de datos de la unidad de TIC del Cuerpo de Bomberos, de aquí se desprenden actividades básicas para el diagnóstico como son evaluación de riesgos, análisis de impactos y la definición de estrategias a seguir.

4.1 Diagnóstico administrativo u operativo

De acuerdo a las respuestas de la entrevista realizada, según cuestionario Anexo (ver Anexo #1), al encargado de administrar las bases de datos de TIC del Cuerpo de Bomberos de Costa Rica, se obtuvieron los siguientes resultados:

4.1.1 Modelo de Gestión de bases de datos

El modelo de gestión es un plan estratégico que define las tácticas a seguir en cuanto a sistemas de información, servicios tecnológicos y servicios de continuidad, que garanticen el valor estratégico de la capacidad y la inversión en tecnología realizada por el Cuerpo de Bomberos de Costa Rica, dicho modelo de gestión incluye la estrategia organizacional y las necesidades de TIC.

De acuerdo a esto se ha determinado que existe muy poco en cuanto a lo relacionado a una estrategia de gestión acorde y alineada a las mejores prácticas. Dentro de esta carencia y como parte del modelo de gestión se llega a la conclusión de que no hay un plan que permita dar continuidad a una eventual suspensión de los servicios de bases de datos y que no perjudiquen en gran volumen el proceso y el trabajo cotidiano que los sistemas necesitan para su desarrollo habitual.

4.1.2 Procedimientos

Actualmente las practicas utilizadas por la Unidad de TIC del Benemérito Cuerpo De Bomberos de Costa Rica, han estado centralizadas en el conocimiento y experiencia de una sola persona en temas de garantizar los respaldos, optimizaciones y cualquier ejecución que se requiera en las bases de datos. Estas prácticas no dejan registro ni documentación que permita establecer procedimientos en caso de una emergencia relacionada a la continuidad de servicios de bases de datos. Es por esta razón que se han venido realizando cambios en el Cuerpo de Bomberos de Costa Rica para poder alcanzar lo dictado por la Contraloría General de la República, la unidad de TIC de Bomberos ha empezado el análisis para la creación de diferentes procedimientos relacionados al servicio de base de datos, como por ejemplo, procedimientos para la solicitud de objetos de bases de datos, restauración de respaldos de bases de datos, ejecución de pases de bases de datos, creación, actualización o retiro de usuarios de bases de datos. Sin embargo no existe un procedimiento que indique los pasos a seguir al enfrentarse a una falta de

los servicios orientados a las bases de datos (configuración de bases de datos, servidores, reglamentación y seguridad de accesos interno o externos, entre otros).

4.1.3 Plan de mantenimiento de Infraestructura

Como parte de los cambios mencionados anteriormente, existe un plan de mantenimiento preventivo de la infraestructura general en cuanto a los servicios de TIC, en el tema de bases de datos, este plan describe las tareas a realizar para el mantenimiento básico de las bases de datos, tal como lo muestra el siguiente cuadro:

Cuadro 1 Plan actual de mantenimiento de infraestructura

Monitoreo de las Bases de Datos	**Fragmentación de Índices** **Espacio en disco** **Uso de CPU, Memoria RAM** **Lecturas y Escrituras en disco** **Log's de Base de Datos**
Monitoreo de las Bases de Datos	Integridad referencial
Base de Datos	Respaldo de las bases de datos Core
Base de Datos	Restauración de base de datos
Base de Datos	Limpieza de Log's Transaccional
Base de Datos	Actualización de contraseñas de usuarios de base de datos

Fuente: Benemérito Cuerpo de Bomberos de Costa Rica (2016).

Como se puede observar del cuadro anterior, el plan de infraestructura no toma en cuenta el o los procedimientos a seguir en eventuales caídas y restauraciones de servidores y bases de datos.

4.1.4 Disponibilidad del personal de bases de datos

Otro de los puntos importantes es la participación activa de los funcionarios involucrados dentro del plan de continuidad, en este caso el personal disponible actualmente para la atención de problemas y en una eventual caída de bases de datos, tiene una limitada disponibilidad de tiempo que se enmarca en la jornada laboral actual, la cual es de Lunes a Viernes de 7:45 am a 4:05 pm, además solamente 2 personas tienen la responsabilidad sobre lo planteado; perjudicando así una atención adecuada a los problemas que se puedan suscitar fuera de esas horas.

Además de los funcionarios de planta, el departamento de TIC cuenta con colaboradores externos, los cuales, pueden suministrar ayuda en caso de presentarse un incidente significativo en la continuidad de los servicios de bases datos, para lo cual se debe disponer de la mejor comunicación posible para su contacto.

4.1.5 Presupuesto para ejecución del proyecto

De acuerdo y como se vayan presentando las necesidades, tanto para la compra de software y equipo para una implementación de un plan de continuidad adecuado, la unidad de TIC cuenta con el presupuesto disponible para este proceso, por disposición administrativa.

4.2 Diagnóstico Técnico

En este apartado se determinan aspecto técnicos de relevancia, los cuales ayudarán a seleccionar las mejores prácticas a implementar para obtener el plan de

continuidad de bases de datos del Benemérito Cuerpo de Bomberos y así cumplir con la ley dictada por la Contraloría General de la República.

4.2.1 Infraestructura Física

La unidad de TIC del Cuerpo de Bomberos cuenta con servidores tanto físicos como virtuales. Los servidores físicos son 7 y se encuentran en modo failover clúster (conmutación por error), el cual consiste en un grupo de estos servidores que realizan tareas en conjunto para mantener en alta disponibilidad los servidores virtuales que se encuentran aquí alojados, esto quiere decir que si un servidor físico falla, otro servidor puede asumir la carga y así mantener activos los servidores virtuales sin ningún tiempo de inactividad, ayudando a mantener los servicios y aplicaciones disponibles. Estos servidores físicos son servidores blade marca HP, con 2 procesadores xenon de 2.50 GHZ, cuentan con una memoria RAM de 128 GB cada uno y sistema operativo Windows Server 2012 R2 Datacenter de 64 bits.

4.2.1.1 Servidores de bases de datos

A nivel de bases de datos existen dos servidores, los mismos son nodos virtualizados en hyper-v herramienta de virtualización de Microsoft, cada uno cuenta con sistema operativo Windows server 2012 estándar, el servidor principal tiene 4 procesadores virtuales mientras que el secundario cuenta con 8 procesadores.

De estos dos servidores de bases de datos, uno de ellos es el activo y el otro tiene la función de replicar por medio de log’s la información de las bases de datos y trabajar como un servidor pasivo, ambos servidores cuentan con 5 particiones en

donde se almacenan las bases de datos, los archivos logs, respaldos, entre otros. Además cuentan con 12 GB de memoria cada uno.

4.2.1.2 Bases de datos

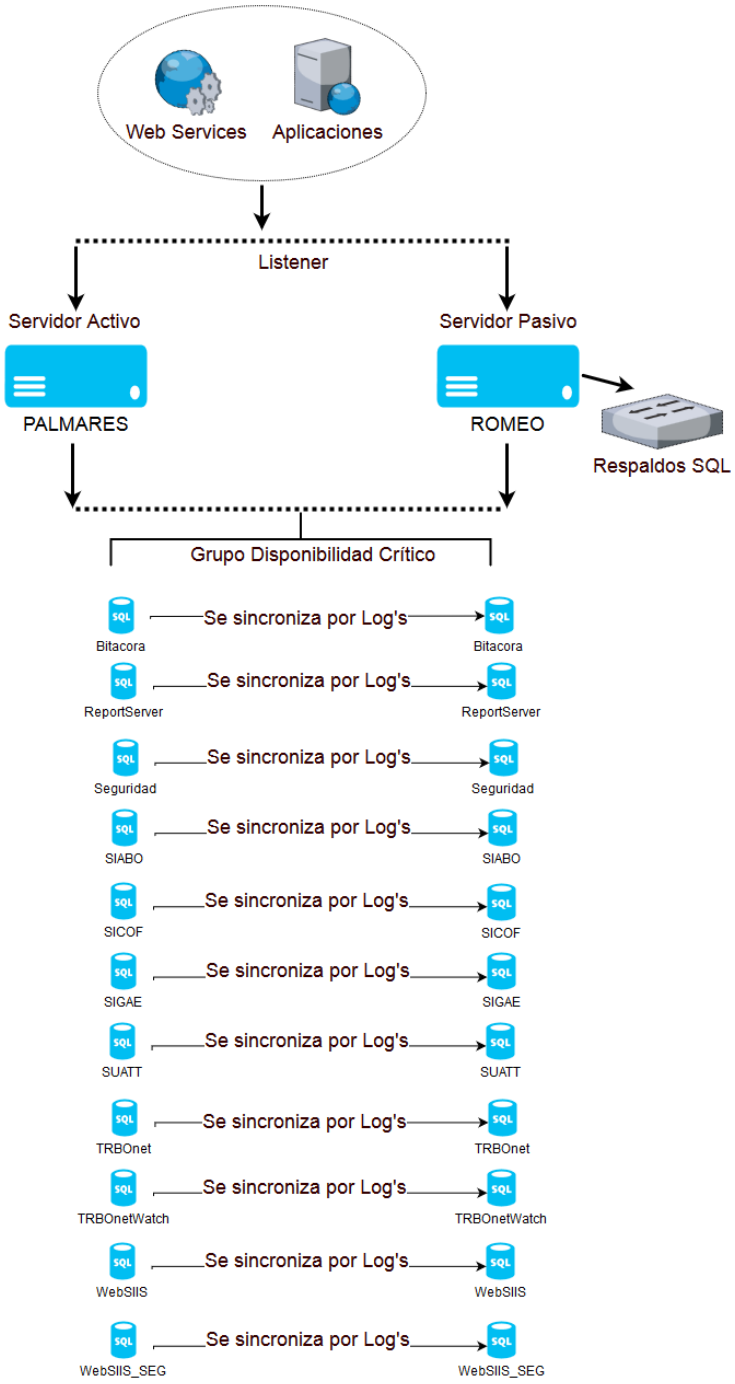
La unidad de TIC del Cuerpo de Bomberos de Costa Rica, administra 16 bases de datos SQL SERVER, las cuales se encuentran compartidas en el servidor principal y son replicadas al servidor secundario mediante log's, donde se realizan las ejecuciones de los respaldos; estas bases de datos son administradas por dos usuarios uno principal y uno secundario.

Para las configuraciones de las bases de datos no existe un estándar, solamente un manual para realizar la instalación de un SQL Server.

Las bases de datos se encuentran clasificadas por dos grupos de criticidad, el grupo critico en donde se almacenan las bases de datos con la información más importante para la institución y el grupo no critico donde se encuentran las bases de datos que si bien no dejan de ser importantes no requieren la atención primordial en el caso de una suspensión de los servicios de bases de datos.

