**UNIVERSIDAD GABRIELA MISTRAL**

**FACULTAD DE INGENIERIA**

# PLAN DE CONTINGENCIA INFORMATICO

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : Carlos Mellado Erices

Profesor Guía : Roberto Caru Cisternas

Profesor Integrante : Jorge Tapia Castillo

Santiago – Chile

Abril, 2014

# *DEDICATORIA*

A mi esposa Carola y a mis hijos Daniel y Sofía, por el apoyo incondicional que me han entregado durante estos dos años. Todo el esfuerzo no ha sido en vano, el conocimiento adquirido me ha permitido ser cada día una mejor persona.

A mi madre y padre por darme las herramientas que me han permitido afrontar las dificultades que se me han presentado en la vida.

A dios, por permitirme ser una mejor persona.

# *AGRADECIMIENTOS*

Debo realizar un especial agradecimiento a la Municipalidad de Santiago, por permitirme la posibilidad de crecer como profesional y en especial por todo el apoyo brindado durante estos últimos dos años.

A la Universidad Gabriela Mistral y a sus profesores por la entrega incondicional de sus conocimientos, la cual me ha permitido ser un mejor profesional.

# *INDICE*

# *1. INTRODUCCION*

Todos los planes de contingencia apuntan a las actividades que se deben realizar para evitar o minimizar el impacto de una contingencia y a recuperar el mayor porcentaje posible de nuestra plataforma informática dañada por alguna razón.

Esto es muy importante ya que un plan de contingencia mal enfocado puede conducir a pérdidas monetarias importantes en una organización.

A pesar de los avances en los sistemas operativos, que en alguna medida previenen la pérdida de información, los desastres dentro de las organizaciones siguen ocurriendo, cuando un desastre ocurre puede significar una pérdida importante de la información y muchas organizaciones no son capaces de sobrevivir cuando la interrupción se produce por mucho tiempo.

La I. Municipalidad de Santiago se encuentra en un proceso de modernización informática que implica el reemplazo de los sistemas que se encuentran licitados, por desarrollos propios.

Actualmente no existe un proceso asociado a salvaguardar la información contra daños producidos por hechos naturales o por causa del hombre.

Para la I. Municipalidad de Santiago es importante disponer de todos sus sistemas informáticos para la correcta entrega de sus servicios diarios a la comunidad.

Es por esta razón que se hace indispensable la creación de un sitio distinto al actual y para eso se ha decidido habilitar en la sucursal de Amunategui un espacio físico que contenga las mismas características que el actualmente ubicado en el edificio Santo Domingo.

Los procedimientos deben poseer la característica de poder ser entendidos por personas que posean algún conocimiento en informática, no necesariamente expertos. Es decir, poder tomar los procedimientos y habilitar nuevamente los sistemas en forma rápida y oportuna.

## *1.1. Municipalidad de Santiago*

La I. Municipalidad de Santiago es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, a quien corresponde la administración de la comuna de Santiago, cuya finalidad es satisfacer las necesidades de la comunidad local y asegurar su participación en el progreso económico, social y cultural de la comuna.

Está constituida por un alcalde y un concejo comunal electos directamente por un periodo de 4 años, renovable. La municipalidad es asesorada por un Consejo Económico y Social Comunal (CESCO), integrado por representantes de las actividades y organizaciones comunales importantes.

## *1.2. Organigrama Municipalidad de Santiago*

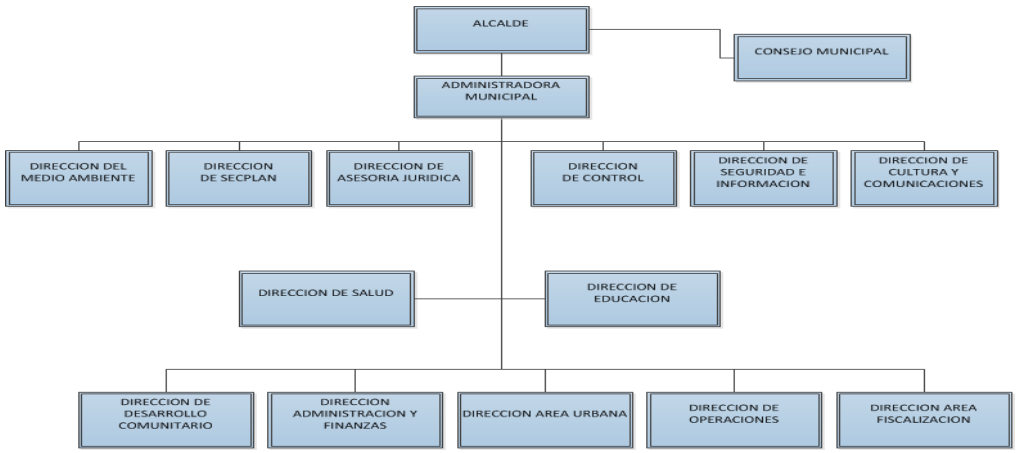


Figura 1. Organigrama I. Municipalidad de Santiago

## *1.3. Hipótesis*

Este trabajo se fundamenta en desarrollar una metodología que nos permita implementar procedimientos claros para la recuperación de los sistemas críticos de la municipalidad de Santiago y así poder mitigar las consecuencias que podría ocasionar un desastre informático.

## *1.4. Objetivo general*

El objetivo de este proyecto es diseñar un plan que permita a la municipalidad la recuperación de los sistemas informáticos en forma rápida y oportuna en caso de desastres. Para eso se propone la creación de otro Sitio que contenga las mismas características que el principal.

## *1.5. Objetivo específicos*

- Determinar la plataforma tecnológica actual.
- Identificar vulnerabilidades de la plataforma actual.
- Proponer medidas preventivas para aminorar ocurrencia de desastres
- Diseñar un plan de respaldo de información
- Diseñar un plan de recuperación

## *1.6. Alcance*

El alcance de este plan de contingencia guarda relación con la infraestructura informática, así como los procedimientos relevantes de su departamento asociados con dicha plataforma.

Entendemos como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio bajo su responsabilidad.

# 2. MARCO TEORICO

Debido a que las organizaciones dependen fuertemente de la tecnología para el correcto funcionamiento de sus operaciones, el plan de contingencia informático es un documento que reúne un conjunto de procedimientos alternativos para asegurar la continuidad de las operaciones de una organización.

## 2.1. Plan de contingencia

### 2.1.1. Qué es un plan de contingencia informático

Un plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de una organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa.

Estos planes lo que pretenden es garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad. Los planes incluyen cuatro etapas básicas: evaluación, planificación, pruebas de viabilidad y ejecución.

Los especialistas recomiendan planificar cuando aún no es necesario; es decir, antes de que sucedan los accidentes. Por otra parte, un plan debe ser dinámico y debe permitir incluir alternativas frente a nuevas incidencias que se pudiesen producir con el tiempo. Es por eso que un plan debe ser revisado y actualizado de forma periódica.

En concreto podemos establecer que todo plan de contingencia tiene que estar conformado a su vez por capítulos que definan las actividades para el respaldo, lo concerniente a la emergencia y lo que corresponda a la recuperación

de la información, es decir, serán los que establezcan las medidas a realizar, las amenazas a las que se hace frente y el tiempo de establecimiento de aquellas.

En primer lugar, está el plan de respaldo que es aquel que se encarga de determinar lo que son las medidas de prevención, es decir, las que se tienen que llevar a cabo con el claro objetivo de evitar que pueda tener lugar la materialización de una amenaza en concreto.

En segundo lugar, integra al proyecto de contingencia lo que es el plan de emergencia que, como su propio nombre indica, está conformado por el conjunto de acciones que hay que llevar a efecto durante la materialización de la amenaza y también después de la misma. Y es que gracias a aquellas se conseguirá reducir y acabar con los efectos negativos de aquella.

Y en tercer lugar está el plan de recuperación que se realiza después de la amenaza con el claro objetivo de recuperar el estado en el que se encontraban las cosas antes de que aquella se hiciera real.

En términos informáticos un plan de contingencia es un programa alternativo para que una organización pueda recuperarse de un desastre informático y restablecer sus operaciones con rapidez. Estos planes se conocen como DRP (Disaster Recovery Plan en inglés).

### *2.1.2. Beneficios de un plan de contingencia informático*

Algunos de los beneficios que nos entrega un buen plan de contingencia informática son:

- Reducir los riesgos que en caso de materializarse las amenazas que los originan, pueden presentar pérdidas económicas.
- Ahorro en tiempo y dinero al afrontar y corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio.

- Mejora la imagen y revaloriza la organización, mostrándoles a los clientes que se toman medidas diarias para garantizar la continuidad del negocio.

### *2.1.3. Dificultades para implementar un plan de contingencia*

Algunas dificultades se podrían presentar al tratar de llevar a cabo un proyecto orientado a la implantación de un plan de continuidad en TI, entre las que se pueden citar las siguientes:

- Falta de compromiso de la dirección.
- Los programas particulares no se integran entre sí.
- En el diseño del plan no se realiza una gestión correcta del riesgo.
- No se realizan pruebas completas del plan.
- Limitaciones de presupuesto.
- Falta de involucramiento del personal de la organización.

### *2.1.4. Tipos de planes de contingencia*

Teniendo en cuenta las características y prioridades de las funciones del servicio en donde puedan ocurrir los inconvenientes con el sistema de información y, en general, con todo lo que pueda estar relacionado con el área de sistemas en la institución, los planes previstos y no previstos se subdividen en tres, cada uno determina las medidas necesarias para lograr su objetivo.

- **Planes automatizados:** son los que le permiten tener resultados de forma automática por intermedio de dispositivos con idénticas funciones y características, con el propósito de otorgarle al usuario el mismo tipo de servicio, es decir al momento de una contingencia poner en funcionamiento el plan de forma rápida y oportuna.

- **Planes Semi-Automatizados**: en este tipo se deben ejecutar procesos tanto de forma manual, como automatizados, para obtener una solución al instante.
- **Planes Manuales:** se utilizan procedimientos manuales, esto significa que no hay ningún uso de sistemas automáticos de apoyo en reemplazo del proceso normal.

Los planes de contingencias siguen un ciclo de vida PHDCA (Planificar – Hacer – Comprobar – Actuar). Estos nacen de un análisis de riesgo donde se identifican los que afectan la continuidad del negocio.

### *2.1.5. Periodo máximo de interrupción*

Hay que tener en cuenta que el objetivo de un plan de continuidad tiene por finalidad la continuidad del negocio tras una contingencia grave y evitar pérdidas económicas significativas en la organización, es por eso que a los datos considerados críticos se les deben realizar copias de seguridad y estar a disposición para su pronta recuperación.

Antes de seleccionar una estrategia, se deben identificar los valores de recuperación de datos, los cuales se conocen como, tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO).

- RPO (Recovery Point Objetive): es el punto en el tiempo desde el cual recuperamos nuestra información. Es decir, la cantidad de información que se puede tolerar perder medido en tiempo desde el último respaldo disponible o bien desde el último trabajo de replicación exitosa.

- RTO (Recovery Time Objetive): es el tiempo en el que se vuelve a poner los servicios en funcionamiento para entregar nuevamente servicio a los usuarios o a los clientes.

El tiempo de recuperación objetivo y el punto de recuperación objetivo, son parámetros específicos que están íntimamente relacionados con la recuperación ante desastres y tienen que ser considerados para que un plan de este tipo pueda ser implementado.

A continuación, la figura 2 grafica los tiempos de recuperación, antes de provocar pérdidas económicas en la organización.

