CAPÍTULO I

1.1 EL PROBLEMA

1.1.1 PLANTEAMIENTO DEL PROBLEMA

La información en la actualidad se encuentra sujeta a daños y a problemas imprevistos, los mismos que en su mayoría suelen suceder por no contar con un Plan de Continuidad de Negocios que permita mantener el servicio a la ciudadanía.

Entre los daños y problemas podemos mencionar algunos de éstos:

- Incidentes serios de seguridad en los sistemas como pérdidas de información, robo de información sensible o su distribución accidental.
- Errores de Operación de los Sistemas porque no se suele conocer o identificar los límites de los mismos, lo que impide de cierta forma prevenir y minimizar pérdidas a la organización.
- Daños en la infraestructura y servicios, fallo de suministro eléctrico y en comunicaciones, ya que el mal funcionamiento de estos servicios podría ocasionar de forma segura perjuicios e incluso deterioro de los dispositivos utilizados en la organización por ende se obtendrán gastos y pérdidas en la misma.
- Fallos en los equipos o en los sistemas incluyendo fallos en la fuente de alimentación y equipos de refrigeración, debido posiblemente al uso inadecuado de los elementos que hemos mencionado.
- Daños deliberados como robos, huelgas, etc.

Estos problemas afectan de forma diferente a cada organización dependiendo de su tamaño y área de actividad, no siendo el tamaño una característica fundamental; las pequeñas y medianas organizaciones también pueden verse seriamente afectadas.

Las consecuencias de estos incidentes sobre las organizaciones que no tienen un Plan de Continuidad de Negocios pueden llegar a ocasionar incluso el cierre de éstas.

1.1.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera se podrá brindar y garantizar la continuidad de negocios en el Gobierno Provincial de Los Ríos?

1.1.3 DELIMITACIÓN

OBJETO DE ESTUDIO: INGENIERÍA DE SISTEMAS

CAMPO DE ACCIÓN: AUDITORÍA INFORMÁTICA

Este estudio se realizará en el Gobierno Provincial de los Ríos durante el año 2011.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Desarrollar una Auditoría Informática que garantice la continuidad de negocios en el Gobierno Provincial de Los Ríos

1.2.2 OBJETIVOS ESPECÍFICOS

- Cimentarse en bases teóricas y científicas que permitan el desarrollo de ésta investigación.

- Estudiar y preparar información para estar al tanto de las múltiples y mejores soluciones.

- Validar y certificar la investigación y resultados contando con la asistencia y apoyo de un experto.

1.3 JUSTIFICACIÓN

A la prontitud con la que se maniobran los negocios actuales, un incidente de pocas horas de duración podría lograr un impacto o consecuencias desastrosas en la organización que lo padece.

La dependencia que existe entre el negocio y los sistemas de información requiere que se esté preparado para controlar y prevenir las múltiples amenazas que ponen en riesgo su operatividad y, en consecuencia, la continuidad del negocio.

El atentado del 11 de Septiembre del año 2001 podría ser un claro ejemplo de un impacto desastroso.

No obstante, en variadas ocasiones no es necesario un desastre de superficies o espacios parecidos a los del ejemplo mencionado para poner en peligro la buena marcha de la organización y su propia conservación y supervivencia; eventos como la intrusión o allanamiento de un virus, la instalación de un parche de seguridad pueden conllevar a la inoperatividad temporal de los sistemas, la pérdida de información crítica o, en última instancia, la inutilización de las infraestructuras.

Una Auditoría de Sistemas permite la identificación de fallas, riesgos y el planteamiento de medidas correctivas; se deben evaluar constantemente la calidad de servicios, las aplicaciones e infraestructuras tecnológicas, las mismas que se brindan a los usuarios finales, que a su vez cuenten con políticas/estándares que permitan la pronta gestión de errores y corrección de problemas, y con planes de continuidad que garanticen la prolongación de las operaciones en caso de desastres que puedan ocasionar la paralización total o parcial de los servicios tecnológicos e inclusive la pérdida de información como se menciona anteriormente.