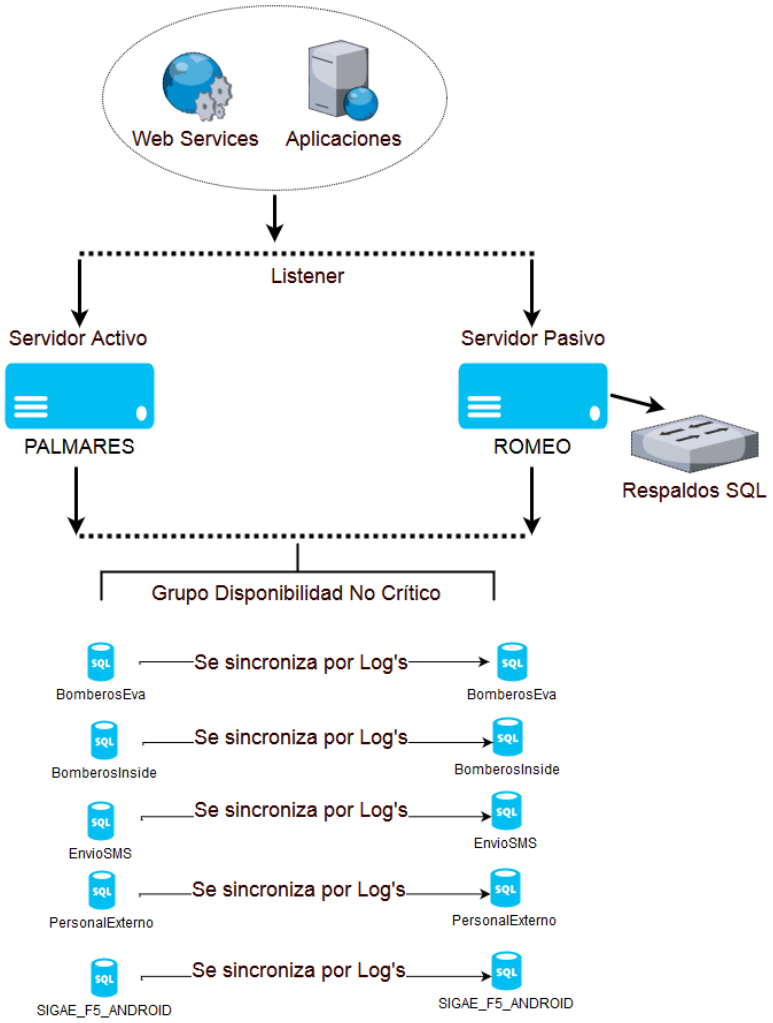
Actualmente existe un inventario de los componentes de bases de datos como servidores, instancias, memoria, discos, Sistema operativo, pero no existe un inventario completo que incluya la estructura de las bases de datos como: tablas, Jobs, procedimientos almacenados, alertas, alarmas, almacenadas o programadas a nivel de base de datos.

Figura 6 Diagrama bases de datos criticas



Fuente: Benemérito Cuerpo de Bomberos de Costa Rica (2016).

Figura 7 Diagrama bases de datos NO criticas



Fuente: Benemérito Cuerpo de Bomberos de Costa Rica (2016).

4.2.1.3 Seguridad de bases de datos

Para una continuidad en los servicios de bases datos, la seguridad de la información y quien la accede tiene una importancia relevante, ya que ayuda a controlar quienes pueden modificar, consultar o eliminar la información almacenada en las bases de datos. A nivel de servidores se cuenta con el antivirus McAfee, el cual previene cualquier ataque que pueda recibir el servidor de bases de datos y así

evitar la sustracción de la información, daño a las bases datos o a los mismos servidores por parte de personas externas a la institución, además, la unidad de TIC utiliza la seguridad con autenticación de Windows con Kerberos o la propia de SQL SERVER, que guarda los log's que registran las modificaciones realizadas por usuarios internos.

4.2.2 Administración técnica actual de base de datos

En la administración de bases de datos pueden existir riesgos que lleven a una caída de las bases de datos, entre los puntos importantes a dar seguimiento y que puedan afectar la continuidad de los servicios están:

4.2.2.1 Respaldos

En bases de datos muchas veces no se piensa en la criticidad de la información, siendo estos vitales para la continuidad de los servicios y para la organización; es por esto que los respaldos de la información contenida en la base de datos son primordiales. Así se evita encontrar respaldos muy viejos, respaldos que fallaron que nunca se probaron, de que no existía el respaldo o que estos estaban incompletos o bien que el respaldo estaba en el mismo disco o servidor que fallo, por ejemplo.

En la unidad de TIC del Cuerpo de Bomberos, el encargado de la administración de bases de datos realiza respaldos completos diariamente y cada 3 horas los respaldos diferenciales, estos son las copias de todos los datos que hayan cambiado desde el último respaldo completo y de los log's transaccionales que son

aquellas tablas de la base de datos en donde todos los cambios a los datos son registrados, ósea un histórico de los cambios a los datos.

4.2.2.2 Restauraciones

Uno de los problemas más importantes al momento de restaurar una base de datos es la integridad de la información, por lo que el punto anterior de respaldos es el que va a dar la pauta a la restauración en caso de una suspensión de servicios por cualquier motivo, por ejemplo, la base de datos se corrompió debido a una falla de hardware, el respaldo logro salvar el 75% de la información, se debe definir un procedimiento alterno para recuperar la información al 100%.

Según el administrador de bases de datos de Bomberos, se establece que las restauraciones a los respaldos de las bases de datos se están efectuando cada mes a las bases de datos críticas y cada 4 meses a las bases de datos que no se consideran críticas. Además, en la Unidad de TIC no se han realizado pruebas donde se pueda evidenciar el tiempo y coste de una recuperación de bases de datos.

4.2.2.3 Monitoreo

El monitoreo constante de los componentes de las bases de datos, ayudan a identificar cualquier inconveniente en tiempo real, esto ayuda a que si alguno de estos componentes presenta algún error, todavía se esté a tiempo de corregir antes de presentarse una caída total del servicio de base de datos. Actualmente la unidad de TIC cuenta con herramientas de monitoreo que indican el comportamiento inmediato de los componentes que conforman el servicio de bases de datos, se

cuenta con SQL check de Idera, la cual es una herramienta libre y que permite monitorear un máximo de 20 parámetros de rendimiento clave, creando estadísticas llamadas “heartbeat” en diferentes intervalos y un dashboard de Griedshield en el cual se monitorean los servidores, ping, partición de discos, CPU, memoria y servicios importantes.

Figura 8 Monitoreo de servidor de bases de datos actuales

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Servidor_Palmares	CPU Load	OK	02-09-2016 21:25:55	5d 11h 46m 25s	1/3	OK CPU Load 12.25%
	DHCP Client	OK	02-09-2016 21:26:22	267d 8h 59m 5s	1/3	1 services active (matching "DHCP Client") : OK
	DNS Client	OK	02-09-2016 21:24:49	131d 13h 14m 28s	1/3	1 services active (matching "DNS Client") : OK
	Device Name	OK	02-09-2016 21:25:17	492d 6h 26m 28s	1/3	Hostname: PALMARES.bomberos.go.cr
	Disk Usage C	OK	02-09-2016 21:25:45	121d 14h 24m 34s	1/3	OK: Mount point: c: total:49.66 Gb - used:27.34 Gb (55%) - free:22.32 Gb (45%)
	Disk Usage E	OK	02-09-2016 21:26:11	339d 15h 43m 16s	1/3	OK: Mount point: e: total:100.00 Gb - used:19.54 Gb (20%) - free:80.45 Gb (80%)
	Disk Usage G	OK	02-09-2016 21:24:56	267d 8h 59m 28s	1/3	OK: Mount point: g: total:100.00 Gb - used:33.36 Gb (33%) - free:66.64 Gb (67%)
	Disk Usage H	OK	02-09-2016 21:25:06	267d 8h 59m 4s	1/3	OK: Mount point: h: total:49.00 Gb - used:4.88 Gb (10%) - free:44.12 Gb (90%)
	Disk Usage L	OK	02-09-2016 21:25:33	121d 14h 24m 41s	1/3	OK: Mount point: l: total:200.00 Gb - used:47.49 Gb (24%) - free:152.51 Gb (76%)
	Disk Usage R	OK	02-09-2016 21:26:01	218d 9h 52m 57s	1/3	OK: Mount point: r: total:25.00 Gb - used:0.83 Gb (3%) - free:24.17 Gb (97%)
	Group Policy Client	OK	02-09-2016 21:24:28	267d 8h 57m 40s	1/3	1 services active (matching "Group Policy Client") : OK
	Hyper-V Data Exchange Service	OK	02-09-2016 21:25:55	267d 8h 57m 5s	1/3	1 services active (matching "Hyper-V Data Exchange Service") : OK
	Hyper-V Guest Shutdown Service	OK	02-09-2016 21:26:22	267d 8h 56m 35s	1/3	1 services active (matching "Hyper-V Guest Shutdown Service") : OK
	Hyper-V Heartbeat Service	OK	02-09-2016 21:24:49	131d 13h 14m 28s	1/3	1 services active (matching "Hyper-V Heartbeat Service") : OK
	Hyper-V Volume Shadow Copy Requestor	OK	02-09-2016 21:25:17	82d 11h 22m 21s	1/3	1 services active (matching "Hyper-V Volume Shadow Copy Requestor") : OK
	McAfee Agent Service	OK	02-09-2016 21:25:45	121d 14h 24m 29s	1/3	1 services active (matching "McAfee Agent Service") : OK
	McAfee McShield	OK	02-09-2016 21:26:12	82d 11h 22m 31s	1/3	1 services active (matching "McAfee McShield") : OK
	McAfee Task Manager	OK	02-09-2016 21:24:56	108d 5h 8m 8s	1/3	1 services active (matching "McAfee Task Manager") : OK
	McAfee Validation Trust Protection Service	OK	02-09-2016 21:25:06	82d 11h 22m 23s	1/3	1 services active (matching "McAfee Validation Trust Protection Service") : OK
	Memory Usage	OK	02-09-2016 21:25:35	121d 14h 24m 41s	1/3	OK: Mount point: Physical Memory total:12.00 Gb - used:10.82 Gb (90%) - free:1.18 Gb (10%)
	Netlogon	OK	02-09-2016 21:26:01	82d 11h 22m 31s	1/3	1 services active (matching "Netlogon") : OK
	Network Store Interface Service	OK	02-09-2016 21:24:28	267d 8h 59m 35s	1/3	1 services active (matching "Network Store Interface Service") : OK
	SNMP Service	OK	02-09-2016 21:25:55	26d 11h 25m 6s	1/3	BULKSNMP_RETRIEVE OK - SNMP trees: .1.3.6.1.2.1.1.3.0
	SQL Full-text Filter Daemon Launcher MSSQLSERVER	OK	02-09-2016 21:26:22	121d 15h 12m 25s	1/3	1 services active (matching "SQL Full-text Filter Daemon Launcher (MSSQLSERVER)") : OK
	SQL Server Agent MSSQLSERVER	OK	02-09-2016 21:24:50	121d 14h 24m 19s	1/3	1 services active (matching "SQL Server Agent (MSSQLSERVER)") : OK
	SQL Server MSSQLSERVER	OK	02-09-2016 21:25:17	82d 11h 22m 23s	1/3	1 services active (matching "SQL Server (MSSQLSERVER)") : OK
	System Uptime	OK	02-09-2016 21:25:45	121d 14h 24m 33s	1/3	UpTime OK - Timeticks: (1050637000) 121 days, 14:26:10.00
	Virtual Memory Usage	OK	02-09-2016 21:26:12	346d 15h 5m 9s	1/3	OK: Mount point: Virtual Memory total:13.81 Gb - used:10.93 Gb (79%) - free:2.88 Gb (21%)
	ping	OK	02-09-2016 21:24:56	494d 10h 22m 54s	1/3	OK - 10.0.200.73: rta 1.977ms, lost 0%

Fuente: Benemérito Cuerpo de Bomberos de Costa Rica (2016)

.