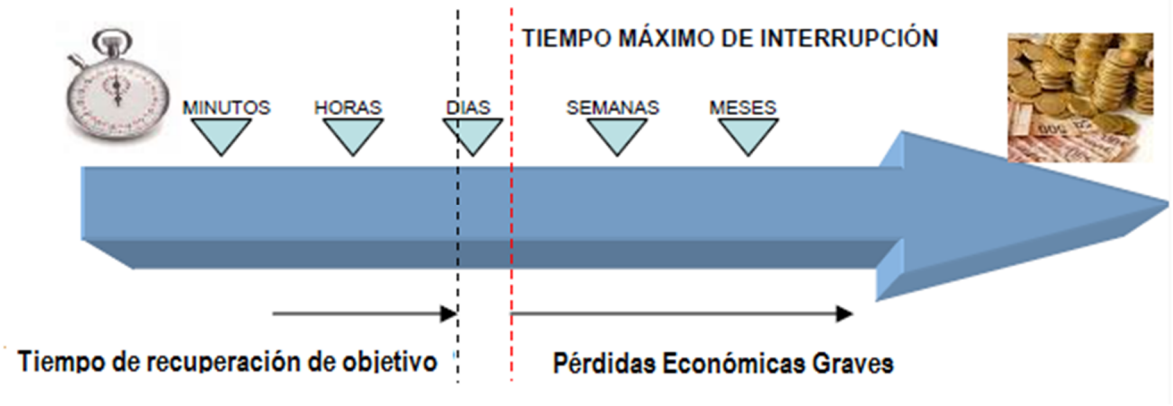


Figura 2. Tiempos de recuperación

Para cada caso en particular se debe analizar cuál es la mejor opción tecnológica de recuperación de acuerdo al tiempo de recuperación objetivo (RTO) y el punto de recuperación objetiva (RPO), como así también del presupuesto con el que se cuenta para el plan de contingencia.

## *2.2. Que es ITIL?*

La Biblioteca de infraestructura de tecnologías de la información más conocida como ITIL, se ha convertido en el estándar mundial, de facto, en la gestión de servicios informáticos. Desarrollado a finales de 1980, como una guía para el gobierno de Reino Unido, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Pertenece a la Oficina de Comercio del Gobierno Británico, pero es de libre utilización.

Uno de los principales beneficios propugnado por los defensores de ITIL dentro de la comunidad de Tecnologías Informáticas (TI) es que proporciona un vocabulario común, consistente en un glosario de términos precisamente definidos y ampliamente aceptados.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la informática para alcanzar sus objetivos. Esta dependencia en aumento ha dado como resultado la necesidad creciente de servicios informáticos de calidad que satisfagan los requisitos y las expectativas del cliente.

A lo largo de todo el ciclo de TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del costo, el resto se invierte en desarrollo del producto.

## 2.3. *Que beneficios tiene para nuestra organización*

Los beneficios están en la reducción efectiva de los costos, esto porque permite a los departamentos de TI entregar un servicio que satisface las necesidades del negocio.

ITIL proporciona extensos conjuntos de procedimientos necesarios para ayudar a nuestra organización a lograr una eficiencia en sus operaciones. Se deben establecer estándares que ayuden al control y administración de mejor manera de los recursos, para lo cual se debe hacer una revisión y probablemente una restructuración de los procesos existentes, lo cual permitirá una mejora continua.

La adopción de esta guía ofrece a los usuarios un amplio rango de beneficios que incluyen:

- Reducción de los gastos.
- Identificación rápida de potenciales problemas
- Reducir el tiempo promedio de solución a los incidentes
- Minimizar el tiempo de caída de los servicios
- Lograr el nivel de servicio especifico
- Continuidad del servicio

## *2.4. Soporte al servicio*

El soporte al servicio se preocupa de los aspectos que garantizan la continuidad, disponibilidad y calidad del servicio prestado.

A continuación la figura 3 grafica los principales aspectos de la metodología de soporte al servicio según ITIL.

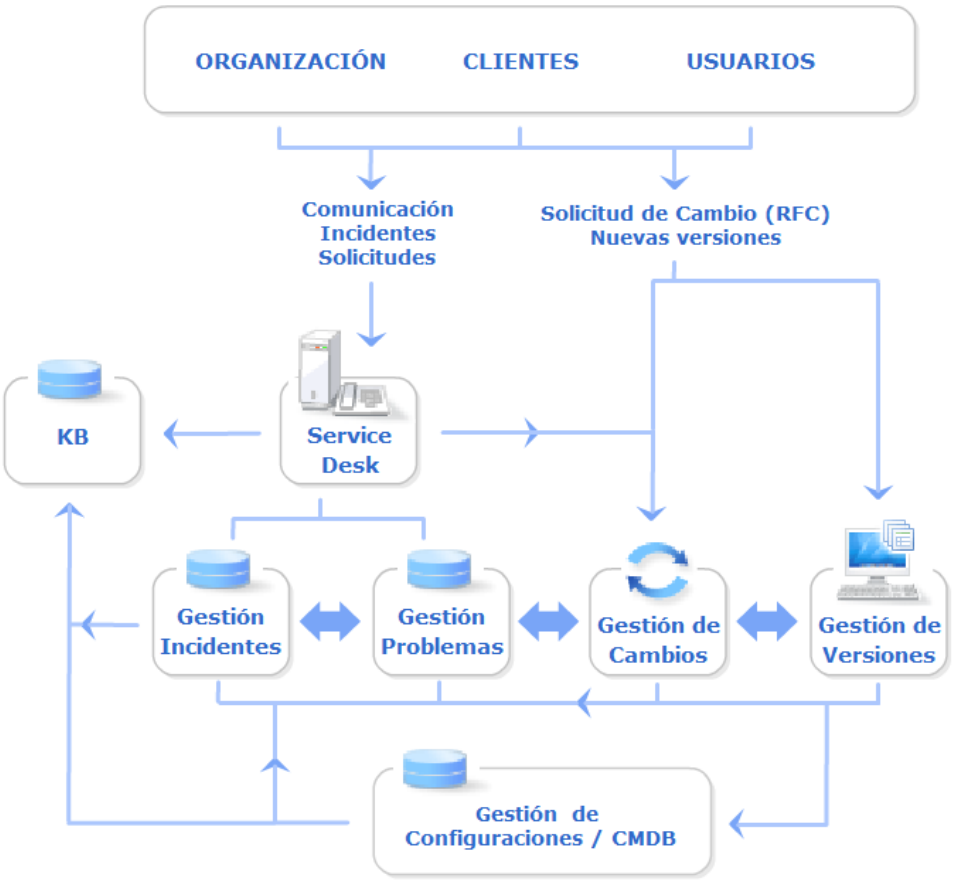


Figura 3. Diagrama soporte al servicio

### 2.4.1. *Gestión de configuración*

La principal función de la gestión de la configuración es la de llevar un registro actualizado de todos los elementos de configuración de la infraestructura TI junto a sus interrelaciones.

Este proceso debe interactuar con las gestiones de incidentes, problemas, cambios y versiones de manera de resolver más eficientemente las incidencias. Además de monitorear periódicamente la configuración de los sistemas en producción y contrastarla con la almacenada en la Base de Datos de la Gestión de Configuraciones (CMDB), para subsanar discrepancias.

Las principales actividades de esta gestión son:

**Planificación**

La Gestión de Configuraciones es uno de los pilares de la metodología ITIL por sus interrelaciones e interdependencias con el resto de los procesos. Por ello su implantación es particularmente compleja.

Una falta de planificación conducirá con total certeza a una Gestión de Configuraciones defectuosa, con las graves consecuencias que esto supondrá para el resto de los procesos.

Algunas consideraciones esenciales para la implementación de la gestión de configuraciones son:

- Designar un responsable.
- Invertir en alguna herramienta de software adecuada para las actividades requeridas.
- Realizar un análisis de los recursos ya existentes.
- Establecer claramente alcance y objetivos

**Clasificación y registros**

La principal tarea de la Gestión de Configuraciones es mantener la CMDB. Es imprescindible, para llevar esta labor con éxito, predeterminar la estructura del CMDB de manera que:

- Los objetivos sean realistas: una excesiva profundidad o detalle puede sobrecargar de trabajo a la organización y resultar, a la larga, en una dejación de responsabilidades.
- La información sea suficiente: debe existir, al menos un registro de todos los sistemas críticos para la infraestructura TI.

**Monitorización**

Es imprescindible conocer el estado de cada componente en todo momento de su ciclo de vida. Esta información puede ser de gran utilidad, por ejemplo, a la Gestión de Disponibilidad, para conocer que Elementos de Configuración (CIs) han sido responsables de la degradación de la calidad del servicio.

Puede ser de gran utilidad para el análisis el uso de herramientas de software que ofrezcan representaciones visuales del ciclo de vida de los componentes, organizados por diferentes filtros (tipo, fabricante, responsable, costos, etc.).

**Control**

La Gestión de Configuraciones debe estar puntualmente informada de todos los cambios y adquisiciones de componentes para mantener actualizada la CMDB.

El registro de todos los componentes de hardware debe iniciarse desde la aprobación de su compra y debe mantenerse actualizado su estado en todo

momento de su ciclo de vida. Asimismo, debe estar correctamente registrado todo el software "en producción".

Las tareas de control deben centrarse en:

- Asegurar que todos los componentes están registrados en la CMDB.
- Monitorizar el estado de todos los componentes.
- Actualizar las interrelaciones entre los elementos de configuración.
- Informar sobre el estado de las licencias.

**Realización de auditorías**

El objetivo de las auditorias es asegurar que la información registrada en la CMDB coincide con la configuración real de la estructura TI de la organización.

Existen herramientas que permiten una gestión remota, centralizada y automática de los elementos de configuración de hardware y software. La información recopilada puede ser utilizada para actualizar la CMDB.

### 2.4.2. *Gestión de incidentes*

Es la encargada de resolver cualquier incidente que cause una interrupción del servicio de manera rápida y eficaz.

Los objetivos principales de este proceso son:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Los beneficios de este proceso son:

- Mejora la productividad de los usuarios.
- Mayor control de procesos.

- Cumplimiento de niveles de servicio.
- Optimización de los recursos disponibles.
- Mejora la satisfacción general de clientes y usuarios.

Es frecuente que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas, este nivel se basa esencialmente en dos parámetros:

- **Impacto:** determina la importancia del incidente dependiendo de cómo este afecta a los procesos del negocio.
- **Urgencia:** depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente.

Es frecuente que el Centro de Servicios no sea capaz de resolver en primera instancia un incidente y para ello deba recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. A este proceso se le denomina escalado.

Básicamente hay dos tipos diferentes de escalado:

- **Escalado funcional:** Se requiere el apoyo de un especialista de más alto nivel para resolver el problema.
- **Escalado jerárquico:** Debemos acudir a un responsable de mayor autoridad para tomar decisiones que se escapen de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico.

Los procesos implicados en la correcta gestión de cambios son:

**Registro**

Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, el mismo Centro de Servicios o el soporte técnico, entre otros.

El proceso de registro debe realizarse inmediatamente pues resulta mucho más costoso hacerlo posteriormente y se corre el riesgo de que la aparición de nuevas incidencias demore indefinidamente el proceso.

**Clasificación**

La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser utilizada para la resolución del mismo. El proceso de clasificación debe implementar al menos, la categorización, establecer el nivel de prioridad, asignación de recursos y monitorizar el estado y tiempo de respuesta esperado.

**Análisis, resolución y cierre de incidentes**

Si la resolución del incidente se escapa de las posibilidades del Centro de Servicios éste re direcciona el mismo a un nivel superior para su investigación por los expertos asignados. Si estos expertos no son capaces de resolver el incidente se seguirán los protocolos de escalado predeterminados.