Un proceso de Auditoría Informática tiene como objetivo la implantación de nuevos y mejores controles, que permitan entregar servicios tecnológicos con calidad y eficiencia, que a su vez servirá para que el Gobierno Provincial de Los Ríos alcance un mejor posicionamiento dentro de las instituciones públicas, apoyando de esta manera a los distintos procesos que está emprendiendo para alcanzar la visión que se ha planteado.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

La información es inherente a la existencia de las personas y de las sociedades. Permite conocer la realidad, interactuar con el medio físico, apoyar en la toma de decisiones, y evaluar la acción de individuos y grupos, el aprovechamiento de la información propicia la mejoría de los niveles de bienestar y permite aumentar la productividad y competitividad de las naciones**.**

El Gobierno Autónomo Descentralizado de la Provincia de Los Ríos es una institución pública que desde hace algunos años ha venido ejecutando varios proyectos relacionados con el área informática, con el objeto de apoyar a las diferentes actividades que desarrollan en la misma, algunos de estos proyectos ya han sido implementados por lo que se encuentran brindando servicios informáticos, con el respectivo soporte técnico y la capacitación para su correcta utilización. Estos servicios se encuentran centralizados en la unidad de gestión de las tecnologías en información y comunicaciones, que se encarga de la administración y gestión de las actividades TI, es decir, el análisis, desarrollo e implantación de los sistemas requeridos y se preocupa por el adecuado funcionamiento de las aplicaciones existentes, las redes y comunicaciones.

Teniendo conocimientos de que esta organización no ha sido objeto de estudio de una auditoría informática en ocasiones anteriores, consideramos de vital pertinencia e importancia el desarrollo de un estudio científico que permita realizar dicha auditoria para así garantizar la continuidad de negocios de la institución.

2.2 FUNDAMENTACIÓN TEÓRICA

2.2.1 AUDITORÍA INFORMÁTICA

2.2.1.1 AUDITORÍA

La palabra auditoría viene del latín auditorius, y de ésta proviene auditor, que tiene la virtud de oír, el auditor debe estar encaminado a evaluar la eficiencia y eficacia con que se está operando para que a través de indicación de recursos de acción, se tome decisiones con la finalidad de corregir y prevenir errores.

La auditoría implica la aplicación de ciertos procedimientos cuyos resultados son de carácter incuestionable. Así como existen normas y procedimientos para la realización de auditorías contables, también deben existir para la auditoría informática, las mismas que pueden estar basadas en experiencias de otras profesiones con características propias y detección de errores; además debe mejorar lo existente, corregir los errores y proponer soluciones.

Es un proceso formal y necesario para las empresas que tiene como fin asegurar que sus activos sean protegidos en forma adecuada.

También es un conjunto de tareas realizadas por un especialista para la evaluación o revisión de políticas y procedimientos relacionados con las diferentes áreas de una empresa:

- Administrativa.
- Financiera.
- Operativa.
- Informática.
- Crédito.
- Fiscales.

2.2.1.1.1 TAREAS PRINCIPALES DE LA AUDITORÍA.

- Estudiar y actualizar permanentemente las áreas susceptibles de revisión.
- Apegarse a las tareas que desempeñen las normas, políticas, procedimientos y técnicas de auditoría establecidas por organismos generalmente aceptados a nivel nacional e internacional.
- Evaluación y verificación de las áreas requeridas por la alta dirección o responsables directos del negocio.
- Elaboración del informe de auditoría (debilidades y recomendaciones).
- Otras recomendadas para el desempeño eficiente de la auditoria.[1]

2.2.1.2 AUDITORÍA EN INFORMÁTICA.

La auditoría en informática es un proceso realizado por especialistas que se desarrolla en función de procedimientos y técnicas orientados a la verificación y aseguramiento de que las normas en la organización se cumplan de manera eficiente y adecuada.
Este proceso metodológico tiene como principal objetivo la evaluación de recursos relacionados con la función informática lo que permitirá garantizar a la organización que dichos recursos se desempeñen satisfactoriamente. Ésta evaluación y verificación deberán ser la pauta para la entrega del informe que contendrá observaciones y recomendaciones para el mejoramiento informático de la organización.

2.2.1.2.1 IMPORTANCIA DE LA AUDITORÍA EN INFORMÁTICA

Entre los puntos clave que reflejan la importancia de la auditoría informática, destacamos los siguientes:

[1] Auditoría en Informática, Ms. Lorena Carmina Jiménez, 2003 Pág. 13

- La alta sistematización de las organizaciones
- Nuevas tecnologías
- Automatización de los controles
- Integración de la información
- Importancia de la información para la toma de decisiones

Proceso metodológico que tiene el propósito principal de evaluar todos los recursos (humanos, financieros, tecnológicos, etc.) relacionados con la función de informática para garantizar al negocio que dicho conjunto opera con criterio de integración y desempeño de niveles altamente satisfactorios para que apoyen la productividad y rentabilidad de la organización.