4.2.2.4 Sitio Alterno de procesamiento de datos

La importancia de contar con un sitio alterno de procesamiento de datos es centralizar todos los recursos informáticos para proveer toda la tecnología necesaria para la operativa diaria. En lo que respecta al almacenamiento auxiliar en las bases de datos el sitio alterno debe tener y estar preparado para recibir la información actualizada y a la vez tener esa información disponible en casos de emergencia.

Actualmente la unidad de TIC cuenta con un sitio alterno pero no se ha realizado ninguna implementación a nivel de bases de datos.

4.2.3 Personal Capacitado

La capacitación del personal involucrado en el mantenimiento y la continuidad del servicio de bases de datos, es un punto primordial para mantener la atención del día a día de los sistemas que utilizan la información contenida en las bases de datos y que además este personal sea capaz de atender los incidentes que puedan afectar este servicio.

Actualmente únicamente existen dos personas que dan soporte a las bases de datos y una de ellas no está al 100% de emitir un criterio técnico para resolver casos específicos que pueden suceder, el segundo recurso se encuentra en un 30% de capacitación para la atención oportuna en caso de una caída de las bases de datos.

4.3 Brechas y Conclusiones del diagnóstico

De acuerdo a la investigación realizada se han arrojado diferencias entre lo que actualmente tiene el servicio de soporte de bases de datos del Cuerpo de Bomberos, con respecto a lo que establece la ley, específicamente lo indicado por la Contraloría General de la República en su apartado de la continuidad de servicios de TI y con respecto a las mejores prácticas de cómo llevar a buen término un plan de continuidad de servicios de las bases de datos. De lo percibido en los diagnósticos anteriores existe un porcentaje elevado de riesgo en cuanto a un efectivo y adecuado método de solución a problemas que se puedan presentar en una interrupción de los servicios de base de datos, tanto en la parte operativa como en la parte técnica y administrativa. Es por esto que se hace necesario y urgente realizar el análisis cualitativo y cuantitativo de los procesos que se deben establecer para que el impacto de un interrupción de servicios sea mínimo y que afecte de la menor manera posible el trabajo diario en cuanto a disponibilidad de datos que utilizan los diferentes sistemas del Cuerpo Bomberos.

El plan de continuidad de servicios de TIC debe estar alineado con un plan general de continuidad para asegurar la consistencia de la propuesta que se presentará.

En primer término las diferencias encontradas y que se desarrollarán en este punto, son vulnerabilidades que deben corregir y que se convertirán en amenazas potenciales a la continuidad de servicios de bases de datos.

Como primera diferencia, se encontró con que el Benemérito Cuerpo de Bomberos de Costa Rica no cuenta con un plan de continuidad de servicio de bases de datos, esto

lógicamente afectaría los servicios en caso de una emergencia donde los datos no estén disponibles.

Se deduce a la respuesta de la definición e identificación de los procesos relacionados a la continuidad del servicio de bases de datos, que estos no están plenamente identificados y COBIT dentro de su estrategia recomienda la identificación de los procesos y recursos de TI que deben ser recuperados para la continuidad de los servicios en caso de una suspensión de los mismos, cualquiera que sea el motivo.

Como tercer punto se puede notar que los modelos de gestión son incompletos por lo que es necesario establecer y definir un modelo de gestión de la continuidad de servicios de bases de datos acorde a lo establecido por ITIL V3, en su apartado Gestión de la continuidad del servicio, en cuanto a seguimiento y control de los datos que dice**: "Controlar riesgos que podrían impactar los servicios de TI y que se ocupa que el administrador siempre pueda proveer un mínimo nivel del servicio propuesto, reduciendo el riesgo de eventos desastrosos y planificando la recuperación de los servicios."** (http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti.php, Osiatis S.A, Itilv3, recuperado el 14/8/2016 a las 02:50pm).

En cuanto al personal disponible, su tiempo, su desempeño y capacitación, se encuentran inconsistencias entre lo investigado y con lo que se debe implementar, para que el personal este no solamente capacitado sino, tenga la disponibilidad necesaria e inmediata en caso de una emergencia, que altere la continuidad de servicios de bases de datos, como lo indica el punto DS3 de COBITv4.1 administrar el desempeño y la capacidad del personal. Además el DS13 Administración de operaciones, indica que se

debe garantizar que el personal este familiarizado con las tareas de operación relativas a ellos. En la investigación saltan resultados de que solo una persona está al 100% de la capacidad en caso de una eventualidad, lo cual forma dependencia y aumenta el riesgo en caso de que esta no esté disponible por razones extraordinarias como lo son incapacidad y vacaciones.

En el punto relacionado a la coordinación con colaboradores externos en donde se indica que por medio de una llamada telefónica o de forma remota se puede asistir en algún problema relacionado con la continuidad de los servicios, se debe analizar profundamente lo que COBIT en su dominio DS2 indica, Administrar los servicios de terceros que establece en donde se deben definir claramente los roles, responsabilidades y expectativas en los acuerdos con ellos, así como, llevar a cabo una revisión y monitoreo de la efectividad, cumplimiento, disponibilidad y confiabilidad de los mismos para accesar no solamente vía teléfono o remoto, sino para realizar la atención al posible problema presentado en el momento que se necesite.

Dentro de los procesos obligatorios del mantenimiento y continuidad de los servicios se establecen los respaldos de la información contenida en las bases de datos, de aquí se desprende que se hacen diariamente y de forma separada las actualizaciones y los históricos. Para los respaldos se tiene el sitio alterno el Datacenter del Instituto Costarricense de Electricidad (ICE), ubicado el sector del Guarco de Cartago. Este punto debe satisfacer que se cumpla con el requerimiento de asegurar el mínimo impacto de los servicios en caso de una interrupción de los mismos, por lo que debe cumplir con las soluciones automatizadas desarrolladas de mantenimiento y prueba de los planes de continuidad que establece el DS4.9 almacenamiento de

respaldos fuera de las instalaciones, con respecto a almacenar respaldos fuera de las instalaciones de la entidad.

Otro de los puntos importantes y que no se deben quedar por fuera es la elaboración de pruebas al plan de continuidad. Actualmente no existe un ambiente de pruebas en el cual podamos medir la capacidad física y de almacenamiento en los servidores, por lo que en un eventual corte de servicios no se tiene los tiempos establecidos para una recuperación de esos servicios, así como pruebas de estrés a los servidores y a los sistemas, que son los que al final manipulan los datos. Para esto se debe ajustar al punto DS4.5 Pruebas del plan de continuidad de TI.

Figura 9 Brechas o conclusiones

Situación Actual	Brechas	Situación Deseada
•No existe modelo de Gestión por lo tanto tampoco un plan de continuidad de servicios. •Disponibilidad de personal limitada a tiempo laboral. •Comunicación limitada con colaboradores externos en caso de emergencia. •Se cuenta con un sitio alterno pero no se ha realizado una implementación a nivel de bases de datos. •Existe solamente una persona con la capacitación adecuada y criterio técnico para resolver las eventualiades. •Las restauraciones de los reslpaldos de bases de datos se estan realizando en tiempos muy distantes. •El modelo de seguridad de aseccos indebidos a las bases de datos, se enfoca únicamente a herramientas de windows o propias de SQL Server.En herramientas de monitoreo se cuenta con una herramienta de SQL y de adquisición gratuita. • No existe un inventario completo de los componentes propios de una base de datos (Procedimientos almacenados, triggers ,entre otros). •No se cuenta con un ambiente de pruebas que pueda evidenciar el tiempo y coste de una recuperación de las bases de datos.	•Se requiere establecer un flujo de procesos que permita crear un adecuado modelo de gestión que incluya el procedimiento adecuado para establecer el plan de continuidad de servicios. •Se require tener dentro del plan de continuidad personal involucrado a la atención de problemas fuera del horario laboral. •Se requiere tener un medio mas eficaz de comunicación con los colaboradores externos en caso de emergencia. •Se necesita implementar un plan de recuperación y actualización de bases de datos desde el sitio alterno. •Se necesita una adecuada capacitación para eventuales problemas de continuidad de servicio en las bases de datos. •Se requiere elaborar dentro del plan una forma mas ágil y a menor tiempo en cuanto a la restauración de las bases de datos. •Se requiere estudiar y tomar en cuenta la adquisición de herramientas licenciadas para el monitoreo y seguimiento del comportamiento de bases de datos.(Estudio de Mercado) • Es necesario tener un inventario completo de las bases de datos incluyendo las restricciones propias y programación adicional en las tablas que conforman las bases de datos. • Se requiere de un ambiente de pruebas que permita analizar el comportamiento de la base de datos (crecimiento, seguridad, integridad).	•Modelo de gestión y plan de continuidad de los servicios de bases de datos. •Personal disponible 24/7. •Comunicación ágil con colaboradores internos y externos. •Sitio alterno con todas las condiciones de implementación a nivel de bases de datos. •Almenos 3 personas que puedan realizar sus labores al mismo nivel de conocimiento y capacitación formal y continua al personal involucrado. •Cronograma que permita la restauración de las bases de datos. •Nuevas herramientas de monitoreo. •Inventario actualizado de componentes y objetos dentro de las bases de datos •Ambiente de pruebas.

Fuente: Elaboración Propia (2016)

CAPÍTULO V PROPUESTA DEL PROYECTO

5.1 Introducción a la propuesta del plan de continuidad de bases de datos.

En este capítulo se va a definir la propuesta a seguir antes, durante y después de una interrupción de los servicios de bases de datos SQL Server del BCBCR y que respondan oportunamente a gestionar la continuidad y restauración de sus procesos buscando el menor impacto en las operaciones.

Para el desarrollo de este tema, como se ha mencionado anteriormente, se aplicará lo propuesto en las Normas Técnicas para la gestión y el control de las tecnologías de información, las cuales son basadas a las mejores prácticas dictaminadas por COBIT V4.1.

Como se ha establecido también en párrafos anteriores, COBIT proporciona un modelo de dominios o procesos que permite visualizar y administrar las tareas a desarrollar en los casos de emergencia en cuanto a la disponibilidad de datos necesarios para que el negocio continúe su trabajo habitual. Esta propuesta va a estar alineada a las estrategias de TIC para alcanzar el uso óptimo de los recursos, por lo que el personal involucrado debe tener claro y entender la propuesta que permitirá administrar los posibles riesgos que se presenten o que afecten la continuidad del servicio.