Si fuera necesario se puede emitir una Petición de Cambio. Si la incidencia fuera recurrente y no se encuentra una solución definitiva al mismo se deberá informar igualmente a la Gestión de Problemas para el estudio detallado de las causas subyacentes.

### *2.4.3. Gestión de problemas*

Este proceso requiere un registro de los incidentes que nos permita identificar la causa y realizar un análisis.

La gestión de problemas puede ser:

- **Reactiva**: analiza los incidentes ocurridos para descubrir su causa y propone soluciones a los mismos.
- **Proactiva**: monitoriza la calidad de la infraestructura TI y analiza su configuración con el objetivo de prevenir incidentes, incluso antes de que estos ocurran.

Cuando un incidente se convierte en recurrente o tiene un impacto en la infraestructura TI, es la función de la gestión de problemas la encargada de determinar las causas y sus posibles soluciones para dichas causas.

Cabe diferenciar entre:

- **Problema:** causa aun no identificada.
- **Error conocido:** problema que se transforma en un error conocido, ya se conocen sus causas.

Los beneficios de una correcta gestión de problemas:

- Aumento de la calidad de los servicios TI.
- Se minimiza el número de incidentes.
- Los incidentes se solucionan más rápidamente y generalmente en la primera línea de soporte.
- La documentación desarrollada es de gran utilidad para la gestión de la capacidad, disponibilidad y niveles de servicio.

Las principales actividades de la Gestión de Problemas son el:

- **Control de Problemas:** se encarga de registrar y clasificar los problemas para determinar sus causas y convertirlos en errores conocidos.

- **Control de Errores:** registra los errores conocidos y propone soluciones a los mismos mediante petición de cambios que son enviadas a la Gestión de Cambios. Asimismo efectúa la Revisión Post Implementación de los mismos en estrecha colaboración con la Gestión de Cambios.

Una eficaz Gestión de Problemas también requiere determinar claramente quienes son los responsables de cada proceso. Sin embargo, en pequeñas organizaciones es recomendable no segmentar en exceso las responsabilidades para evitar los costos asociados: sería poco eficaz y contraproducente asignar recursos humanos desproporcionados al proceso de identificación y solución de problemas.

### *2.4.4. Gestión de cambios*

El objetivo principal de la gestión de cambios es la evaluación y planificación del proceso de cambio para asegurar que, si se lleva a cabo, se realice de la forma más eficiente, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio.

Los principales beneficios derivados de una correcta gestión del cambio son:

- Se reduce el número de incidentes y problemas potenciales.
- Se puede retornar a configuraciones estables de manera sencilla.
- Se reduce el número de “back-outs” necesarios.
- Los cambios son mejor aceptados.
- Se evalúan los verdaderos costos asociados al cambio.

- La CMDB está correctamente actualizada.
- Se desarrollan procedimientos de cambio estándar que permiten la rápida actualización de sistemas no críticos.

En principio, todo cambio debe estar dentro de las tareas de la Gestión de Cambios. Sin embargo a veces es imposible gestionar todos los cambios mediante este proceso. El alcance de la Gestión de Cambios debe ir en paralelo con el de la Gestión de la configuración, es decir, todos los cambios deben estar registrados en la CMDB y así también ser correctamente supervisados y registrados.

Los procesos de la gestión de cambios son:

**Registro**

El primer paso del proceso de cambio es registrar adecuadamente las peticiones del cambio.

Para cambios de escasa importancia o que se repiten periódicamente pueden acordarse procedimientos estándar que no requieran la aprobación de la Gestión de Cambios en cada caso.

**Aceptación y clasificación**

Tras el registro de la petición del cambio se debe evaluar preliminarmente su pertinencia. Una petición de cambio puede ser rechazada si se considera que el cambio no está justificado o se puede solicitar su modificación si se considera que algunos aspectos de la misma son susceptibles de mejora o mayor definición.

Tras su aceptación se deben asignar a la petición de cambios una prioridad y categoría dependiendo de la urgencia y el impacto de la misma.

La categoría determina la dificultad e impacto de la RFC y será el parámetro relevante para determinar la asignación de recursos necesarios, los plazos previstos y el nivel de autorización requerido para la implementación del cambio.

**Aprobación y planificación**

La planificación es esencial para una buena gestión del cambio. El consejo asesor del cambio debe reunirse periódicamente para analizar y eventualmente aprobar las peticiones de cambio pendientes y elaborar el calendario correspondiente.

Una vez aprobado el cambio debe evaluarse si este ha de ser implementado aisladamente o dentro de un paquete de cambios.

**Implementación**

Aunque la Gestión de Cambios NO es la encargada de implementar el cambio, algo de lo que se encarga habitualmente la Gestión de Versiones, si lo es supervisar y coordinar todo el proceso.

**Evaluación**

Antes de proceder al cierre del cambio es necesario realizar una evaluación que permita valorar realmente el impacto del mismo en la calidad del servicio y en la productividad de la organización.

**Cambios de emergencia**

Aunque habitualmente los cambios realizados mediante procedimientos de emergencia son resultado de una planificación deficiente a veces resultan inevitables.

Cualquier interrupción del servicio de alto impacto, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas o servicios críticos para la organización, debe encontrar una respuesta inmediata. Es frecuente que la solución al problema requiera un cambio y que éste haya de realizarse siguiendo un procedimiento de urgencia.

### *2.4.5. Gestión de la seguridad*

La función de este proceso se relaciona con los procesos de gestión de servicios de TI, los que están basadas en tres pilares fundamentales:

- **Confidencialidad**: acceso a la información solo a quien corresponde.
- **Integridad**: la información debe ser correcta y completa.
- **Disponibilidad**: Acceso a la información cuando sea necesaria.

La gestión de la seguridad debe conocer en profundidad el negocio y los servicios que presta la organización TI para establecer protocolos de seguridad que aseguren que la información este a disposición del negocio y sea utilizada por los que tienen autorización para hacerlo.

Una vez comprendidos cuales son los requisitos de seguridad del negocio, la Gestión de la Seguridad debe supervisar que estos se hallen convenientemente plasmados en los acuerdos de niveles de servicio correspondientes para garantizar su cumplimiento.

La seguridad debe ser proactiva y evalúa a priori los riesgos de la seguridad que puedan suponer los cambios realizados en la infraestructura.

Los beneficios de una correcta gestión de seguridad son:

- Se evitan interrupciones del servicio causados por virus y ataques informáticos.
- Se minimiza el número de incidentes.
- Se tiene acceso a la información cuando se necesita y se preserva la seguridad de los datos.
- Se preserva la confidencialidad de los datos.
- Se cumplen las reglas de protección de datos.

- Mejora la percepción y confianza de los clientes y usuarios.

Los procesos de la gestión de la seguridad son:

**Plan de seguridad**

Este plan debe ser desarrollado en colaboración con la gestión de niveles de servicio, que es la responsable tanto de la calidad del servicio prestado a los clientes como del servicio recibido por la propia organización TI.

Un aspecto esencial a tener en cuenta es el establecimiento de protocolos de seguridad coherentes en todas las fases del servicio y para todos los estamentos implicados. "Una cadena es tan resistente como el más débil de sus eslabones", por lo que carece de sentido, por ejemplo, establecer estrictas normas de acceso si una aplicación tiene vulnerabilidades frente a inyecciones de SQL. Quizá con ello se puede engañar a algún cliente durante algún tiempo ofreciendo la imagen de "fortaleza" pero esto valdrá de poco si alguien descubre que la "puerta de atrás está abierta".

**Aplicación de medidas de seguridad**

Es necesario que la gestión de la empresa reconozca la autoridad de la Gestión de la Seguridad respecto a todas estas cuestiones y que incluso permita que ésta proponga medidas disciplinarias vinculantes cuando los empleados u otro personal relacionado con la seguridad de los servicios incumplan con sus responsabilidades.

**Evaluación y mantenimiento**

No es posible mejorar aquello que no se conoce, es por lo tanto indispensable evaluar el cumplimiento de las medidas de seguridad, sus resultados y el cumplimiento de los acuerdos de nivel de servicios.

Es asimismo importante que la Gestión de la Seguridad esté al día en lo que respecta a nuevos riesgos y vulnerabilidades frente a virus, spyware, ataques

de denegación de servicio, etcétera, y que adopte las medidas necesarias de actualización de equipos de hardware y software, sin olvidar que: el factor humano es normalmente el eslabón más débil de la cadena.

## *2.5. Provisión del servicio*

La provisión del servicio se ocupa de los servicios ofrecidos. En particular de los niveles de servicio, su disponibilidad, su continuidad, su viabilidad financiera, la capacidad necesaria de la infraestructura TI y los niveles de seguridad.

La figura 4, que se muestra a continuación resume los principales aspectos de la metodología de provisión del servicio según estándares ITIL.


Figura 4. Diagrama aspectos de la provisión de servicios

### *2.5.1. Gestión de niveles de servicio*

Es el proceso por el cual se definen, negocian y supervisan la calidad de los servicios TI ofrecidos.

Además es la responsable de buscar un compromiso realista entre las necesidades y expectativas del cliente y los costos de los servicios asociados.

Para cumplir sus objetivos es indispensable que la gestión de niveles de servicio conozca las necesidades de sus clientes, defina correctamente los servicios ofrecidos y monitoree la calidad del servicio.

Los beneficios son:

- Diseñados para cumplir sus auténticos objetivos.
- Se facilita la comunicación con los clientes impidiendo malentendidos.
- Se establecen objetivos claros y metrizables.
- Se establecen las responsabilidades respectivas de los clientes y proveedores de servicio.
- Los clientes conocen y asumen los niveles de calidad ofrecidos.
- La constante monitorización del servicio permite detectar los “eslabones más débiles de la cadena” para su mejora.
- La gestión TI conoce y comprende los servicios ofrecidos lo que facilita los acuerdos con proveedores y subcontratistas.

La Gestión de Niveles de Servicio es responsable de buscar un compromiso realista entre las necesidades y expectativas del cliente y los costos de los servicios asociados, de forma que estos sean asumibles tanto por el cliente como por la organización TI.

Las principales actividades de la Gestión de Niveles de Servicio se resumen en:

**Planificación**

La correcta planificación de la Gestión de Niveles de Servicio requiere la implicación de prácticamente todos los estamentos de la organización TI. Y, si esto no fuera ya de por sí una labor lo suficientemente compleja, resulta imprescindible la colaboración activa de los clientes y usuarios de los servicios TI.

**Implementación**

La fase de planificación debe concluir con la elaboración y aceptación de los acuerdos necesarios para la prestación del servicio.

Estos acuerdos incluyen los Acuerdos de Nivel de Servicio, Niveles de Operación y Contratos de Soporte.

**Monitorización**

El proceso de monitorización de los niveles de servicio es imprescindible si se quiere mejorar progresivamente la calidad del servicio ofrecido, su rentabilidad y la satisfacción de los clientes y usuarios.

La monitorización requiere el seguimiento tanto de procedimientos y parámetros internos de la organización como los relacionados con la percepción de los usuarios.

**Revisión**

Esta revisión debe realizarse en base a parámetros objetivos y metrizables resultado de la experiencia previa.

Este proceso de revisión no debe limitarse a aquellos SLAs que por una u otra razón ha sido incumplido, aunque, evidentemente, en estos casos sea

inexcusable, sino que debe tener como objetivo mejorar y homogeneizar la calidad del servicio.

### *2.5.2. Gestión financiera*

El principal objetivo de la gestión financiera es evaluar y controlar los costos asociados a los servicios TI, de forma que se ofrezca un servicio de calidad a los clientes, con un uso eficiente de los recursos TI.