El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficiente, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos, la certeza de que la información que pasa por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.

La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalaciones, con el objeto de evaluar su efectividad y presentar recomendaciones a la gerencia.

2.2.1.2.2 FORMAS DE LLEVAR A CABO UNA AUDITORÍA EN INFORMÁTICA.

Los pasos de una auditoría son principalmente:

- Fijación del calendario y de los interlocutores, tanto de la empresa auditada como de la empresa que audita.
- Recogida de la documentación e información oportuna.
- Entrevistas con los usuarios.
- Análisis de la documentación y de la información previamente recogida.

- Entrega del Informe de Auditoría y del Reglamento de Medidas de seguridad.

2.2.1.2.3 SÍNTOMAS DE NECESIDAD DE UNA AUDITORÍA INFORMÁTICA.

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

2.2.1.2.3.1 Síntomas de descoordinación y desorganización:

- No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.
- Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante.

2.2.1.2.3.2 Síntomas de mala imagen e insatisfacción de los usuarios:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.- No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

2.2.1.2.3.3 Síntomas de debilidades económico-financieras:

- Incremento desmesurado de costes.- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).- Desviaciones Presupuestarias significativas.
- Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

2.2.1.2.3.4 Síntomas de Inseguridad: Evaluación de nivel de riesgos

- Seguridad Lógica
- Seguridad Física
- Confidencialidad

[Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales]

- Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia* Totales y Locales.
- Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

2.2.1.2.3.5 Planes de Contingencia:

Por ejemplo, la empresa sufre un corte total de energía o explota, ¿Cómo sigo operando en otro lugar? Lo que generalmente se pide es que se hagan Backups de la información diariamente y que aparte, sea doble, para tener un Backup en la empresa y otro fuera de ésta. Una empresa puede tener unas oficinas paralelas que posean servicios básicos (luz, teléfono, agua) distintos de los de la empresa principal, es decir, si a la empresa principal le proveía teléfono Telecom, a las oficinas

paralelas, Telefónicas. En este caso, si se produce la inoperancia de Sistemas en la empresa principal, se utilizaría el Backup para seguir operando en las oficinas paralelas. Los Backups se pueden acumular durante dos meses, o el tiempo que estipule la empresa, y después se van reciclando.

2.2.1.2.4 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA

2.2.1.2.4.1 Cuestionarios:

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la complementación de cuestionarios pre impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes, muy específicos para cada situación y muy cuidadosos en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos pre impresos hubieran proporcionado.

2.2.1.2.4.2 Entrevistas:

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante “entrevistas” en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, que es diferente para cada caso particular.

2.2.1.2.4.3 Checklist:

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y

hará preguntas “normales”, que en realidad servirán para la complementación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.
Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la Checklist de modo que el auditado responda claramente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que

exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes.

De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de “filosofía” de calificación o evaluación:

2.2.1.2.4.3.1 Checklist de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

2.2.1.2.4.3.1.1 Ejemplo de Checklist de rango:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tiene los siguientes significados:

1. Muy deficiente.
2. Deficiente.
3. Mejorable.
4. Aceptable.
5. Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La complementación de la Checklist no debe realizarse en presencia del auditado.

-¿Existe personal específico de vigilancia externa al edificio?

-No, solamente un guardia por la noche que atiende además otra instalación adyacente.

<Puntuación: 1>

-Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?

-Si, pero sube a las otras 4 plantas cuando se le necesita.

<Puntuación: 2>

-¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?

-Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.

<Puntuación: 2>

-El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?

-No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente mas que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.

<Puntuación: 4>

El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

2.2.1.2.4.3.2 Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

2.2.1.2.4.3.2.1 Ejemplo de Checklist Binaria:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

-¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

-¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

<Puntuación: 1>

-¿Se aplica dicha norma en todos los casos?

<Puntuación: 0>

-¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuacion: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

-¿Se conoce la norma anterior?

<Puntuación: 0>

-¿Se aplica en todos los casos?

<Puntuación: 0>

Las Checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las Checklists Binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

2.2.1.2.4.4 Trazas y/o Huellas:

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se acordará de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones desequilibran el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio de acuerdo a los tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante en la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de Sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio Sistema: Así, en los ficheros de <Accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, como en los <Log*> de dicho Sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.

Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.