Al implementar COBIT V4.1 como parte de la solución al problema de la continuidad de servicios tenemos las siguientes:

- Mejor alineación, con base en su enfoque de negocios.
- Una visión, entendible para la gerencia, de lo que hace TI.

- Propiedad y responsabilidades claras, con base en su orientación a procesos.
- Aceptación general de terceros y reguladores.
- Entendimiento compartido entre todos los interesados, con base en un lenguaje común.

Dentro del marco establecido en COBIT v4.1, se enfocará la propuesta en el Dominio Entregar y dar Soporte (DS), este dominio recibe las soluciones y las hace utilizables por los usuarios finales.

5.2 Vulnerabilidades en la continuidad del servicio de base de datos

Según la investigación llevada a cabo, se encontraron diferentes vulnerabilidades que podría afectar la continuidad del servicio de las bases de datos en caso de una eventual suspensión de los mismos. Para esto se realizó el análisis sobre lo que dictan las Normas Técnicas de la Contraloría General de la República, basadas en el DS4 (Garantizar la continuidad del servicio) de COBIT V 4.1, encontrando las siguientes vulnerabilidades:

1- DS4.1 Marco de trabajo de Continuidad de TI:

El cual tiene como objetivo: "**Ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus**

clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI." (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf)**.**Es por esto que se determina que la Unidad de TIC del Cuerpo de Bomberos cuenta con estrategias de gestión que no están acordes ni alineadas a las mejores prácticas.

2- DS4.2 Planes de Continuidad de TI:

Este proceso define que se deben: **"Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas."** (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf)**.** Según lo mencionado anteriormente se comprueba que la Unidad de TIC, no cuenta con un plan que permita dar continuidad a una eventual suspensión de los servicios de bases de datos. Tampoco existen procedimientos de bases de datos para realizar tareas como respaldos, ejecución de pases de bases de datos, creación, actualización o eliminación de usuarios, configuración de las bases de datos. No existe documentación de tablas, Jobs, procedimientos almacenados, alertas, alarmas almacenadas o programadas a nivel de base de datos.

3- DS4.5 Recursos Críticos de TI:

Este proceso tiene como objetivo: **"Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio."** (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf**).** Si bien el Cuerpo de Bomberos tiene mapeado algunos de los recursos críticos que se ven involucrados en el servicio de base de datos, al no existir un plan de continuidad la unidad de TIC, no se cuenta con pasos a seguir para determinar las prioridades de recuperación, además no se han establecido tiempos y costos. Por otro lado uno de los recursos más importantes es el personal técnico disponible para la atención oportuna del servicio en caso de una suspensión, sin embargo existe una limitación en disponibilidad de este personal, ya que se apega al horario de oficina, el cual es de 7:45 am a 4:05 pm.

4- DS4.5 Pruebas del Plan de Continuidad de TI

En este proceso se menciona sobre la importancia de: **"Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta apunta y en pruebas integradas con el proveedor."** (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf)**.** A raíz de esto se determina que no existen pruebas documentadas que ayuden a determinar tiempos, costos, planes de acción y prioridades ante una recuperación de bases de datos.

5- DS4.6 Entrenamiento del Plan de Continuidad de TI

Este proceso indica que se debe **"Asegurar de que todos las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia."** (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf)**.** Dado lo anterior, la Unidad de TIC cuenta con poco personal capacitado, ya que solamente dos

personas tienen el conocimiento técnico, sin embargo una de las personas cuenta con 100% de conocimiento y otro al 30 %, limitando la atención del servicio ante cualquier eventualidad.

6- DS4.8 Recuperación y Reanudación de los Servicios de TI

En este proceso se manifiesta que se deben: **"Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio."** (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf**).**

DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones

El objetivo de este proceso es: **"Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La**

gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados." (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf).Con Base a estos dos procesos descritos anteriormente, se determina que el Cuerpo de Bomberos cuenta con un sitio alterno donde se envían los respaldos de las bases de datos SQL, sin embargo este sitio no cuenta con los componentes, ni la configuración necesaria para ejecutar las restauraciones y poner en funcionamiento el servicio. Tampoco se realizan pruebas de restauraciones por lo que no se valida la integridad de los datos ni se pueden probar los respaldos de las bases de datos, ya que tampoco existen respaldos de las aplicaciones en ese sitio.

Una vez puesto en marcha el plan de continuidad se deben tomar en cuenta los procesos descritos anteriormente y también es necesario darle mantenimiento al plan de continuidad como lo indica el proceso DS4.4 Mantenimiento del Plan de Continuidad de TI **"Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna."** (COBIT 4.1, IT Governance Institute,

2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf).También es importante realizar evaluaciones después de ejecutar el plan de continuidad del servicio de base de datos como lo indica el proceso DS4.10 Revisión Post Reanudación **"Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia."** (COBIT 4.1, IT Governance Institute, 2007, p.114. Recuperado de http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf).

5.3 Diseño del plan de continuidad

5.3.1 Definición de grupo de trabajo

Para el inicio de la propuesta de continuidad de servicios de bases de datos, se propone contar con un grupo de trabajo el cual se encargará de atender de forma oportuna e inmediata los incidentes provocados por una caída de servicios independientemente de la causa. Este grupo de trabajo tiene que definir un responsable que se encargará de la coordinación y supervisión de evacuar el incidente presentado.

Es necesario, para cumplir con este requisito, que el personal involucrado al menos el encargado, tenga una disponibilidad inmediata a la solución del problema. Es necesario también que este funcionario pueda contar con la comunicación fluida e inmediata, con los demás miembros del grupo de trabajo.

Como lo indica COBIT V 4.1 en su apartado DS4.1 Marco de trabajo de la administración de los niveles de servicio, se debe tomar en cuenta la estructura

organizacional para administrar la continuidad, la cobertura de roles, las tareas y responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes.

5.3.2 Personal Interno

Según lo expuesto en el punto 4.2.3 Personal Capacitado, se propone nombrar a las personas necesarias responsables de las bases de datos y crear el rol de guardia, el cual consiste en que una de estas personas esté con disponibilidad de atención y soporte a las bases de datos en un horario de 24/7, rotativo cada semana. Esto permitirá una atención oportuna a cualquier incidente que se pueda presentar y que requieran la intervención de una de estas personas. Estas personas deben ser incluidas en el formulario de “Directorio de contactos internos”. (Ver Anexo # 10 del plan de continuidad.)

5.3.3 Proveedores externos

Al contar con proveedores externos que tengan que dar mantenimiento o que puedan colaborar con una suspensión de servicios de esos sistemas y sus bases de datos. Se recomienda entonces, tener identificados por parte del grupo de trabajo a los funcionarios externos con un formulario que contenga el nombre del proveedor, persona a contactar, teléfonos, celular, correo electrónico y dirección (ver Anexo # 11 del plan de continuidad), clasificados de acuerdo a sus responsabilidades y que tengan la disponibilidad por parte de su empresa para que sean el apoyo técnico al encargado o encargados de cubrir el incidente por parte de Bomberos. Es conveniente también que

se evalué contantemente a los proveedores para documentar que se esté cumpliendo con lo establecido en los contratos en cuanto a la prestación de sus servicios, como lo desarrolla COBIT 4.1 en su apartado DS2 Administrar los servicios de terceros.

5.3.4 Continuidad del servicio de bases de datos SQL server 2014

La continuidad de servicios de bases de datos como parte de lo que debería ser un plan integral, tiene el propósito principal de mantener los servicios de bases de datos disponibles a cualquier evento que afecte el trabajo cotidiano en los sistemas, en los servidores y en las bases de datos propiamente.

Como punto primordial para restablecer el estado normal de la base de datos que posee actualmente en producción el Benemérito Cuerpo de Bomberos de Costa Rica y como se mencionó en los puntos 4.2.2.1 Respaldos y 4.2.2.2 Restauraciones, se debe de tener certeza de que los respaldos de bases de datos sean lo más recientes posible, pero es importante antes de crear una estrategia de respaldo y restauración de las bases y sus datos, calcular cuánto espacio en disco usará la copia de seguridad completa.

En el plan a desarrollar el cual es el Anexo principal a este documento (ver Anexo #2), se contemplarán varias fases, las cuales contienen lo necesario para mantener la continuidad del servicio de bases de datos SQL del Cuerpo de Bomberos.

5.3.5 Fase preventiva

En esta fase se propone ejecutar un mantenimiento a los servidores y bases de datos que bridan soporte a los sistemas informáticos del Benemérito Cuerpo de Bomberos de Costa Rica.

Como parte de este mantenimiento se propone desarrollar por el grupo de trabajo mencionado anteriormente, iniciar con un inventario de sistemas (cuantos y cuales son web y cuantos y cuales son cliente servidor) y de las bases de datos ligados a estos, se debe tener también un inventario del equipo físico y virtual (servidores).

Dentro del inventario de la base de datos debe existir la descripción de todas las instancias y objetos relacionados a las mismas para determinar la estructura y los atributos de los objetos, por ejemplo:

- Número y nombre de las tablas y vistas de las bases de datos, números de columnas de una tabla o vista, junto con el nombre, el tipo de datos, la escala y la precisión de cada columna, así como las observaciones y descripción de las mismas. (ver Anexo #1 del plan de continuidad)
- Las restricciones definidas en una tabla.
- Los índices y claves definidos por una tabla.
- Procedimientos almacenados y funciones agrupados por sistema.
- Revisiones periódicas de los clúster donde se encuentran los servidores de bases de datos.

Para simplificar la tarea en una posible caída de servicios de bases de datos, o daño de un servidor o alguno de esos componentes (Disco duro, memoria, particiones, entre otros), se debe de contar con el procedimiento adecuado para la configuración,

seguridad, creación y gestión de bases de datos al tiempo que se proporcione el mecanismo de integración con otros sistemas y políticas de seguridad; así como las herramientas que permitan su programación, tanto a nivel de diseño como a nivel de reglas y procedimientos integrados en la arquitectura de base de datos. Estos procedimientos deben estar documentados, respaldados y en propiedad en cada uno de los funcionarios que componen el grupo de trabajo. No se puede dejar por fuera a estas observaciones la posibilidad de documentar que la información pueda estar almacenada en varios servidores por lo que el volumen de la información en caso de una replicación de datos debe ser considerado en este procedimiento.

5.3.5.1 Ubicación y ejecución de los respaldos.

Los respaldos de bases de datos y servidores se ubican en el centro de datos del Cuerpo de Bomberos F5, dentro de este centro de datos existe un servidor el cual contiene un software llamado data protector, el mismo es un software de copia de seguridad y recuperación que proporciona una protección de datos completa, análisis en tiempo real y optimización guiada. Este software está configurado para que envié los respaldos ejecutados diariamente a un dispositivo de back up, donde son almacenados en cintas virtuales las cuales emulan las cintas físicas. Luego estos respaldos son enviados por un enlace hacia el sitio alterno, sin embargo solamente son enviados para custodia y no se realiza ninguna otra tarea con estos.