Por regla general, a mayor calidad de los servicios mayor es su costo, por lo que es necesario evaluar cuidadosamente las necesidades del cliente para que el balance entre ambos sea óptimo.

Para lograr esto, la Gestión Financiera debe:

- Evaluar los costos reales de la prestación de servicios.
- Proporcionar al Departamento de TI toda la información financiera precisa para la toma de decisiones y fijación de precios.
- Asesorar al cliente sobre el valor añadido que proporcionan los servicios TI prestados.
- Evaluar el retorno de las inversiones.
- Llevar la contabilidad de los gastos asociados a los servicios TI.

Los principales beneficios son:

- Se reducen los costos y aumenta la rentabilidad del servicio.
- Se ajustan, controlan, adecuan y justifican los precios del servicio.
- Los clientes controlan servicios que le ofrecen una buena relación costo/rentabilidad.
- La organización TI puede planificar mejor sus inversiones.
- Los servicios TI son usados más eficazmente.

- La organización TI funciona como una unidad de negocio y es posible evaluar su rendimiento.

La clasificación de costos por servicio o producto puede realizarse en virtud de uno o más criterios, algunos de ellos son:

- **Costos Directos:** son los relacionados específicamente con un producto o servicio, por ejemplo, los servidores.
- **Costos Indirectos:** aquellos que no son específicos y exclusivos de un servicio, por ejemplo, la conectividad de la organización TI.
- **Costos Fijos:** son independientes del volumen de producción.
- **Costos Variables:** incluyen los que dependen del volumen de producción, por ejemplo, gastos en personal.
- **Costos de capital:** Provienen de la amortización del activo fijo o inversiones a largo plazo.
- **Costos de Operación:** son los costos asociados al funcionamiento diario de la organización TI.

Las principales actividades de la Gestión Financiera se resumen en:

**Presupuestos**

Los presupuestos realizados pueden tener diferentes horizontes temporales. Pueden ser a corto plazo, incluyendo los costos de los servicios prestados en la actualidad, o resultar de una proyección sobre la evolución prevista del negocio en dos o más años.

Es imprescindible que los presupuestos tengan en cuenta estas incertidumbres y se muestren precavidos al respecto para evitar que se conviertan en papel mojado al menor vaivén del mercado.

**Contabilidad**

Es esencial que el proceso contable tenga en cuenta la complejidad de las interrelaciones TI y a su vez no alcance un excesivo nivel de detalle que lo encarezca más allá de lo razonable.

Una de las actividades principales de la Gestión Financiera es identificar los denominados elementos de costo que se pueden clasificar de forma genérica en: costos de hardware y software, costos de Personal y costos generales.

**Fijación de precios**

Para que la organización TI pueda funcionar como una verdadera unidad de negocio es imprescindible tanto conocer los costes reales de los servicios prestados como establecer una política de precios que, cuando menos, permita recuperar los costos en los que se ha incurrido.

**Supervisión**

No es tarea de la Gestión Financiera de los Servicios TI sino de la Gestión de Niveles de Servicio negociar con los clientes y elaborar el catálogo de servicios. Sin embargo, es recomendable que, en los aspectos económicos, su actividad sea supervisada por la Gestión Financiera.

### *2.5.3. Gestión de la capacidad*

Es la encargada de que todos los servicios se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada.

Entre las responsabilidades se encuentran:

- Asegurar que se cubran las necesidades de capacidad TI tanto presentes como futuras.

- Controlar el rendimiento de la infraestructura TI.
- Desarrollar planes de capacidad asociados a los niveles de servicio acordados.
- Gestionar y racionalizar la demanda de servicios TI.

La gestión de la capacidad intenta evitar situaciones en las que se realizan inversiones innecesarias en tecnologías que no están adecuadas a las necesidades reales del negocio o por el contrario evitar que la productividad se vea mermada por un insuficiente uso de las tecnologías.

Los beneficios son:

- Se optimizan el rendimiento de los recursos informáticos.
- Se dispone de la capacidad necesaria en el momento oportuno, evitando que se recienta la calidad del servicio.
- Se evitan gastos innecesarios producidos por compras de última hora.
- Se planifica el crecimiento de la infraestructura adecuándolo a las necesidades reales del negocio.
- Se reducen los gastos de mantenimiento y administración asociados a equipos y aplicaciones obsoletas.
- Se reducen posibles incompatibilidades y fallos en la infraestructura informática.

Los procesos de la gestión de capacidad son:

**Planificación**

El Plan de Capacidad debe incluir información sobre los costos de la capacidad actual y prevista. Esta información es indispensable para que la Gestión Financiera pueda elaborar los presupuestos y previsiones financieras de manera realista.

Cuanto más compleja sea una infraestructura informática más difícil es prever las necesidades de capacidad futura. En esos casos, es imprescindible

realizar modelos y simulaciones sobre posibles escenarios de desarrollo futuro que aseguren la correcta escalabilidad de las aplicaciones y hardware.

**Recursos**

Es importante que la Gestión de la Capacidad participe en las primeras etapas de desarrollo de un producto, servicio o definición de un SLA para asegurar que se dispondrá de la capacidad necesaria para llevar el proyecto a buen término.

**Supervisión**

La Gestión de la Capacidad es un proceso continuo e iterativo que monitoriza, analiza y evalúa el rendimiento y capacidad de la infraestructura TI y con los datos obtenidos optimiza los servicios o eleva una petición de cambios (RFC) a la Gestión de Cambios.

**Gestión de la demanda**

El objetivo de la Gestión de la Demanda es el de optimizar y racionalizar el uso de los recursos TI.

Aunque la Gestión de la Demanda debe formar parte de las actividades rutinarias de la Gestión de la Capacidad ésta cobra especial relevancia cuando existen problemas de capacidad en la infraestructura TI.

La Gestión de la Demanda es la encargada en estos casos de redistribuir la capacidad para asegurar que los servicios críticos no se vean afectados o, cuando menos, lo sean en la menor medida posible. Para llevar a cabo esta tarea de forma eficiente es imprescindible que la Gestión de la Capacidad conozca las prioridades del negocio del cliente y pueda actuar en consecuencia.

### *2.5.4. Gestión de la disponibilidad*

Es la responsable de optimizar y monitorear los servicios TI para que estos funcionen ininterrumpidamente y de manera fiable, cumpliendo los acuerdos y todo ello a un costo razonable. La satisfacción del cliente y la rentabilidad de los servicios TI dependen en gran medida de su éxito.

Las responsabilidades son:

- Determinar los requisitos de disponibilidad en estrecha colaboración con los clientes.
- Garantizar el nivel de disponibilidad establecido para los servicios TI.
- Monitorizar la disponibilidad de los sistemas TI.
- Proponer mejoras en la infraestructura y servicios TI con el objetivo de aumentar los niveles de disponibilidad.
- Supervisar el cumplimiento de los acuerdos de nivel de operación y contrato de soporte acordados con proveedores internos y externos.

Los indicadores clave sobre los que se sustenta el proceso de Gestión de la Disponibilidad se resumen en:

- **Disponibilidad:** porcentaje de tiempo sobre el total acordado en que los servicios TI han sido accesibles al usuario y han funcionado correctamente.
- **Fiabilidad:** medida del tiempo durante el cual los servicios han funcionado correctamente de forma ininterrumpida.
- **Mantenibilidad:** capacidad de mantener el servicio operativo y recuperarlo en caso de interrupción.
- **Capacidad de Servicio:** determina la disponibilidad de los servicios internos y externos contratados y su adecuación a los Acuerdos de Nivel de Operación (OLAs) y los Contratos de Soporte (UCs) en vigor. Cuando un

servicio TI es subcontratado en su totalidad la disponibilidad y la capacidad de servicio son términos equivalentes.

Los beneficios son:

- Cumplimiento de los niveles de disponibilidad acordados.
- Se reducen los costos asociados a un alto nivel de disponibilidad.
- El cliente percibe una mayor calidad de servicio.
- Se aumentan progresivamente los niveles de disponibilidad.
- Se reduce el número de incidentes.

Los procesos de la gestión de la disponibilidad son:

**Requisitos**

Aunque en principio todos los clientes estarán de acuerdo con unas elevadas cotas de disponibilidad es importante hacerles ver que una alta disponibilidad puede generar unos costos injustificados dadas sus necesidades reales.

**Planificación**

La correcta planificación de la disponibilidad permite establecer unos niveles de disponibilidad adecuados tanto en lo que respecta a las necesidades reales del negocio como a las posibilidades de la organización TI.

**Mantenimiento y Seguridad**

Aunque hayamos realizado un correcto diseño de los servicios según el Plan de Disponibilidad y se hayan tomado todas las medidas preventivas necesarias, tarde o temprano, nos habremos de enfrentar a interrupciones del servicio.

En esos casos es necesario recuperar el servicio lo antes posible para que no tenga un efecto indeseado sobre los niveles de disponibilidad acordados.

**Monitoreo de la disponibilidad**

La monitorización de la disponibilidad del servicio y la elaboración de los informes correspondientes son dos de las principales actividades de la Gestión de la Disponibilidad.

**Métodos y técnicas**

Es habitual definir la disponibilidad en porcentajes y se hace de la siguiente manera:

$$\% \text{ Disponibilidad} = \frac{(AST - DT)}{AST} \cdot 100$$

Dónde:

- **AST=** Tiempo acordado de servicio.
- **DT=** Tiempo de interrupción

La Gestión de la Disponibilidad tiene a su disposición un buen número de métodos y técnicas que le permiten determinar qué factores intervienen en la disponibilidad del servicio y que le permiten consecuentemente prever que tipo de recursos se deben asignar para las labores de prevención, mantenimiento y recuperación, así como elaborar planes de mejora a partir de dichos análisis.

### *2.5.5. Gestión de la continuidad de servicio*

La gestión de la continuidad de servicio es la actividad que se lleva a cabo en una organización para asegurar que todos los procesos críticos del negocio estarán disponibles para los clientes. La gestión de la continuidad no se implanta cuando ocurre un desastre, sino que hace referencia a todas aquellas actividades

que se llevan a cabo diariamente para mantener el servicio y facilitar su recuperación.

La estrategia de esta gestión debe combinar procedimientos:

- **Proactivos:** se encargan de impedir o minimizar las consecuencias provocadas por una grave interrupción de los servicios.
- **Reactivos:** su propósito es reanudar los servicios tan pronto como sea posible y de la mejor manera, luego del desastre.

Los principales objetivos de la gestión de continuidad de servicio se resumen a:

- Garantizar la pronta recuperación de los servicios críticos TI tras un desastre.
- Establecer políticas y procedimientos que eviten, en la medida de lo posible, las consecuencias de un desastre o causa de fuerza mayor.

Las principales actividades de la gestión de continuidad se grafican en la figura 5.


Figura 5. Diagrama actividades de la gestión de continuidad

### *2.5.5.1. Alcance*

La gestión de la organización debe demostrar su implicación con el proceso desde un primer momento pues la implantación de la gestión de la continuidad de

servicio puede resultar compleja y costosa sin la contrapartida de un retorno obvio a la inversión.

La gestión de la continuidad de servicio está destinada al fracaso sino se destina una cantidad de recursos suficientes, tanto en el plano humano como de equipamiento tecnológico.

Hay que destinar un esfuerzo importante en la formación del personal, el cual debe conocer perfectamente las tareas que se espera desempeñe antes de que ocurra la emergencia.