La auditoría financiero-contable convencional emplea trazas con mucha frecuencia. Son programas encaminados a verificar lo correcto de los cálculos de nóminas, primas, etc.

2.2.1.2.4.5 *Log:

El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la Aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se inclina todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar cronológicamente que es lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos.

2.2.1.2.4.6 Software de Interrogación:

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente <paquetes de auditoría>, capaces de generar programas para auditores escasamente calificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la elaboración de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía “Cliente-Servidor”, han llevado a las firmas de software a desarrollar

interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía.

Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Texto, paquetes de Gráficos, Hojas de Cálculo, etc.[2]

2.2.1.3 OBJETIVOS DE UNA AUDITORÍA INFORMÁTICA

Los objetivos de la auditoría Informática son:

- El control de la función informática.
- El análisis de la eficiencia de los Sistemas Informáticos.
- La verificación del cumplimiento de la Normativa en este ámbito.
- La revisión de la eficaz gestión de los recursos informáticos.

[2] Auditoría en informática, Ms. Lorena Carmina Jiménez, Pág. 16-24

2.2.1.4 TIPOS DE AUDITORÍA INFORMÁTICA

2.2.1.4.1 AUDITORÍA INTERNA Y AUDITORÍA CONTABLE / FINANCIERA

La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada.

La auditoría interna abarca los tipos de:

- Auditoría Administrativa.
- Auditoría Operacional.
- Auditoría Financiera.

La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes, las cuales no son tan perceptibles como en las auditorías convencionales. La auditoría interna tiene la ventaja de que puede actuar periódicamente realizando Revisiones globales, como parte de su Plan Anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las Auditorías, especialmente cuando las consecuencias de las Recomendaciones habidas benefician su trabajo.

La auditoría interna proviene de la auditoría financiera y consiste en: una actividad de evaluación que se desarrolla en forma independiente dentro de una organización, a fin de revisar la contabilidad, las finanzas y otras operaciones como base de un servicio protector y constructivo para la administración. En un instrumento de control que funciona por medio de la medición y evaluación de la eficiencia de otras clases de control, tales como: procedimientos; contabilidad y demás registros; informes financieros; normas de ejecución etc.[3]

2.2.1.4.2 AUDITORÍA ADMINISTRATIVA.

Es el examen metódico y sistemático que permite evaluar en forma integral o parcial a una organización con el propósito de evaluar el nivel

[3]http://www.gerencie.com/auditoria-interna.html; Autor: Mauricio León Consultor en Administración de Operaciones http://www.mitecnologico.com/Main/ClasificacionObjetivosDeTiposDeAuditoria; Universidad Dr. Andrés Bello El Salvador C.A.

de rendimiento o desempeño de las diferentes áreas o niveles funcionales de ésta. Así como su interrelación con el medio ambiente.

La auditoría administrativa involucra una revisión de los objetivos, planes y programas de la empresa, su estructura orgánica y funciones, sus sistemas, procedimientos y controles, el personal y las instalaciones de la empresa y el medio en que se desarrolla, en función de la eficiencia de operación y el ahorro en los costos.

Este tipo de auditoría puede ser llevada a cabo por el profesional en administración de empresas y otros profesionales capacitados, incluyendo al contador auditor preparado en disciplinas administrativas o, respaldadas por otros especialistas.

El resultado de la auditoría administrativa es un informe sobre la eficiencia administrativa de toda la empresa o parte de ella.

Es la que se encarga de verificar, evaluar y promover el cumplimiento y apego al correcto funcionamiento de las fases o elementos del proceso administrativo y lo que incide en ellos es su objetivo, también el evaluar la calidad de la administración en su conjunto.[4]

2.2.1.4.3 AUDITORÍA CON INFORMÁTICA

Los Procedimientos de auditoría con informática varían de acuerdo con la filosofía y técnica de cada departamento de auditoría en particular. Sin embargo, existen ciertas técnicas y procedimientos que son compatibles en la mayoría de ambientes de informática. Estas técnicas caen en dos categorías: Métodos manuales y métodos asistidos por computadora.

[4]http://www.mitecnologico.com/iem/Main/AuditoriaAdministrativa; Autor: Prof. Lauro Soto, BC, México.

2.2.1.4.3.1 UTILIZACIÓN DE TÉCNICAS DE AUDITORÍAS ASISTIDAS POR COMPUTADORAS

El computador será utilizado por el auditor en el proceso de ejecución de la auditoría, lo que permitirá ampliar la cobertura del examen reduciendo el tiempo/costo de las pruebas y procedimiento de muestreo.