5.3.5.2 Sitio alterno

Para la ejecución correcta del plan de continuidad se propone la implementación de un proceso de restauración de los respaldos en el sitio alterno con el que cuenta el Cuerpo de Bomberos, tomando en cuenta todos los componentes necesarios para una rápida, eficaz y eficiente restauración del servicio de base de datos en caso de desastre en el sitio principal, esto para garantizar la continuidad del servicio. Los componentes a tomar en cuenta y que deben ser instalados y configurados en este sitio para poder ofrecer la continuidad de las bases de datos son:

1 Servidor virtual con:

- 12 GB de memoria
- 2 procesadores

Para almacenamiento:

- 1 partición de 50GB (sistema operativo)
- 2 particiones de 100GB
- 1 partición de 200GB
- 1 partición de 25GB
- 1 partición de 50GB
- 1 licencia de Windows server 2012 estándar
- 1 licencia de SQL Server Enterprise 2014
- Framework 3.5

Red

- Enlace directo del sitio principal al sitio alterno.

Es de importancia el poder establecer pruebas de restauración con los respaldos realizados, estas pruebas son necesarias que se implemente no solamente en el centro de datos principal, sino que es vital que estas pruebas se realicen en el sitio alterno al menos una vez a la semana, en el cual en caso de desastre será el que se active inmediatamente declarada la emergencia. Sin estas pruebas la continuidad de los servicios de bases de datos y la disponibilidad de los datos corren el peligro de no solo tener a estos disponibles si no que puede crear además crisis de información que lógicamente alteraran el servicio de los sistemas primordiales que utiliza el Cuerpo de Bomberos.

Además es importante realizar en el sitio alterno pruebas de estimación de tiempos en ejecución de respaldos y restauraciones, para así poder determinar el tiempo prudencial para levantar el servicio nuevamente en caso de un incidente y generar el menor impacto posible a la institución.

5.3.5.3 Capacitación del personal

En cuanto a la capacitación de personal se recomienda establecer para todas las personas involucradas en el soporte de bases de datos, un esquema de capacitación en el cual el nivel de conocimiento y de capacidad de estas personas sea equitativo y sea lo suficientemente actualizado para responder a los problemas de interrupción de servicios de las bases de datos.

Para el plan de capacitación es recomendable que se lleven a cabo cursos certificados de SQL server que permitan a estos funcionarios desarrollarse como DBA. Para esto Microsoft establece niveles de capacitación debidamente certificados por

niveles de experiencia y conocimiento; es necesario que para esto también se destine la partida presupuestaria para facilitar este proceso, el cual es necesario dentro de este plan de gestión. Cumpliendo así con el punto DS4.6 de COBIT V4.1. Es por esto que el plan de continuidad define un formulario para el registro de capacitaciones (ver Anexo # 2 del plan de continuidad).

5.3.6 Fase de ejecución y restauración

En esta fase se ejecuta el restablecimiento del servicio ya sea en el sitio principal o en el sitio alterno. Para esto se debe realizar un análisis de la situación actual, se determinan las causas del incidente y se determinan los pasos a seguir para levantar el servicio.

Luego de este análisis es importante que el grupo de trabajo calcule los tiempos en que se puede restaurar el servicio y completar el formulario de evaluación de daños de los componentes (Ver Anexo # 3 del plan de continuidad), de ser necesario se deberá activar el sitio alterno.

Una vez solucionado el incidente en el sitio principal se deberá restablecer el servicio en este y pasar el sitio alterno a estado pasivo. El grupo de trabajo deberá completar el formulario de registro de problemas (ver Anexo # 4 del plan de continuidad).

5.3.7 Fase de Pruebas

En esta fase es necesario aplicar pruebas tanto en la fase preventiva como en la fase de ejecución durante del proceso de restauración del servicio, ya que esto ayudará a tomar decisiones en cuanto a que es lo más conveniente realizar para que el servicio vuelva a la normalidad, una vez restablecido el servicio es conveniente continuar con las pruebas para así asegurar que todo funciona correctamente y evitar una nueva caída del servicio de bases de datos. Es necesario completar el formulario de programación de pruebas (ver Anexo # 5 del plan de continuidad), ya que este contempla información las aplicaciones y componentes, capa a probar, fecha, tipo de prueba a realizar y el personal involucrado. Una vez finalizadas las pruebas es importante realizar la evaluación de las pruebas para así obtener puntos de mejora en la realización de las mismas (ver formulario # 6 del plan de continuidad).

5.3.8 Fase de documentación

Las personas designadas como responsables de ejecutar el plan de continuidad de servicios, que son el personal capacitado, deben realizar un levantamiento de la información necesaria con los procedimientos y pasos a seguir para el resguardo, almacenamiento, configuración de las bases de datos y de los servidores, seguridad de las bases de datos, manipulación, respaldo y restauración tanto de bases de datos como de servidores; convirtiendo esta información en manuales técnicos y manuales de usuario, ya que ayudarán a futuros funcionarios con una guía para la solución de los problemas incluyendo este plan, que además cuenta con una serie de formularios en los cuales quedará el registro de los incidentes, su solución, responsables de atender y corregir, colaboradores externos, tiempos de recuperación, evaluación de los daños y

las evaluaciones tanto de las pruebas realizadas así como del plan en general, entre otros.

Por lo expuesto en el marco de trabajo de continuidad de TI, según COBIT, se tiene que documentar de forma detallada los sistemas (aplicaciones) y las bases de datos que utiliza cada sistema.

5.3.9 Seguridad de las bases datos

La protección de la seguridad en SQL Server conlleva una serie de pasos dentro los cuales afectan 4 áreas: la plataforma, la autenticación, los objetos (incluidos los datos) y las aplicaciones que tienen acceso al sistema.

Los elementos que se deben proteger y aplicar la seguridad son: el servidor, la base de datos y los objetos incluidos en las bases de datos.

Con la ayuda de la creación del catálogo de bases de datos mencionado en el punto 4.3, es posible identificar la sensibilidad de los datos y aplicarles la seguridad necesaria para mantener estas bases de datos libres de ataques externos.

Se recomienda hacer una evaluación de la configuración de la bases de datos, para verificar las forma en que se instaló. Se deben de comprobar los privilegios asignados a roles específicos que permitan leer, escribir y ejecutar en la base de datos. Para ello el administrador de la base de datos debe:

- Limitar el acceso a los procedimientos a ciertos usuarios
- Delimitar el acceso a los datos para ciertos usuarios, procedimientos, y/o datos

Con base al inventario a realizar es necesario tener en cuenta cuales bases de datos, tablas y datos en general no están siendo usados por los sistemas actuales, por

lo que deben ser respaldados y eliminados de las bases de datos actualmente utilizados. (Ver Anexo # 1 del plan de continuidad).

Es recomendable mantener y crear nuevas pistas de auditoria que mantengan controlado la integridad de los datos.

5.4 Propuesta del plan de continuidad del servicio de bases de datos

Con base a todo el análisis realizado, tomando en cuenta las Normas Técnicas de la Contraloría General de la República y las mejores prácticas internacionales, se creó la propuesta del plan de continuidad correspondiente al servicio de bases de datos que administra la Unidad de TIC del Cuerpo de Bomberos de Costa Rica. Como se podrá observar en el apéndice #2 plan de continuidad, ahí se describen los procesos de gestión de continuidad, el análisis de riesgos y los equipos de recuperación. Para esto se crearon los siguientes formularios de apoyo:

5.4.1 Catálogo de base de datos

En este catálogo se definirán aspectos importantes de las bases de datos entre ellas, nombre de las tablas, vistas, logs, columnas, índices, información de autorizaciones y permisos de las tablas de bases de datos. Este catálogo servirá para tener actualizado el inventario de la estructura de las bases de datos.

5.4.2 Registro de capacitaciones

Este registro contendrá la información de las capacitaciones que realice el personal técnico a carga de administrar las bases de datos, entre la información a completar esta el nombre de la persona que recibe la capacitación, puesto, duración de la capacitación, temas tratados, entre otros.

5.4.3 Evaluación de daños de los componentes de bases de datos

En este formulario se registraran los incidentes que afecten el servicio de base de datos, se hará una evaluación del incidente, así como la infraestructura afectada y las personas encargadas de dicha evaluación. En caso de requerir ayuda de los proveedores, se estará definiendo en este formulario el nombre del proveedor, el apoyo recibido y las recomendaciones brindadas.

5.4.4 Registro de problemas

En este registro se determinará la información de los equipos de recuperación que respondan a los problemas presentados, acá se definen fecha y hora del problema, quien lo identificó, como se resolvió, tiempo en resolver el mismo, y persona que resolvió el problema.

5.4.5 Programación de pruebas

Este es un registro sobre las pruebas a realizar, así como los componentes o aplicaciones donde se llevaran a cabo las pruebas, capas, fecha de prueba, tipo y personal requerido para ejecutar la misma.

5.4.6 Evaluación posterior a la prueba

Posterior a cada prueba se debe realizar un análisis de la misma, para esto es necesario completar este formulario, el mismo contendrá datos generales, evaluación de actividades programadas y la evaluación general de la prueba, esta última está constituida por diferentes ítems a evaluar y se deberá otorgar una calificación así como establecer los puntos de mejora.

5.4.7 Evaluación posterior a la ejecución del plan

Una vez ejecutado el plan de continuidad del servicio de bases de datos se deberá realizar una evaluación posterior al mismo, basados en niveles de satisfacción y tomando en cuenta una serie de aspectos definidos dentro de esta evaluación.

5.4.8 Registro de cambios

Este formulario contiene la información sobre los cambios realizados, entre ellos, descripción del cambio, motivo, persona encargada, actividades realizadas para la ejecución del cambio y persona que da visto bueno.

5.4.9 Gestión de riesgo

Para asegurar una continuidad de los servicios de bases de datos, es recomendable analizar posibles riesgos que puedan afectar dicho servicio. En este formulario se definirá la descripción del riesgo, la probabilidad, el impacto, el nivel de riesgo, el tratamiento que se le aplicará así como la persona responsable de mitigar ese riesgo.

5.4.10 Directorio de contactos internos

Ante una eventual suspensión de los servicios de bases de datos, es necesario tener mapeado al personal interno de la institución que deberán tomar responsabilidades para asegurar la continuidad del servicio. En este formulario se deberá detallar la información de este equipo, entre ellos, nombres, roles, teléfonos y correos electrónicos.

5.4.11 Directorio de contactos externos

Al igual que los contactos internos, los proveedores juegan un papel muy importante en la continuidad de los servicios, ya que ellos realizan tareas que el personal interno no pueden realizar, es por esta razón que también se debe documentar la información

del personal externo, como nombre, teléfono, correos electrónicos y la dirección sonde pueden ser localizados.

CAPÍTULO VI CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

1. De acuerdo al análisis realizado de la situación actual, se pudo determinar que los equipos donde se alojan las bases de datos cuentan con redundancia en el mismo sitio, sin embargo, al contar con un sitio alterno que no está preparado para brindar la continuidad del servicio, concibe que a la hora de presentarse un incidente en el sitio primario, se vea afectado en gran medida el servicio de bases de datos que se brinda en la unidad de TIC.