### *2.5.5.2. Análisis de impacto*

El análisis de impacto de negocio, conocido comúnmente como BIA (Bussines Impact Analysis), será la guía que determine que necesita ser recuperado y el tiempo que tardara dicha recuperación. El apoyo del BIA es invaluable para identificar que está en riesgo una vez que se presente la contingencia permitiendo así justificar los gastos que se requieren en protección y capacidad de recuperación.

La realización del BIA se inicia identificando los procesos que se realizan en la organización, y asignándoles un líder. Con los líderes de proceso se puede conformar un equipo de planeación que hará la evaluación del proceso que tengan asignado. Una vez identificados los procesos y sus líderes, se debe listar cada una de las actividades que se realiza para cada uno de los procesos para entender cuál es el propósito de los mismos, aquí se debe analizar cada actividad que se ejecute en tres aspectos: riesgo financiero de no ejecutar la actividad, riesgo regulatorio o legal de no ejecutar tal actividad, y el riesgo de reputación o con el cliente de no ejecutar la actividad.

- **Financiero:** incluye pérdida de ingresos, perdida de intereses con entidades bancarias, penalización por no cumplir compromisos contractuales.
- **Regulatorio:** perdidas por no presentar reportes financieros o de impuestos en las fecha indicadas.
- **Reputación o con el cliente:** incluye la pérdida de confianza de los clientes, reclamos, clientes insatisfechos por el servicio, apariciones en noticias por quejas de clientes.

La organización debe revisar cada una de las tareas con el mismo patrón de referencia y calcular cuánto tiempo pueden dejar de realizar esta actividad sin que ello cause perdidas económicas. Todos los procesos de la organización, así como los recursos tecnológicos en los que se soportan tales procesos deben ser clasificados de acuerdo a su prioridad de recuperación.

#### *2.5.5.3. Evaluación del riesgo*

Si no se conocen los riesgos reales a los que se enfrenta la infraestructura TI es imposible realizar una política de prevención y recuperación ante desastres.

La gestión de la continuidad del servicio debe enumerar y evaluar, dependiendo de su probabilidad e impacto, los diferentes factores de riesgos. Este concepto general está representado en la figura 6, el que muestra el análisis de riesgos y su gestión, las cuales están relacionadas entre sí pero como actividades separadas.


Figura 6. Diagrama de riesgos

Gracias a los resultados de este detallado análisis se dispondrá de información suficiente para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio.

La prevención frente a riesgos genéricos y poco probables puede resultar muy cara y no estar siempre justificada, sin embargo, las medidas preventivas o de recuperación frente a riesgos específicos pueden resultar sencillas, de rápida implementación y relativamente baratas.

### *2.5.5.4. Estrategias de continuidad*

La continuidad de servicios debe conseguirse mediante medidas preventivas, que eviten la interrupción del servicio TI, o por el contrario medidas reactivas, que permitan recuperar los servicios en el menor tiempo posible.

En este caso se deben diseñar actividades de prevención de incidentes y de recuperación.

- **Actividades preventivas:** requieren de un análisis detallado del riesgo y vulnerabilidades.
- **Actividades de recuperación:** por muy eficientes que sean las actividades de prevención, será necesario poner en marcha los procedimientos de recuperación.

### *2.5.5.5. Organización y planificación*

En este proceso es necesario asignar y organizar los recursos necesarios. Para lo cual se deben generar una serie de documentos entre los que se incluyen:

- **Plan de prevención de riesgos:** su objetivo es evitar o minimizar el impacto de un desastre en la infraestructura TI.
- **Plan de gestión de emergencias:** en caso de una situación de emergencia es indispensable que estén claramente determinadas las responsabilidades y funciones del personal así como los protocolos de acción.
- **Plan de recuperación:** cuando la interrupción es inevitable y llega el momento de poner en marcha el plan de recuperación se debe considerar: reorganizar el personal involucrado, restablecer los sistemas y recuperar datos.

Cuando se pone en marcha el plan de recuperación no hay espacio para la improvisación, porque cualquier decisión puede tener graves consecuencias.

Aunque pueda resultar paradójico, un “desastre” puede ser una buena oportunidad para demostrar a nuestros clientes la solidez de nuestra organización TI y por lo tanto incrementar su confianza.

### *2.5.5.6. Supervisión*

Una vez que se establecen las políticas, estrategias y planes de prevención y recuperación es indispensable que la organización se prepare para su correcta implementación. Para ello depende de dos factores:

- **Formación:** pueden existir unos planes de recuperación completísimos, pero si no existen personas que estén familiarizadas con los planes de prevención no servirá de nada.
- **Actualización y auditorias:** las políticas, estrategias y planes deben ser actualizados periódicamente para asegurar que respondan a los requisitos de la organización.

# *3. DESARROLLO DEL TRABAJO*

## *3.1. Antecedentes generales*

En la actualidad uno de los principales activos de las organizaciones es la información y por tanto, debe ser protegida. Para ello las organizaciones deben aportar los recursos necesarios con el objetivo de proporcionar la seguridad requerida.

En la mayoría de los casos, los costos ocasionados por las consecuencias de la pérdida de información son muy superiores a la inversión necesaria para prevenirla, y en algunas ocasiones puede producir daños irreparables.

La municipalidad durante años ha licitado sus sistemas informáticos, por periodo de 2 años renovables. En este proceso participan las empresas que poseen sistemas informáticos estándares para las municipalidades de Chile.

En este sentido cabe destacar que el constante cambio de proveedores informáticos, ha causado una enorme cantidad de problemas cada vez que se realizan las implementaciones. Es por eso que la administración municipal en su constante desempeño de otorgar un mejor servicio a la comunidad, decidió en el año 2010 crear una unidad de desarrollo de sistemas dentro del departamento de informática, la cual se encargara del diseño y desarrollo de los sistemas que irán de forma paulatina reemplazando todos los sistemas licitados.

Durante los últimos 3 años la I. Municipalidad de Santiago ha dedicado gran cantidad de recursos al diseño y desarrollo de sus sistemas informáticos, pero ha dejado de lado la importancia que tiene el proceso dedicado a salvaguardar la información ante un incidente.

Sin lugar a dudas la municipalidad entiende la necesidad de respaldar la información, pero sin embargo, colocaba esta problemática bien atrás en su lista de prioridades al momento de invertir.

A continuación se mencionan algunos de los incidentes ocurridos durante el último tiempo en la sala de servidores.

- El aire acondicionado dejo de funcionar, lo que ocasiono calentamiento de los servidores.
- Perdida de información correspondiente a giros e ingresos de dinero.
- Ingreso de personas no autorizadas a la sala de servidores.
- Instalación de programas no autorizado en los servidores de producción (ej. Ares, TeamViewer)

### *3.1.1. Situación Actual*

Le forma precaria en la cual se realizan los respaldos de la información crítica de la I. Municipalidad de Santiago, en dos discos duros externos de 1tb de capacidad cada uno, los cuales nadie supervisa para saber si el respaldo se ha hecho correctamente y cuál era la calidad de la información guardada. En varias ocasiones estos discos externos se han quedado sin espacio y han pasado varios días antes que alguien se dé cuenta de que la información no se ha respaldado.

Ase aproximadamente seis meses, la I. Municipalidad de Santiago gasto varios millones de pesos en la compra de una unidad de cintas HP StorageWorks, la cual permite realizar copias de seguridad sin supervisión y para su posterior recuperación. Esta unidad se encuentra en la sala de servidores y por distintas razones no se había puesto en funcionamiento.

Al no existir un procedimiento de cómo realizar los respaldos de la información crítica y que se debe hacer con estos mismos, es que todas las unidades de respaldo están en la misma sala de servidores y no hay una preocupación de mantener copias fuera del edificio, en caso que ocurra algún incidente en la sala de servidores.

### *3.1.2. Propuesta*

Ante los acontecimientos expuestos, se le ha propuesto a la I. Municipalidad de Santiago la necesidad de realizar una investigación que abarque la creación de un sitio distinto al actual, además de realizar copias de seguridad de forma periódica y tomar algunas medidas preventivas, todo esto con el objetivo de dar continuidad a las actividades ante futuros incidentes no previstos. Esto será abarcado más extensamente en capitulo “estrategias de continuidad”.

## *3.2. Definición de la Arquitectura actual*

La red de datos de la municipalidad se encuentra estructurada con la topología tipo árbol, es decir, a través de una topología de red en la que los nodos están organizados jerárquicamente en forma de árbol, desde una visión topológica, es parecida a una serie de redes en estrella interconectadas exceptuando en que no se tiene un nodo central, sino que varios nodos organizados en forma jerárquica.

La red de datos municipal, como se muestra en la figura 7, se interconecta lógicamente a través de redes con direccionamiento privado clase B, es decir, en una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts por cada red es de 65.534 hosts.

Esta estructura lógica de la red de datos permite que se interconecten sin problemas alrededor de 2000 host o equipos computacionales existentes en el municipio.

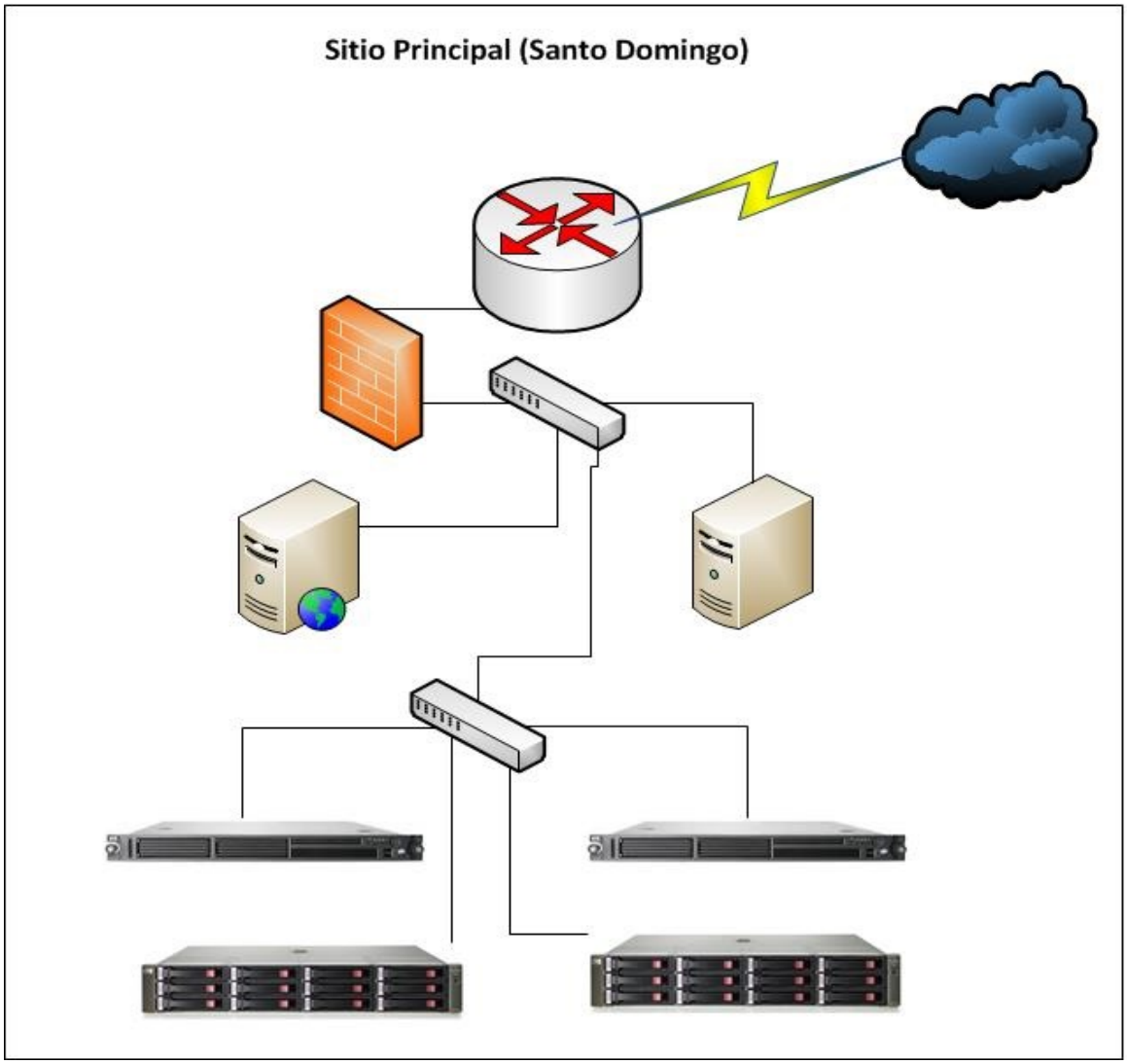


Figura 7. Diseño de la red municipal

## *3.3. Alcance*

El trabajo que se realiza a continuación tiene por objetivo la implementación de un plan de contingencia informático, que permita a la municipalidad restaurar los servicios informáticos lo antes posible, en caso de la ocurrencia de un desastre.