El auditor puede emplear la computadora para utilizar paquetes de auditorías, supervisar la elaboración de programas para el desarrollo de la auditoría interna, usar programas de auditoría que verifiquen la eficiencia del computador y su operación.

Todo programa empleado en la auditoría debe permanecer bajo control del departamento de auditoría. Los programas desarrollados con objeto de hacer auditoría deben estar cuidadosamente documentados para definir sus propósitos y objetivos que aseguren una ejecución continua.

Los auditores internos deberán asegurarse de:

- Mantener el control sobre programas catalogados y emprender protecciones apropiadas.
- Observar el procesamiento de la aplicación de auditoría.
- Desarrollar programas que monitoreen el procesamiento de auditoría.
- Mantener el control sobre las especificaciones de los programas, documentación y comandos de control.
- Controlar la integridad de los archivos que se están procesando y las salidas generadas.

2.2.1.4.3.2 TÉCNICAS AVANZADAS DE AUDITORÍA CON INFORMÁTICA

Cuando en una instalación se encuentren operando sistemas avanzados de computación como procesamiento en línea, bases de datos y procesamiento distribuido, se podría evaluar el sistema empleado mediante técnicas avanzadas de auditoría. Éstos métodos requieren un

experto por tanto el departamento debe contar con el entrenamiento adecuado.

- Pruebas Integrales:consiste en procesar datos de un departamento ficticio comparando los resultados con resultados predeterminados.
- Simulación**:**consiste en desarrollar programas de aplicación para probar y comparar resultados de la simulación con la aplicación real.
- Revisiones de acceso**:**En este punto se conserva un registro computarizado de todos los accesos a determinados archivos.
- Operaciones en paralelo**:**Es la verificación de la exactitud de la información sobre los resultados que produce un sistema nuevo que sustituye a uno ya auditado.
- Evaluación de un sistema con datos de prueba**:**Consiste en la prueba de resultados producidos en la aplicación con datos de prueba contra los resultados que fueran obtenidos inicialmente en las pruebas del programa.
- Registros extendidos**:**consiste en agregar un campo de control a un registro como un campo especial a un registro extra que pueda incluir datos de todos los programas del procesamiento de determinada transacción.
- Totales aleatorios en ciertos programas**:**se trata de conseguir totales en el sistema para ir verificando su exactitud en forma parcial.
- Resultados de ciertos cálculos para comparaciones posteriores**:**son los que permiten comparar los totales en diferentes fechas.

Todas estas técnicas le ayudan al auditor interno, sin embargo actualmente se desarrollan programas y sistemas de auditoría que eliminan los problemas de responsabilidad del departamento de auditoría.

El empleo de la microcomputadora facilita tareas como:

- Trasladar los datos del sistema a un ambiente de control del auditor.
- Llevar a cabo la selección de datos.
- Verificar la exactitud de los cálculos.
- Muestreo estadístico.
- Visualización de datos.
- Ordenamiento de la información.
- Producción de reportes e histogramas.

El auditor interno debe participar en el desarrollo de los sistemas con la finalidad de asegurar que se tengan todos los controles de acuerdo con las políticas internas, antes de que se comience la programación del sistema.

2.2.1.4.4 AUDITORÍA DE PROGRAMAS

Auditoría de programas, comprende la revisión del conjunto de funciones y actividades que integran un programa específico asignado a una o varias unidades. En este caso se revisará aquel programa, subprograma, proyecto, etc., que esté establecido en la estructura programática del presupuesto, excluyéndose los otros que pudieran estar bajo la responsabilidad de la misma unidad.

2.2.1.4.5 AUDITORÍA DE SEGURIDAD.

Las auditorías son actividades muy comunes en entornos empresariales, especialmente las realizadas por personal externo y permiten conocer el nivel de seguridad y las acciones a emprender para corregir los posibles fallos.

La auditoría de seguridad tiene un costo siempre menor que el valor que pueden tener los datos internos en la empresa. Ésta auditoría resulta cada vez más conveniente debido a la vulnerabilidad de los datos ya que

cada vez existen más personas que se dedican a cometer delitos informáticos.

El proceso de la auditoría de seguridad comienza con un análisis de las amenazas potenciales que enfrentan a una organización; examina sistemas, políticas y prácticas de la organización para identificar sus vulnerabilidades.