2. Si bien la institución está comprometida con la continuidad del negocio y el servicio a los usuarios, actualmente no existe un plan de continuidad para las bases de datos, ni el personal capacitado, por lo que de presentarse un incidente mayor, no se podría levantar el servicio en un lapso de tiempo apto para la institución.

3. A pesar de que se tienen claramente definidos los procedimientos de los procesos de respaldo, los procesos de restauración no son ejecutados según recomiendan las mejores prácticas, además en caso de presentarse un incidente en el sitio principal, no se cuenta con el equipo ni la configuración adecuada para levantar el servicio en otro sitio.

4. El Benemérito Cuerpo de Bomberos de Costa Rica al igual que otras entidades, es vulnerable a sufrir situaciones de riesgo que puedan generar un incidente. Esta situación tendría un efecto significativo en el negocio, por lo que es

importante que la institución realice un esfuerzo para establecer un plan de continuidad, en el que se describan los pasos a seguir por cada uno los participantes involucrados.

6.2 Recomendaciones

1. Se recomienda realizar la inversión necesaria para la instalación y configuración de los equipos que se deben utilizar en el sitio alterno para poder brindar una continuidad del servicio de bases de datos si el sitio principal presentara algún inconveniente.

2. Se recomienda aprobar la propuesta del plan de continuidad de bases de datos para seguir brindado el servicio de manera continua y afectar lo menos posible las operaciones del negocio.

3. Asignar, formalmente, al personal técnico de la unidad de TIC y con la disponibilidad necesaria, los cuales serán responsables de velar por la continuidad del servicio de bases de datos que ofrece esta unidad.

4. Brindar la capacitación necesaria al personal involucrado con las funciones establecidas en el plan de continuidad de las bases de datos, para que puedan aplicar los procedimientos necesarios en caso de una necesidad de contingencia.

5. Realizar pruebas o simulacros periódicos del plan de continuidad de base de datos, para verificar los tiempos de respuesta y las funciones del personal involucrado, y así, en caso de presentarse algún evento real, tener la experiencia de haber aplicado antes el plan.

6. Una vez aprobado el plan propuesto y dada la constante dinámica de las operaciones, se recomienda realizar revisiones periódicas, para mantenerlo actualizado.

7. Se recomienda adecuar este plan al futuro plan de continuidad de TIC, el cual se encuentra en desarrollo por parte del encargado del programa de seguridad y continuidad.

CAPÍTULO VII REFERENCIAS BIBLIOGRÁFICAS

Benemérito Cuerpo de Bomberos de Costa Rica. (2016). Nosotros Bomberos de Costa Rica. Disponible en http://www.bomberos.go.cr/quienes-somos/

Acevedo Juárez, H. ITIL ¿qué es y para qué sirve?, Magazcitum. 2010. Disponible en http://www.magazcitum.com.mx/?p=50

Contraloría General de la República de Costa Rica. (2007). Normas técnicas para la gestión y el control de las Tecnologías de Información. Disponible en http://www.ocu.ucr.ac.cr/Leyes/Nuevas%20normas%20de%20TI%20-CGR%20N-2-2007-CO-DFOE.pdf

Osiatis S.A. (Sin fecha). ITIL Foundation. Estrategias para los servicios de TI. Disponible en http://itilv3.osiatis.es/estrategia_servicios_TI.php

Pérez, D. (2007). Maestros del web. ¿Qué son las bases de datos? Disponible en http://www.maestrosdelweb.com/que-son-las-bases-de-datos/

Gómez, J. (2001). CEPAL. Vulnerabilidad y medio ambiente. Disponible en http://www.cepal.org/publicaciones/xml/3/8283/jjgomez.pdf

Universidad Internacional de Valencia. (Sin fecha). Concepto y utilidad de las buenas prácticas en la enseñanza. Disponible en http://www.viu.es/concepto-y-utilidad-de-las-buenas-practicas-en-la-ensenanza/

Real Academia Española. (2016). Significado de Implementar. Disponible en http://dle.rae.es/?id=L4eKVkR

Shuttleworth, M (2010). Estudio piloto. Obtenido de Explorable.com: https://explorable.com/es/estudio-piloto

Ortiz, C. (Sin fecha). La importancia de un plan de contingencia, Foro de seguridad. Perú. Disponible en http://www.forodeseguridad.com/artic/discipl/4132.htm

IT Gobernance Institute. (2007). Cobit v4.1. Disponible en http://www.slinfo.una.ac.cr/documentos/EIF402/cobit4.1.pdf

Mora y Vargas. (Sin fecha). Continuidad de servicio de TI en el Ministerio de Trabajo y seguridad Social de Costa Rica. Disponible en http://bb9.ulacit.ac.cr/tesinas/publicaciones/041861.pdf

RECOPE. (2015). Gerencia General. Política de continuidad de negocio y Política de seguridad de la Información. Disponible en https://www.recope.go.cr/wp-content/uploads/2015/05/Politicas_de_continuidad_y_seguridad_de_la_Informacion2.pdf

Universidad de Costa Rica. (2015). La Gaceta Universitaria. Directrices de seguridad de la información de la Universidad de Costa Rica. Disponible en http://www.cu.ucr.ac.cr/uploads/tx_ucruniversitycouncildatabases/officialgazette/2015/a07-2015.pdf

Romeo y Domenech. (Sin fecha). Materiales de lengua y literatura. La entrevista. Disponible en http://www.materialesdelengua.org/EXPERIENCIAS/PRENSA/f_entrevista_web.pdf

Mella, O. (2000). Grupos Focales. Técnicas de Investigación cualitativa. Disponible en http://biblioteca.uahurtado.cl/ujah/856/txtcompleto/txt105091.pdf

Osiatis S.A. (Sin fecha). Gestión de la continuidad de servicios TI. España. Disponible en http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti.php

CAPÍTULO VIII APÉNDICES

Apéndice #1 Entrevista

Estado actual del manejo de continuidad del servicio de bases de datos del Cuerpo de Bomberos de Costa Rica

Diagnóstico del estado actual:

1. ¿Cuenta el Benemérito Cuerpo de Bomberos con un plan que ayude a mantener la continuidad del servicio de bases de datos?

   R/

2. ¿Qué procesos se encuentran definidos e identificados relacionados a la continuidad del servicio de base de datos?

   R/

3. ¿Qué modelos de gestión existen para ayudar a administrar de forma transparente, eficaz y eficiente las bases de datos?

   R/

4. ¿Existen planes de contingencia para la recuperación de las bases de datos, cada cuanto se revisan estos planos?

   R/

5. ¿Cuál es la disponibilidad de personal para la atención en caso de una caída de las bases de datos?

   R/

6. ¿Quiénes son las personas encargadas en el mantenimiento y atención oportuna en caso de una caída de bases de datos?

   R/

7. ¿Cuál software se utiliza en TIC para evitar el acceso a las bases de datos de entes externos?

R/

8. ¿Cuál es el presupuesto que dispone el Departamento de TIC a razón de invertir en software y en equipo para la implementación de un plan de continuidad?

   R/

9. ¿Cuáles son los riesgos identificados hasta el momento, que puedan afectar la continuidad de los servicios de bases de datos?

   R/

10. ¿Con que nivel de capacitación cuenta el personal a cargo para identificarlos y combatirlos?

    R/

11. ¿En caso de presentarse un incidente significativo en la continuidad de los servicios de bases de datos, de qué forma se coordina con colaboradores internos y externos que puedan suministrar su ayuda inmediata?

    R/

12. ¿Qué herramientas de monitoreo existen que indiquen el comportamiento inmediato de los componentes que conforman el servicio de bases de datos?

    R/

13. ¿Con que frecuencia se realizan respaldos de bases de datos?

    R/

14. ¿Cada cuánto se restauran estos respaldos?

    R/

15. ¿Existe un inventario de los componentes de la base de datos?

    R/

16. ¿Cuáles serían las estimaciones de pérdida de tiempo y dinero en una posible suspensión del servicio de bases de datos?

    R/

17. ¿Cuenta la unidad de TIC con un sitio alterno para levantar el servicio de bases de datos en una posible interrupción, se han realizado restauraciones en este sitio?

R/

18. ¿Es necesario el traslado de personal a este sitio?

R/

19. ¿Qué estándares se utiliza en las configuraciones de las bases de datos?

R/

Apéndice #2 Plan de Continuidad

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	**Unidad de Tecnologías de Información y Comunicaciones**			Código: **Versión: 01**
	Plan de continuidad del servicio de bases de datos de TIC			**Oficio de aprobación:**
	Escrito por: Luis Alejandro Madrigal	Revisado por:	Aprobado por:	Fecha de aprobación:

PLAN DE CONTINUIDAD DEL SERVICIO DE BASE DE DATOS DE TIC

1- PROPÓSITO

Mantener el estado normal de los componentes de bases de Datos que existen en el ambiente de producción que se encuentran actualmente en la unidad de TIC.

2- ALCANCE

Ejecución de mantenimiento preventivo, la recuperación y restauración exclusiva de la plataforma de base de datos.

3- INTRODUCCIÓN

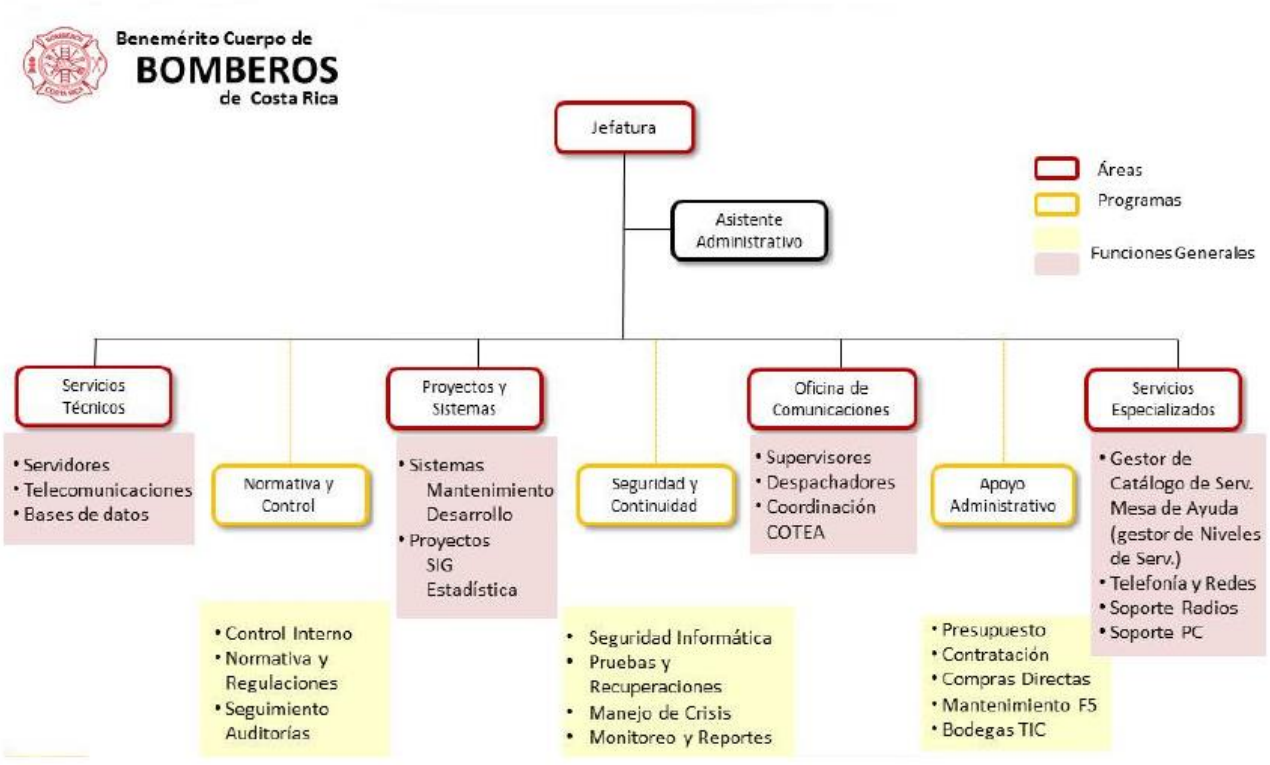
La planificación de la recuperación ante desastres de tecnología de información es una necesidad en el mundo automatizado de hoy. Las amenazas (naturales, ambientales y humanas) son reales y los desastres pueden resultar de muchas fuentes. Considerando el impacto de la perdida de la información y de las operaciones del día a

día, desde la perspectiva del negocio o legal, se hace necesario realizar preparativos para su protección y recuperación.