Durante el diseño del plan se han identificado los aplicativos, sistemas operativos, insumos, archivos de datos que resultan críticos para continuidad del negocio, así como los tiempos necesarios para la recuperación después de que se presenta el desastre.

Para este proceso de recuperación en caso de un desastre del sitio principal (DRP), utilizaremos el análisis de impacto, más conocido como BIA (Business Impact Analysis por sus siglas en ingles). El BIA será la guía que determine que necesita ser recuperado y el tiempo que tarde dicha recuperación. El apoyo del BIA es invaluable para identificar que está en riesgo una vez que se presente un riesgo permitiendo justificar los gastos que se requieren en protección y capacidad de recuperación.

## *3.4. Análisis de impacto*

El propósito fundamental del análisis de impacto sobre el negocio, conocido más comúnmente como BIA, (Business Impact Análisis) es determinar y entender que procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Este proceso es parte fundamental dentro de la elaboración de un plan de contingencia informática.

Para el desarrollo de este plan, se realizó un inventario de los sistemas de la municipalidad, estableciendo tiempos de recuperación de los mismos, antes de incurrir en pérdidas graves.

En reuniones sostenidas con las distintas entidades que interactúan en este proceso, se ha determinado el tiempo máximo que se puede


Figura 8. Impacto en el negocio

A continuación explicaremos la figura 8, la cual muestra la pérdida de datos (RPO) y el tiempo de interrupción (RTO).

- RTO (2 días): Significa que ante la ocurrencia de un incidente se debe tardar como máximo 2 días en poner los servicios en funcionamiento nuevamente, antes de incurrir en graves pérdidas económicas.
- RPO (1 minuto): La información recuperada tendrán una antigüedad de 1 minuto desde que ocurrió el incidente, esto quiere decir que la información perdida es aquella que se generó entre el último respaldo y el momento del incidente.

### *3.4.1. Identificación de procesos críticos*

La determinación de los procesos críticos son aquellos que provocaran impactos económicos y operacionales importantes en el negocio.

Para identificar los sistemas a recuperar mediante este plan de contingencia se consideraron diferentes elementos para establecer la calificación de criticidad de los sistemas, algunos de ellos fueron:

- Ingresos que se dejaran de recibir.
- Penalizaciones por incumplimiento de contratos con clientes.
- Demandas de los proveedores por no pago.
- Hora hombre por realizar trabajos de forma manual que son menos eficientes.
- Sanciones administrativas por incumplimiento de leyes.

A continuación se detallan los sistemas y su criticidad.

| Nombre Sistema | Descripción | Criticidad |
|---|---|---|
| Tesorería | Programa encargado de cobrar todos los giros realizados por los distintos sistemas municipales. | 1 |
| Patentes Comerciales | Sistema encargado de generar los cobros a las patentes comerciales de la comuna, además de llevar un registro actualizado de dichas patentes. | 1 |
| Adquisiciones | Este programa se encarga de todas las compras que realiza la municipalidad a los distintos proveedores. | 3 |
| Licencias conducir | Permite tomar el examen para el | 2 |

| | | |
|---|---|---|
| | otorgamiento de la licencia de conducir. | |
| Permisos circulación | Programa encargado de otorgar los permisos de circulación de los vehículos motorizados. | 2 |
| Gestión Documental | Este sistema se encarga de toda la documentación que circula por las oficinas de la municipalidad. | 3 |
| Declaración de trabajadores | Sitio Web, destinado a los contribuyentes para la declaración de número de trabajadores por patentes y las sucursales fuera de la comuna. | 3 |

Los rangos de criticidad son:

**1** = no pueden reemplazarse por métodos manuales y muy baja tolerancia a las interrupciones.

**2** = Pueden realizarse manualmente por un periodo breve y el costo de interrupción un poco más bajos.

**3** = Funciones que pueden interrumpirse por tiempos prolongados a un costo pequeño o nulo.

El proceso de Tesorería y Patentes Comerciales son claves para esta organización, ya que patentes comerciales es el encargado de generar los giros y tesorería de recaudarlos. Estos dos procesos generan alrededor del 70% de los ingresos percibidos por la municipalidad, los cuales ascienden aproximadamente a la suma de 300 millones de pesos diarios.

Para la unidad de rentas de la municipalidad es tan complejo realizar de forma manual el cobro de una patente, que realizar ese mismo proceso a 200 contribuyentes de la comuna de Santiago que acuden diariamente sería imposible. Es por esa misma razón que se determinó la importancia que estos procesos sean recuperados lo antes posible.

Aunque los procesos de adquisiciones, licencias de conducir, permisos de circulación y declaración de trabajadores son importantes, la municipalidad puede esperar semanas antes que se restablezcan.

### *3.4.2. Tiempo máximo de recuperación de los sistemas*

Teniendo en cuenta que el objetivo del plan es dar continuidad al negocio tras un incidente o contingencia grave con las menores perdidas económicas posibles para la municipalidad, estimaremos para cada uno de los procesos considerados críticos, el tiempo a partir del cual las pérdidas económicas afectaran gravemente a la municipalidad.

A continuación se detallan los sistemas y sus tiempos de recuperación.

| **Nombre sistema** | **Tiempos de recuperación** | **Criticidad** |
|---|---|---|
| Tesorería | 2 a 3 días | 1 |
| Patentes Comerciales | 2 a 3 días | 1 |
| Adquisiciones | 15 a 30 días | 3 |
| Licencias conducir | 5 a 10 días | 2 |
| Permisos circulación | 5 a 10 días | 2 |
| Gestión Documental | 15 a 30 días | 3 |
| Declaración de trabajadores | 15 a 30 días | 3 |

Cabe mencionar que los tiempos máximos de interrupción han sido definidos en conjunto con las áreas usuarias de los sistemas de información, con

el propósito de establecer cuanto tiempo los procesos TI, podrán estar sin operación entes que causen daños económicos a la municipalidad.

## *3.5. Análisis de riesgos*

El objetivo de este análisis es poner de manifiesto aquellas debilidades actuales de la municipalidad, que por su situación o su importancia pueden poner en marcha, antes de lo deseable el plan de recuperación. Es por eso que este análisis debe centrarse en los procesos o actividades del negocio que se han considerado críticos.

### *3.5.1. Inventario de activos*

Para cada uno de los procesos críticos de la municipalidad es necesario realizar un inventario de los activos involucrados en el proceso. Los activos se definen como los recursos de una organización que son necesarios para la consecución de sus objetivos de negocio. Ejemplos de activos de la municipalidad de Santiago son: Información, Equipamiento, Conocimiento, Sistemas.

A continuación se describen los activos más relevantes para la municipalidad.

| ACTIVO | TIPO | VALOR |
|---|---|---|
| Servidor de aplicaciones | Hardware | MEDIO |
| Sistema de tesorería | Aplicación | ALTO |
| Sistemas de patentes comerciales | Aplicación | ALTO |
| Sistema Adquisiciones | Aplicación | MEDIO |
| Sistema Licencias de conducir | Aplicación | MEDIO |

| | | |
|---|---|---|
| Sistema Permisos Circulación | Aplicación | MEDIO |
| Sistema Declaración de Trabajadores | Aplicación | MEDIO |
| Servidores de bases datos | Hardware | MEDIO |
| Información de clientes | Aplicación | ALTO |
| Redes de comunicaciones | comunicaciones | BAJO |

### *3.5.2. Amenazas*

Las amenazas tendrán una probabilidad de ocurrencia. Dependerá de la existencia de una vulnerabilidad que pueda ser explotada para materializarse como incidente.

A la hora de analizar los riesgos hay que evaluar las distintas amenazas, las cuales pueden provenir de diferentes fuentes, entre las cuales se incluyen los desastres naturales, amenazas no intencionales e intencionales.

A continuación se detallan las amenazas que puedan afectar a los sistemas de la municipalidad.

| AMENAZAS | POSIBLE |
|---|---|
| **DESASTRES NATURALES** | |
| Incendios | x |
| Terremotos | x |
| **DAÑOS ACCIDENTALES** | |
| Fuego fortuito | x |

| | |
|---|---|
| Fallo del aire acondicionado | x |
| Fallo de suministro eléctrico | x |
| Perdida de confidencialidad | x |
| Incumplimientos legales | x |
| **ATAQUES INTENCIONALES** | |
| Accesos no autorizados a las oficinas | x |
| Accesos no autorizados a datos de la municipalidad | x |
| Robo de equipos | x |
| Robo de datos / documentos | x |

### *3.5.3. Vulnerabilidades*

Las vulnerabilidades son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede causar daños graves a la municipalidad.

A continuación se detallan algunas vulnerabilidades que pueden afectar a los sistemas de la municipalidad.

| ESCENARIOS | NIVEL DE PROTECCION | RESPUESTA |
|---|---|---|
| 1.Fallas del suministro eléctrico | ¿Existen unidades de suministro eléctrico alternativos (ups)? | NO |
| 2.Perdida de información clave de la compañía | ¿Se realizan copias de los datos periódicamente? | NO |

| | | |
|---|---|---|
| 3.Acceso no autorizados al edificio | ¿Existe un control de acceso a las oficinas de la organización? | NO |
| 4.Robos de datos | ¿Existen perfiles adecuados de acceso a datos? | NO |
| 5.Falla en enfriamiento de la sala de servidores | ¿Existe más de un aire acondicionado en la sala? | NO |
| 6.Falla en la detección de fuego en la sala | ¿Existen detectores de humo en la sala? | NO |

Para identificar estas vulnerabilidades que pueden afectar a la municipalidad nos tuvimos que preguntar: ¿Cómo puede ocurrir una amenaza?

Si no se responde afirmativamente a las preguntas realizadas, se consideran como vulnerabilidad que podrían utilizarse de forma que la amenaza se convierta en incidente real y causar daños importantes en la municipalidad.

### *3.5.4. Evaluación de riesgos*

Cuanto más baja sea la probabilidad de ocurrencia (no existen vulnerabilidades) y el impacto sobre la municipalidad sea también bajo, se estará en un nivel de riesgo bajo.

Sin embargo, si existen vulnerabilidades que aumenten la probabilidad de ocurrencia o el impacto del incidente sea alto para la municipalidad, se estará en unos niveles de riesgo medio-alto.