El BCBCR reconoce que existen amenazas significativas ante la posibilidad de la ocurrencia de un incidente o desastre que afecte el servicio de bases de datos, como también la necesidad de recuperarse en el menor tiempo posible, garantizando la continuidad del servicio.

Este plan de continuidad del servicio de bases de datos, ayudará a responder organizadamente a eventos que interrumpen la normal operación de sus procesos y que pueden generar impactos sensibles en el logro de los objetivos.

4- ESTRUCTURA JERARQUICA DE LA CONTINUIDAD DE TI Y DE NEGOCIO



5- PROCESO DE LA GESTIÓN DE CONTINUIDAD

5.1 Fase preventiva: Mantenimiento de servidores y bases de datos que dan soporte a los sistemas informáticos:

- Actualización del catálogo de bases de datos: El encargado de bases de datos debe mantener todas las estructuras de las bases de datos actualizadas y completar el catálogo de bases de datos de acuerdo a los cambios que puedan sufrir sus objetos, por ejemplo, un nuevo procedimiento almacenado, funciones, triggers, entre otros. (ver Anexo # 1)
- Monitoreo de servidores y bases de datos: El administrador de servidores, debe mantener constantemente monitoreado los equipos donde se almacenan las bases de datos, por ejemplo, espacio de disco, memoria, servicios de SQL Server entre otros. Además de mantener actualizados los servidores en cuanto a actualizaciones de sistema operativo y del antivirus. El encargado de bases de datos debe velar por el buen funcionamiento de las mismas y que estas se encuentren disponible en todo momento.
- Respaldo de servidores y bases de datos: En cuanto a los servidores los respaldos deben ser ejecutados diariamente por su respectivo encargado y los respaldos de bases de datos deben ser ejecutados por el administrador de bases de datos o su suplente, diariamente y se deben enviar al sitio alterno para sus pruebas de restauración al menos una vez por semana.
- Capacitación técnica: se debe capacitar continuamente al grupo de trabajo, los cuales son los responsables de velar por la continuidad de servicios, la jefatura de TIC debe completar el formulario registro de capacitaciones (ver Anexo # 2)

5.2 Fase de ejecución y recuperación: Restablecimiento del servicio de base de datos:

- Análisis de la situación actual: En una interrupción de los servicios el grupo de trabajo debe analizar las causas, para establecer los procedimientos a seguir para la restauración del servicio.
- Determinar los tiempos de restauración: El grupo de trabajo debe calcular los tiempos en el que se pueda restaurar los servicios una vez analizadas las causas según se establece en la fase de documentación en su formulario de evaluación de daños de los componentes de las bases de datos.
- Levantamiento del servicio en el sitio alterno: Si existe un problema en los componentes de bases de datos a nivel de sitio principal que impida la continuidad del servicio de base de datos, el grupo de trabajo debe asegurarse que el sitio alterno entre en función, para esto existen dos formas:

    1. Automática: Por medio de un listener, se realiza un monitoreo a los servidores de bases de datos, en el momento que los servidores tanto principal como secundario ubicados en el sitio principal no respondan, este re direcciona la conexión de bases de datos al servidor terciario, ubicado en el sitio alterno. Este escenario podría darse cuando existe un problema a nivel lógico de los servidores de bases de datos.
    2. Manual: Esta opción se da cuando ocurre un desastre en el sitio principal y los servidores sufren daños físicos, el cual no permite tener acceso a la configuración de los mismos, para esto es necesario tener actualizado tanto el servidor de bases de datos ubicado en el sitio alterno como los servidores de aplicaciones, se debe verificar la funcionalidad de los componentes y realizar la conexión de las aplicaciones a las bases de datos correspondientes.
- Restauración del servicio en el sitio principal: Una vez solucionadas las causas en el sitio principal, el grupo de trabajo coordina la restauración del servicio en este sitio, manteniendo un monitoreo constante y ejecutando

pruebas de rendimiento, memoria, capacidad de disco, entre otros y se pasa el sitio alterno a un estado pasivo. Además este grupo debe completar el formulario de registro de problemas (ver Anexo # 4)

5.3 Fase de pruebas: Ejecución de las pruebas

- Programación de pruebas: En esta etapa se deben contemplar actividades como:

    - Coordinar la ejecución de las pruebas de recuperación de las Bases de Datos.
    - Determinar el periodo de ejecución de las prueba.
    - Coordinar los recursos (equipo y personal) para ejecutar las pruebas.
    - Documentar acciones a mitigar o mejorar y presentarlas a la jefatura de TIC.

    Para esto el grupo de trabajo debe llenar el formulario de programación de pruebas programadas (Ver Anexo # 5), las cuales serán pruebas de restauración de respaldos de bases de datos, integridad de estructuras, integridad de datos y pruebas de conexión, que ayudarán a asegurar la continuidad del servicio.
- Evaluación posterior a la prueba: Después de realizar las pruebas el grupo de trabajo debe evaluar las mismas para determinar puntos de mejora, para eso debe llenar el formulario correspondiente (ver Anexo #6)

5.4 Fase de documentación: Registra el incidente presentado.

- Evaluación de daños de los componentes de las bases de datos: el grupo de trabajo debe realizar la evaluación de los componentes de las bases de datos y determinar si es necesario el cambio o una nueva configuración en los equipos. Para esto se debe completar el formulario correspondiente. (Ver Anexo #3)
- Registro de problemas: El encargado de seguridad y continuidad debe llenar el formulario de registro de problemas (ver Anexo #4) donde se indica

fecha/hora del incidente, persona que lo identifico, descripción de problema, ¿cómo se resolvió?, ¿Cuándo se tardó en resolver? y ¿Quién lo resolvió?

- Evaluación posterior a la ejecución del plan: el grupo de trabajo debe completar este formulario (ver Anexo #7) para poder obtener conclusiones importantes en todo el proceso de continuidad y así determinar si se debe realizar algún cambio.
- Registro de cambios: El administrador de servidores y el administrador de bases de datos deben completar este formulario (ver Anexo #8) según los cambios realizados tanto en bases de datos como servidores.
- Gestión de riesgos: El grupo de trabajo debe medir el riesgo al impacto y la probabilidad de que suceda, además determinar las acciones para mitigar los problemas generados, para lo cual se debe completar el formulario correspondiente (ver Anexo #9) utilizando la matriz de priorización. Esta consta de los siguientes puntos:

5.3.1 Probabilidad: Frecuencia que podría presentar el riesgo.

- ✓ **Alta:** Es muy factible que el riesgo se presente.
- ✓ **Media:** Es factible que el riesgo se presente.
- ✓ **Baja:** Es muy poco factible que el riesgo se presente.

Probabilidad	Calificación Cuantitativa	Calificación Cualitativa	Código de Colores
Altamente probable (AP)	5	Puede ocurrir diariamente.	
Muy probable (MP)	4	Puede ocurrir varias veces en un mes.	
Probable (P)	3	Puede ocurrir al menos una vez al año.	
Poco Probable (PP)	2	Puede ocurrir alguna vez entre uno y cinco años.	
Improbable (IP)	1	Puede ocurrir al menos una vez en periodos superiores a cinco años.	

5.3.2 **Impacto:** Forma en la cual el riesgo podría afectar los objetivos estratégicos.

- ✓ **Alto:** Afecta en alto grado los objetivos estratégicos.
- ✓ **Medio:** Afecta en grado medio los objetivos estratégicos.
- ✓ **Bajo:** Afecta en grado bajo los objetivos estratégicos.

Impacto	Calificación Cuantitativa	Calificación Cualitativa	Código de Colores
Impacto Catastrófico	5	Puede ocasionar daños muy considerables y una interrupción completa de los servicios.	
Impacto Alto	4	Puede ocasionar daños muy considerables o una interrupción de los servicios.	
Impacto Medio	3	Puede ocasionar algunos daños y una interrupción parcial de los servicios.	
Impacto Moderado	2	Puede ocurrid una interrupción parcial de los servicios.	
Impacto Bajo	1	Existe una alerta, pero no hay interrupción de los servicios ni daños ocasionados.	

5.3.3 Matriz de Priorización:

Mapa de Calor		Impacto				
		Bajo	Moderado	Medio	Alto	Catastrófico
Probabilidad	**Valor**	1	2	3	4	5
Altamente probable	5	Medio	Alto	Alto	Catastrófico	Catastrófico
Muy probable	4	Moderado	Medio	Alto	Alto	Catastrófico
Probable	3	Moderado	Medio	Medio	Alto	Alto
Poco Probable	2	Bajo	Moderado	Medio	Medio	Alto
Improbable	1	Bajo	Bajo	Moderado	Moderado	Medio

5.3.4 Nivel de riesgo

Nivel de riesgo	Rango
Bajo	**1 - 2**
Moderado	**3 - 4**
Medio	**5 - 9**
Alto	**10 -16**
Catastrófico	**17 - 25**

6- PREMISAS DEL PLAN

- El plan de continuidad del servicio de base de datos está aprobado.
- Están identificadas las personas de ejecutar el plan.
- El personal a cargo del plan cuenta con la capacitación necesaria para ejecutarlo.
- El personal a cargo del plan cuenta con la disponibilidad 24/7 para brindar soporte ante cualquier incidente.
- El sitio alterno cuenta con las condiciones necesarias para brindar la continuidad del servicio de base de datos cuando sea necesario.

- El sitio alterno cuenta con la configuración necesaria de los servidores de aplicaciones para la gestión de la información almacenada en las bases de datos.

7- EQUIPO DE RECUPERACIÓN

El equipo de recuperación es el encargado de poner en marcha todo el proceso de recuperación para restaurar los servicios ya sea en el sitio principal o el sitio alterno.

Grupo	Nombre completo	Responsabilidades
Jefatura de TIC	**Ana María Ortega**	• Coordinar la ejecución oportuna del plan • Supervisión del personal encargado de las áreas • Supervisión de actividades y coordinación estratégica entre las áreas • Seguimiento y control de las actividades y objetivos del plan • Aseguramiento del recurso humano en términos de cantidad de recurso, capacitación y disponibilidad.
Encargado de Seguridad y continuidad	**David Reyes**	• Monitorear y actualizar los sistemas de seguridad de la infraestructura del Cuerpo de Bomberos • Monitorear la disponibilidad efectiva del sitio de contingencia • Participar en la evaluación de vulnerabilidades de los componentes de la plataforma de bases de datos. • Asegurar un ambiente óptimo desde el punto de vista informático dentro de la plataforma tecnológica institucional.
Encargado de bases de datos	**Cristian Ceciliano**	• Administra y monitorea las bases de datos de los sistemas de información institucionales. • Respalda periódicamente la información de las bases de datos. • Envió de los respaldos de bases de datos al sitio alterno.

		• Ejecutar restauraciones de los respaldos de bases de datos en el sitio alterno. • Mantener el inventario de los componentes de las bases de dato actualizado.
Encargado de servidores y respaldos	**Luis Alejandro Madrigal**	• Mantener actualizado el sistema operativo de los servidores y monitorear los componentes del mismo para asegurar que los servidores se encuentren activos en todo momento. • Mantener un respaldo actualizado de los servidores • Mantener el inventario de servidores actualizado
Encargado de proyectos y sistemas	**Iveth Bolaños**	• Analiza y detalla requerimientos nuevos para los sistemas existentes • Evalúa y propone soluciones ante errores que se detectan en los sistemas de información relacionados a las bases de datos • Da seguimiento y coordina pruebas de usuario de las modificaciones realizadas a los sistemas de información • Establece las metodologías y estándares de desarrollo y documentación de los sistemas
Encargado de Telecomunicaciones	**Lorenzo Alvarado**	• Velar por la ejecución oportuna del mantenimiento y monitoreo de la red de datos • Monitorear y administrar los servicios de telecomunicaciones con el sitio alterno

8- ESQUEMA DE COMUNICACIÓN

Esquema de activación parcial

Consecutivo	**Actividad**
1	**Reporte de incidente por parte de los usuarios**
2	**Mesa de ayuda atiende el incidente**

Esquema de activación total

Consecutivo	Actividad
1	**Reporte de incidente por parte de los usuarios**
2	**Mesa de ayuda atiende el incidente y no pudo resolver**
3	**Análisis por parte del grupo de trabajo**
4	**Solución por parte del encargado del servicio afectado(BD, Servidores, Sistemas, Telecomunicaciones)**

Árbol de llamadas

Directorios de continuidad

Definen los contactos tanto internos como externos que colaboran en la continuidad y recuperación del servicio de base de datos. (Ver formularios Anexos 10 y 11).

Medios de comunicación

1 - Número de extensión de la oficina
2- Teléfono Celular
3- Radio portátil
4- Correo electrónico
5- Grupos de WhatsApp

9- FORMULARIOS DE APOYO

Anexo 1: Catálogo de bases de datos

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Catálogo de Base de Datos			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre las tablas, Vistas y Logs									
Nombre de la tabla	Esquema	ID tabla	Tamaño en bytes de la fila	Número de columnas	Número de índices	Número de filas	Fecha de creación de la tabla	Tipo de tabla	Número de claves foráneas

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Catalogo de Base de Datos			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre las columnas de todas las tablas y vistas de la BD					
Nombre de la columna	ID columna	Número de la columna	Tipo de datos de la columna	Tipo de datos de la columna	Longitud física de la columna

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Catálogo de Base de Datos			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre todos los índices de las BD					
Nombre del índice	**Esquema**	**ID de la tabla**	**Tipo de índice (U: único, D: duplicado)**	**Clúster (sí, no)**	**Número de columna del primer elemento del índice**

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Catálogo de Base de Datos			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre las autorizaciones y permisos para las tablas			
Persona que crea la autorización	**Usuario al que se asigna el permiso**	**ID de la tabla**	**Privilegios (select, update, insert, delete y alter)**

Anexo 2: Registro de capacitaciones

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Registro de capacitaciones			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre las capacitaciones al personal

Nombre del funcionario	Puesto	Duración	Contenido de la capacitación	Fecha de inicio	Fecha de finalización	Objetivo de la capacitación	Certificación	Resultado	Observaciones

Anexo 3: Evaluación de daños de los componentes de bases de datos

1. Información del incidente			
Fecha:		ID del incidente:	
Hora inicio del incidente:		Hora de finalización del incidente:	
Descripción del incidente:			

2. Evaluación del incidente	
Severidad	__ **Muy alta**: Pérdida total de toda la infraestructura crítica __ **Alta**: Gran parte de la infraestructura crítica se vio afectada __ **Media**: Una pequeña porción de la infraestructura crítica sufrió daños. __ **Baja**: No hay daños en la infraestructura crítica

3. Infraestructura afectada					
Sistema afectado	Componentes relacionados	¿Se puede recuperar?	RTO del sistema afectado	Tiempo estimado de recuperación RTA	¿Se activará el Plan de Recuperación del sistema?

4. Apoyo de proveedor/entidades externas		
Nombre proveedor/entidades	Apoyo recibido	Recomendaciones

5. Personal Encargado de la evaluación de los daños a la infraestructura		
Nombre	Puesto	Firma

Anexo 4: Registro de problemas

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Registro de problemas			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre el equipo de recuperación						
Fecha y hora	Persona que identificó el problema	Descripción del problema	¿Cómo se resolvió el problema?	¿Cuanto se tardó en resolver el problema?	¿Quién resolvió el problema?	Observaciones

Anexo 5: Programación de pruebas

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Programación de pruebas			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre las pruebas a realizar				
Aplicaciones o componentes	**Capa a probar**	**Fecha programada de ejecución**	**Tipo de prueba**	**Personal requerido para la prueba**

Anexo 6: Evaluación posterior a la prueba

1- Datos generales	
Aplicaciones o componentes	
Fecha de evaluación	
Nombre de funcionario	

2- Evaluación de las actividades programadas		
Nombre de la actividad	Calificación	Observaciones

3- Evaluación general		
Por evaluar	Calificación	Oportunidad de mejora
¿Los participantes de las pruebas ejecutaron satisfactoriamente las actividades asignadas?		
¿Las actividades iniciaron y finalizaron según lo planeado?		
¿Se cumplieron los objetivos establecidos?		
¿Se contó con la disponibilidad de los recursos requeridos en la		

prueba (software/hardware)?		
¿Fue la documentación soporte para ejecutar la prueba clara, precisa y completa?		
¿Si se presentaron inconvenientes, los participantes pudieron restablecer el proceso de la prueba sin afectar el alcance?		
¿Los participantes contaron con habilidades técnicas para ejecutar la prueba?		
¿Cuál fue el nivel de desempeño de la prueba por parte del proveedor?		
¿Se mantuvo el nivel de desempeño de la aplicación en el ambiente de pruebas?		
¿Cuál fue el nivel de desempeño de las actividades de retorno a la operación normal?		
¿Cuál es la evaluación general de la prueba ejecutada?		

4- Eventos que interrumpieron la ejecución de la prueba

ID	Evento	Causa	Acciones contingentes durante la prueba

5- Oportunidades de mejora

ID	Oportunidades de mejora	Responsable

Anexo 7: Evaluación posterior a la ejecución del plan

1- Definiciones	
Nivel de satisfacción	
Muy alto	Cumplió totalmente con lo esperado
Alto	Casi cumplió con lo esperado pero presentó pocos inconvenientes
Medio	Presentó algunos inconvenientes
Bajo	Presentó muchos inconvenientes
Muy bajo	No cumplió con lo esperado
No aplica	No aplica y no se sede considerar para la calificación

2- Evaluadores		
Nombre	Área	Firma

3- Evaluación de la ejecución del plan de continuidad de bases de datos de TIC							
Aspecto a evaluar	Documentación involucrada	Nivel de satisfacción	¿Es necesario darle un tratamiento?	Tratamiento a ejecutarse	Responsable	¿Incluido en el registro de cambios?	Observaciones
¿La notificación del incidente fue oportuna?							
¿Se tuvo acceso inmediato a la documentación de continuidad de TIC?							
¿El grupo de manejo de incidentes se mantuvo informado en todo momento?							
¿La comunicación por parte de todos los miembros del grupo de trabajo fue apropiada?							
¿Se mantuvo informado al negocio del incidente y del tratamiento en ejecución?							
¿Los encargados de recuperación supieron cómo utilizar los instructivos de acciones contingentes?							

¿Los instructivos de acciones contingentes fueron efectivos para la recuperación?							
¿La evaluación del incidente por parte del grupo de trabajo fue realizada correctamente, el grupo sabía lo que había que hacer?							
¿Se presentaron problemas durante la ejecución del plan, fueron estos resueltos?							
¿Las bases de datos pudieron recuperarse apropiadamente?							
¿La degradación del servicio de bases de datos fue mayor a la esperada?							
¿La información generada manualmente fue ingresada a los sistemas una vez concluida la crisis?							
¿Las instalaciones y equipos del centro alterno se encontraron							

disponibles?							
¿Los proveedores requeridos apoyaron la recuperación del servicio?							
¿Los respaldos de información se encontraban disponibles y fueron recuperados apropiadamente?							

Anexo 8: Registro de cambios

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Registro de cambios			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre el registro de cambios									
Documentación involucrada	Descripción del cambio	Motivo del cambio	Persona encargada del cambio	Personas que participan en el cambio	Actividades que se realizarán para implementar el cambio	Fecha/ Hora/ Lugar de sesiones	Estado	Persona que dio visto bueno sobre documento	Observaciones

Anexo 9: Gestión de riesgo

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Gestión de riesgos			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre los riesgos encontrados					
Descripción del riesgo	Probabilidad	Impacto	Nivel de riesgo	Tratamiento	Responsable

Anexo 10: Directorio de contactos internos

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Directorio de Contactos internos			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre el equipo de recuperación					
Nombre	**Rol**	**Teléfono(s)**	**Celular**	**Correo Electrónico de Bomberos**	**Correo Electrónico personal**

Anexo 11: Directorio de contactos externos

BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA	Unidad de Tecnologías de Información y Comunicaciones			Código:
				Versión 1.0
	Directorio de Contactos externos			Oficio de Aprobación:
	Escrito Por: Luis Alejandro Madrigal Benavides.	Revisado Por:	Aprobado por:	Fecha de Aprobación:

Contiene Información sobre los proveedores externos					
Nombre del proveedores	**Persona a contactar**	**Teléfono(s)**	**Celular**	**Correo Electrónico**	**Dirección**

10- CONTROL DE VERSIONES

Versión	Fecha	Origen del cambio

Revisado por:

Jefatura de TIC

Aprobado por:

Comité de TIC