A continuación se muestra la siguiente tabla con la probabilidad de ocurrencias.

| DESCRIPCION | PROBABILIDAD | IMPACTO | RIESGO |
|---|---|---|---|
| Terremotos | Media | Medio | Medio |
| Perdida del servicio por fallas de alimentación eléctrica | Alta | Medio | Alto |
| Accesos no autorizados a las oficinas | Alta | Alto | Alto |
| Robo de información confidencial de la municipalidad | Media | Alto | Medio |
| Perdida de información crítica de la municipalidad | Media | Alto | Medio |

## *3.6. Estrategias de continuidad*

### *3.6.1. Actividades preventivas*

Para mitigar los riesgos detectados y mitigarlos en la medida de lo posible, se han recomendado a la dirección de informática, la puesta en marcha de algunas contramedidas que permitan mitigar en la medida de lo posible los riesgos, algunas de ellas se detallan continuación:

- Realizar copias de seguridad periódicamente.
- Controlar el acceso a la información estableciendo mecanismos de autenticación.
- Establecer un control de acceso físico al lugar donde se encuentran los equipos con información clave para la municipalidad.
- Establecer detectores de humo y alarmas de fuego.
- Instalación aire acondicionado duplicado (respaldo).
- Comprar e instalar ups.

Las medidas que se han puesto en marcha para mitigar los riesgos son una proporción entre el esfuerzo y el costo necesarios para su implantación, para lo cual se realizó una evaluación costo-beneficio.

### *3.6.2. Estrategias de recuperación*

Una estrategia de recuperación es la que identifica la mejor manera de recuperar el funcionamiento de un sistema informático en caso de desastre y provee una guía necesaria para un correcto desarrollo de los procedimientos necesarios para dicha recuperación.

Es importante destacar que cuando se diseña una estrategia de recuperación de la información se deben tomar en cuenta algunos factores que agregan más complejidad a la estrategia utilizada:

- **Disponibilidad**: para la municipalidad los sistemas deben estar disponibles todo el tiempo posible, es por eso que la estrategia debe adaptarse a esta necesidad.
- **Capacidad**: se debe garantizar que todos los datos necesarios estén siendo respaldados adecuadamente.
- **Frecuencia**: se debe tener los datos lo más actualizados posibles.

En el caso de la municipalidad por poseer distintas sedes, se han propuesto dos estrategias para mitigar el impacto de una interrupción, las cuales se detallan a continuación.

### *3.6.3. Plan de Respaldos*

Para esto se considera el uso de una unidad de respaldo HP StorageWorks MSL2024, la cual posee el software HP Data Protector, que permite generar copias de seguridad sin supervisión, con capacidad de archivado. Las cintas de respaldos serán almacenadas fuera del edificio donde está el sitio principal.

Las cintas de respaldos serán rotuladas de tal forma que indiquen:

- Nombre del área de servicios informáticos
- Sistemas al que pertenecen los archivos
- Fecha y hora de realización de la copia
- Número que identifique la copia.
- Retención.

Se ha determinado que el respaldo de la información más importante para la continuidad del servicio debe ser diario y se realizarán durante las noches, debido a que en ese horario los sistemas tienen menos uso y hay menos probabilidades de ocasionar alguna interrupción en el normal funcionamiento de ellos.

### *3.6.4. Sitio alternativo (de contingencia)*

Dentro de este plan de continuidad se propuso la implementación de un sitio de contingencia distinto al principal, el cual comprenderá servidores, redes y almacenamiento de datos. Esta solución impone algunos desafíos adicionales a las soluciones de redundancia, y podríamos generalizar diciendo que aquí se vuelve imprescindible la distribución geográfica de la solución.

Si bien en los esquemas de redundancia existe una capa externa a los servicios en sí que permite la sincronización de la operación de todos los componentes de la infraestructura, en los esquemas de contingencia es necesaria una capa adicional que provea los servicios de replicación de datos, para asegurar que sea cual sea el nodo que se encuentre operando en cualquier momento, los datos sean siempre los mismos o al menos estén lo más actualizados posible.

Esta solución utilizará el método de “replicación asincrónica” de datos, por software, esto significa que el sitio de producción operará de forma independiente a como se replican los datos, generando un punto de recuperación mayor, pero ofrece más flexibilidad y mejor tiempo de respuesta de la aplicación en producción.

A continuación en la figura 9 se muestra en forma gráfica la solución:

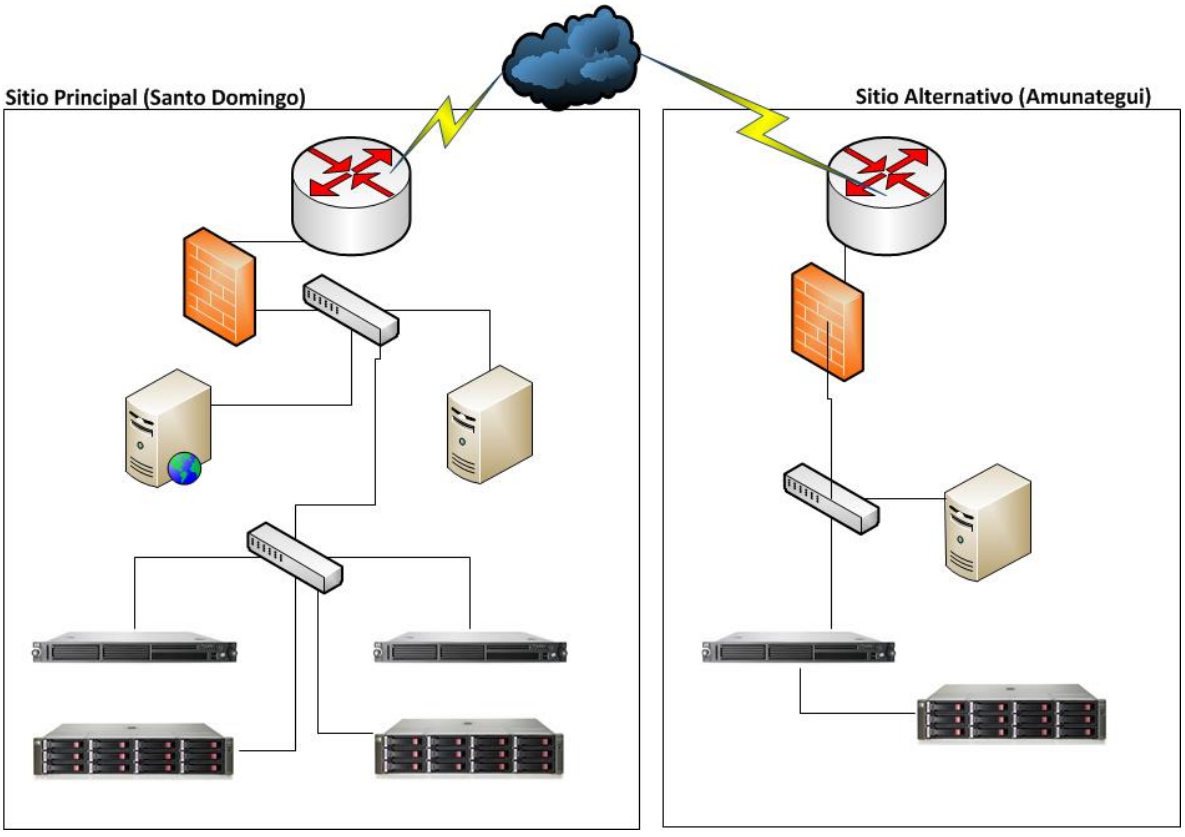


Figura 9. Diagrama de la solución

Para lograr el objetivo propuesto en este proyecto fue necesario realizar algunas actividades, las cuales serán detalladas a continuación.

**Habilitación del espacio físico**

En el espacio físico ubicado en el edificio de calle Amunategui, existía una bodega en la cual se almacenaban todos los equipos informáticos que posteriormente serán dados de baja. Para poder habilitar este espacio y dejarlo como sala de servidores, se debieron realizar los siguientes trabajos:

- Instalaciones eléctricas.
- Instalación de aire acondicionado.
- Conexión de red de alta velocidad.
- Habilitación de una chapa con clave de acceso a la sala.
- Instalación de detectores de humo.
- Extintores de incendio.

Gran parte de este trabajo fue realizado por el departamento de gestión administrativa y supervisado por el departamento de informática.

**Adquisición del equipamiento**

Después de realizar un análisis de las necesidades de equipamiento informático necesarias para la habilitación del nuevo sitio, se procedió a realizar la solicitud al comité técnico financiero de la I. Municipalidad de Santiago, la cual es la entidad encargada de aprobar todas las compras.

El equipamiento solicitado en la compra, corresponde a:

- Servidores de bases de datos y de aplicación.
- Rack para servidores.

- Unidad de aire acondicionado.
- Switch de comunicación.
- Unidades de respaldo (discos externos).
- UPS (baterías que proporcionan energía eléctrica).

**Habilitación de la infraestructura**

Esta etapa comprendió la conexión de los diferentes equipos informáticos que se adquirieron con la finalidad de habilitar el nuevo sitio, esto incluyo la instalación de los sistemas bases para el funcionamiento de los servidores. Este trabajo fue realizado en conjunto con personal de la unidad de redes computacionales, dependiente de la dirección de informática.

Las tareas realizadas por este equipo, fueron:

- Instalación de rack para los servidores.
- Conectar switch de comunicación.
- Configuración de red LAN.
- Conectar discos de almacenamiento.
- Configuración de software base de servidores.
- Instalación de antivirus.
- Configuración de funcionalidades de la plataforma.

**Habilitación de sistemas y Migración de datos**

El trabajo de habilitación de los sistemas y de migración de las bases de datos desde el sitio actual ubicado en el edificio de Santo Domingo al nuevo sitio en calle Amunategui, fue realizado por expertos en el área informática.

Las tareas realizadas en esta etapa fueron las siguientes:

- Instalación y configuración de sistemas de producción.

- Restauración y habilitación de base de datos.
- Configuración del software de réplica de datos.
- Certificación técnica y funcional.
- Pruebas de funcionamiento del sitio.

## *3.7. Organización y planificación*

### *3.7.1. Roles y responsabilidades*

Con el propósito de cumplir con los objetivos propuestos, los equipos de emergencias están formados por el personal clave y necesario en la activación del plan de contingencia. Cada equipo tiene sus funciones y procedimientos, las cuales tendrán que desarrollar en las distintas fases de la ejecución del plan.

**Equipo director o comité de crisis**

Este equipo está conformado por personas que tienen injerencia en los planes estratégicos de la municipalidad. Vale decir el director de informática y el director de administración y finanzas.

El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este comité debe tomar las decisiones claves durante los incidentes, además de hacer de enlace con la administración municipal, manteniéndolos informados de la situación regularmente.

Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación.
- Decisión de activar o no el plan de continuidad.
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.

- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

**Equipo de relaciones publicas**

Será el encargado de canalizar la información que se realizará al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son:

- Si el tipo de incidente lo requiere, emitir un comunicado oficial a los contribuyentes en el que indique que se restablecerán los servicios lo antes posible.
- Atender a los contribuyentes para proporcionarles información sobre incidentes y tranquilizarlos lo máximo posible.

Uno de los valores más importantes de la municipalidad son sus contribuyentes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación, que eviten la incertidumbre y el caos.

Integrantes del equipo de recuperación.

| Nombre | Posición | Teléfono |
|---|---|---|
| | Director departamento | xxxxxxxxx |
| | Encargada de sistemas | xxxxxxxxx |

**Equipo de las unidades de negocio**

Estos equipos estarán formados por las personas que trabajan con las aplicaciones que identificamos como críticas, y serán los encargados de realizar todas las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.

Integrantes de las unidades de negocio

| Nombre | Posición | Teléfono |
|---|---|---|
| | Técnico informático | xxxxxxxxx |
| | Técnico informático | xxxxxxxxx |

**Equipo de recuperación**

El equipo de recuperación será el encargado de poner en marcha el proceso de recuperación para restaurar los servicios en el sitio alternativo ubicado en Amunategui, lo más pronto posible. Para lo cual se deben realizar las siguientes actividades.

- Poner en marcha los sistemas por orden de criticidad.
- Una vez restaurados los sistemas, se debe comprobar su operatividad.
- Informar al comité de crisis en qué etapa esta la ejecución del plan.

Integrantes del equipo de recuperación

| Nombre | Posición | Teléfono |
|---|---|---|
| | Encargado de sistemas | xxxxxxxxx |
| | Técnico informático | xxxxxxxxx |
| | Técnico en redes | xxxxxxxxx |

## *3.8. Plan de Pruebas*

**Objetivos del plan de prueba**

El Plan de Continuidad no se considerará válido hasta que no se haya superado satisfactoriamente el Plan de Pruebas que asegure la viabilidad de las soluciones adoptadas.

El Plan de Pruebas diseñado tiene como objetivos:

- Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la municipalidad.
- Probar la efectividad y los tiempos de respuesta del Plan para comprobar que están alineados con la definición realizada en el diseño.
- Identificar las áreas de mejora en el diseño y ejecución del Plan.
- Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.
- Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operativa en situación de contingencia.
- Concienciación y formación para los empleados a través de la realización de pruebas.

**Test completo**

Los ejercicios de test, son ejercicios planificados que implican la restauración real de la capacidad de proceso del sitio de contingencia. En este caso los procesos de producción no serán interrumpidos, pero se planificará una validación en el centro alternativo. Este tipo de prueba requerirá la participación de toda la organización de continuidad del negocio, incluyendo usuarios, personal técnico y de operaciones.

**Ejercicios técnicos**

Este tipo de ejercicio va a requerir la ejecución de los procedimientos de notificación y operativos, el uso de equipos de hardware, software, redes y los métodos alternativos para asegurar un rendimiento adecuado. Ejemplos de elementos que serán verificados durante el ejercicio de simulación serán:

- Procedimientos de emergencia
- Líneas de comunicaciones
- Capacidad y rendimiento del hardware
- Accesibilidad al sitio alternativo
- Recuperación de ficheros y documentación almacenados en sitio alternativo.
- Recuperación de datos.
- Recuperación de sistemas.

Estos ejercicios deben ser realizados al menos una vez al año, o en su defecto cada vez que existan cambios importantes. Los resultados de los ejercicios serán reportados formalmente al comité de crisis o equipo director. Además se debe considerar la actualización del plan en el caso que esto sea necesario.

**Revisión del plan de continuidad**

Por la propia dinámica del negocio, se van incorporando nuevas soluciones a los sistemas de información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas.

La correcta planificación del mantenimiento del plan de continuidad evitará que este quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.

**Fase de alerta**

La fase de alerta define los procedimientos a seguir ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos.

**Notificación de desastre**

Cualquier empleado de la municipalidad que se dé cuenta del incidente que afecte a los servicios informáticos de la municipalidad, debe comunicarlo al encargado de seguridad, proporcionando el mayor detalle posible.

Dicho encargado debe evaluar la situación e informar al responsable del equipo director, que en este caso es el director del departamento de informática.

**Ejecución del plan**

El equipo director evaluará la situación, con toda la información disponible sobre el incidente y decidirán si se activa o no el plan de contingencia informático. En caso que sea afirmativo, se iniciará el procedimiento la ejecución del plan.

En caso de que no se active el plan de continuidad, porque la gravedad del incidente no lo requiere, si será necesario gestionar el incidente para que no aumente su gravedad.

**Notificación de ejecución del plan**

Para activar el plan se deberá llamar a los integrantes de los diferentes equipos que van a participar de dicho plan.

Una vez avisados los equipos y puesto en marcha el plan, deben acudir al sitio alternativo ubicado en el edificio en calle Amunategui.

**Puesta en marcha del sitio ubicado en calle Amunategui**

Una vez que el equipo de recuperación llegue a edificio ubicado en calle Amunategui, deben verificar que los sistemas estén funcionamiento correctamente.

Los primeros sistemas en ser revisados, corresponden a patentes comerciales y tesorería, los cuales deben estar en funcionamiento antes de 48 horas, esto está identificado en el análisis de impacto.

Una vez revisados los sistemas, se avisará a los equipos de unidades de negocio para que realicen las comprobaciones necesarias que certifiquen que los sistemas funcionan de manera correcta y los datos estén lo más actualizado posible y puedan continuar dando servicio.

Una vez que el sitio de contingencia está en marcha y solventada la contingencia, hay que plantearse las estrategias y acciones para recuperar la normalidad del sitio principal ubicado en calle Santo Domingo.

## 3.9. Capacitación al personal

Para el buen funcionamiento del plan de contingencia informático, se deben realizar capacitaciones de forma permanente al personal involucrado en el plan para así asegurar la continuidad de TI. Los procesos de capacitación pueden ser a través de seminarios, reuniones o documentos escritos. Estos deberán ejecutarse al menos dos veces al año, o cuando un cambio importante en el negocio así lo requiera.

En las capacitaciones a realizar, estas presentaciones deben incluir temas tales como:

- Componentes del plan de continuidad.
- Porque es importante el plan de continuidad.
- Líderes y coordinadores.
- Presentación del plan de ensayos.
- Como el plan será activado.

## 3.10. Ejecución de pruebas al sitio alternativo

Para poder realizar el correcto funcionamiento del sitio alternativo ubicado en calle Amunategui, fue necesario reunir al personal tanto de redes como de desarrollo de sistemas. Los resultados obtenidos en las pruebas del sitio se detallan a continuación.

**Replicación de datos:**

El objetivo fue probar que tanto la tecnología de replicación de datos, como las unidades y cintas de respaldo estuvieran configuradas y que su funcionamiento fuera el correcto.

Los tiempos obtenidos en la replicación de datos fueron satisfactorios y estaban dentro de lo esperado.

Además se revisó la unidad de cinta y las unidades de discos externos y se logró determinar que los respaldos eran coherentes.

**Pruebas del sistema:**

Esto permitió asegurar la apropiada navegación dentro de los sistemas informáticos, además permitió ingresar de datos, procesarlos y recuperarlos apropiadamente.

En este proceso se Incluyeron pruebas funcionales, de usabilidad, de performance, documentación, procedimientos y seguridad.

Se produjeron algunos inconvenientes de configuración de los sistemas durante las pruebas, pero fueron rápidamente subsanadas y todas las pruebas planeadas fueron correctamente ejecutadas.

**Pruebas de integridad de los datos:**

Lo que se pretendió comprobar es que todos los datos introducidos en la base de datos son precisos, válidos y coherentes.

El criterio de comprobación es que todos los métodos de acceso y proceso de la base de datos funcionan como fueron diseñados y sin corrupción de ellos.

Se consideró la utilización de un grupo pequeño de datos para incrementar la visibilidad de cualquier anormalidad. Los procesos fueron invocados manualmente y el resultado fue satisfactorio.

**Pruebas de configuración:**

El objetivo fue validar y verificar que el sistema funciona adecuadamente en las estaciones de trabajo. Incluyo la apertura y cierre de varias aplicaciones desde computadores personales utilizados para dicha prueba, algunas de las transacciones simularon actividades cotidianas de los usuarios y las aplicaciones que interactúan con la base.

Las pruebas de las aplicaciones realizadas fueron satisfactorias, además nos permitieron revisar las velocidades de las transacciones con los servidores tanto de aplicación, como de bases de datos.

La revisión solo consideró la realización de pruebas al sitio alternativo ubicado en el edificio de calle Amunategui. La planificación de las pruebas del plan completo que incluirá a todos los actores se resolverá en una reunión solicitada por el director del departamento de informática a los distintos involucrados.

Después de analizadas las pruebas a los diferentes aspectos del sitio y faltando algunos puntos por resolver que no son de relevancia para el buen funcionamiento de dicho sitio, es que los resultados obtenidos han sido óptimos y satisfactorios para la organización.

# *4. CONCLUSIONES*

Las ventajas del plan de contingencia informático que se implementó en la municipalidad, es que otorga la flexibilidad para reaccionar ante un incidente importante que interrumpa el normal funcionamiento de los servicios informáticos, y poder retornar lo antes posible a su normal funcionamiento.

Para la generación de este proyecto, se comenzó por realizar un análisis de los sistemas críticos de la municipalidad, para lo cual se realizaron reuniones de trabajos con los distintos involucrados en los procesos considerados críticos de la organización.

Durante el desarrollo de este proyecto de tesis ha quedado claro que se debe hacer todo lo posible para garantizar al máximo la continuidad operacional para la que se elaboró un plan de contingencia y ha de quedar en claro que esa garantía está estrechamente ligada al factor económico, cuanto más dinero se invierta más seguros se estará ante cualquier contingencia y/o interrupción. Pero no se debe olvidar, y aquí viene algo a tener muy en cuenta, que se haga lo que se haga siempre se deberá asumir ciertos riesgos, no existe la seguridad total.

Algo que tampoco se debe olvidar es que la protección de los sistemas de la información es un proceso vivo. Mientras exista la organización debe existir preocupación para hacer frente a los problemas que pongan en peligro su continuidad.

**Recomendaciones**

- Es fundamental para el logro de este proyecto el apoyo de la alta dirección.
- Asignar la responsabilidad de la mantención del plan de contingencia a un equipo o persona experta.
- Asegurar la existencia de los procedimientos documentados para el plan de mantención.
- Crear un programa anual o semestral de conciencia del plan de contingencia.
- Se debe capacitar adecuadamente a los nuevos empleados.
- Probar que los procedimientos de respaldo y replicación de toda la información funcionen.
- Involucrar a todos los miembros de la municipalidad, en las pruebas del plan de contingencia.

# *5. GLOSARIO*

**CMDB**

Base de Datos de la Gestión de la Configuración es una base de datos que contiene detalles relevantes de cada elemento de la configuración.

**OLAs**

Acuerdo de Nivel de Operación

**UCs**

Contrato de Soporte

**TI**

Tecnologías de Información

**SLA**

Acuerdo de nivel de servicios, es un contrato escrito entre el proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

**RFC**

Petición de cambios

**CIs**

Elemento de configuración

**CFIA:** Que son las siglas de Component Failure Impact Analysis (Análisis del Impacto de Fallo de Componentes).

**FTA:** Que son las siglas de Failure Tree Analysis (Análisis del Árbol de Fallos).

**CRAMM:** Que son las siglas de CCTA Risk Analysis and Management Method (Método de Gestión y Análisis de Riesgos de la CCTA).

**SOA:** Que son las siglas de Service Outage Analysis (Análisis de Interrupción del Servicio).

# *6. BIBLIOGRAFIA*

**Manuales / Libros**


- Libro de SQL server 2008
- Herramientas de recuperación y protección de datos.
- Documentación de respaldo de bases de datos
- Documentos de ITIL.


**Internet**


- www.itil-officialsite.com
- http://itil.osiatis.es/Curso_ITIL
- http://www.vensign.com/
- http://seguinfo.wordpress.com/2008/12/03/%C2%BFque-es-itil-2/
- http://en.wikipedia.org/wiki/Disaster_recovery
- http://definicion.de/plan-de-contingencia/
- http://seguridadinformacioncolombia.blogspot.com/2010/05/analisis-de-impacto-de-negocios.html
- http://www.compuchannel.net/2011/04/03/redundancia-contingencia-continuidad-resiliencia/