2.2.1.4.5.1 Consideraciones inmediatas para la auditoría de seguridad

2.2.1.4.5.1.1 Uso de la computadora

Se debe observar el uso adecuado de la computadora y su software

2.2.1.4.5.1.2 Cantidad y Tipo de Información

El tipo y cantidad de información debe considerarse como un factor de alto riesgo ya que puede estar en manos de algunas personas, además del problema que podría ocasionarse como dependencia de pérdida de datos.

2.2.1.4.5.1.3 Control de Programación

Se debe controlar que los problemas no contengan bombas lógicas, los programas deben contar con fuentes y sus últimas actualizaciones, documentación técnica, operativa y de emergencia.

2.2.1.4.5.1.4 Personal

En este punto se deberá tener en cuenta que se trata de las personas que están ligadas directamente al sistema de información, por ende se deben tomar en consideración varios aspectos, entre ellos conocer la capacitación del personal en situaciones de emergencia.

2.2.1.4.5.1.5 Medios de Control

Se debe contemplar la existencia de medios de control para conocer cuando se produce un cambio o fraude en el sistema.

2.2.1.4.5.1.6 Rasgos al personal

Se debe conocer el carácter del personal relacionado con el sistema para evitar malos manejos de administración, negligencia o ataques deliberados.

2.2.1.4.5.1.7 Instalaciones

Significan un alto grado de riesgo, por lo que se debe verificar la continuidad de flujo eléctrico y efectos del mismo sobre el software y hardware, así como evaluar las conexiones con los sistemas eléctrico, telefónico, cable, etc.

2.2.1.4.5.1.8 Control de Residuos

Observar cómo se maneja la basura de los departamentos de mayor importancia, donde se almacena y quien lo maneja.

2.2.1.4.5.1.9 Establecer áreas y prado del riesgo

Es de vital importancia crear conciencia en los usuarios de la organización sobre el riesgo que corre la información y hacerles comprender que la seguridad es parte de su trabajo.

2.2.1.4.5.2 Consideraciones para elaborar un sistema de seguridad integral

Diseñar un sistema de seguridad significa planear, organizar, dirigir y controlar actividades destinadas a mantener y garantizar la integridad física de los recursos en la función informática. Un sistema integral debe contemplar entre otras actividades las siguientes:

- Definir políticas de seguridad.
- Organizar y dividir las responsabilidades.
- Definir prácticas de seguridad para el personal.
- Definir necesidades de sistemas de seguridad.
- Planificación de programas de desastre y sus pruebas.
- Planificación de equipos de contingencia con carácter periódico.

2.2.1.4.5.3 Etapas para implementar un sistema de seguridad

- Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
- Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos y ambientales.
- Elaborar un plan para un programa de seguridad.

2.2.1.4.5.4 Etapas para implantar un sistema integral en marcha

- Introducir el tema de seguridad en la visión de la empresa
- Definir los procesos de flujo de información y sus riesgos.
- Capacitar a los gerentes y directivos contemplando el enfoque global.
- Designar y capacitar supervisores de área.
- Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
- Mejorar las comunicaciones internas.
- Identificar claramente las áreas de mayor riesgo corporativo y plantear soluciones de alto nivel.
- Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

2.2.1.4.5.5 Beneficios de un sistema de seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales.[5]

2.2.1.5 PLANIFICACIÓN DE LA AUDITORÍA INFORMÁTICA.

Como todo proyecto implantado dentro de una organización, el proyecto de auditoría informática debe iniciar con una fase de planeación en la cual participen todas las áreas de la organización para identificar los recursos necesarios que permitirán llevar a cabo este proyecto, como son, objetivos que se pretenden alcanzar con el proyecto, análisis costo/beneficio, personal humano que intervendrá en el proyecto. Esto cumplirá varios objetivos fundamentales que son:

- Evaluación de los sistemas yprocedimientos.
- Evaluación de los equipos de cómputo
- Evaluación del proceso de datos,

Lo cual se resume en obtener un conocimiento inicial de la organización a evaluar, con especial énfasis en sus procesos informáticos basados en evaluaciones administrativas realizadas a los procesos electrónicos, sistemas y procedimientos, equipos de cómputo, seguridad y confidencialidad de la información, y aspectos legales de los sistemas y la información.

Una vez que se ha obtenido un conocimiento inicial de la organización se procede a establecer metas, programas de trabajo de auditoría, personal que intervendrá en el proyecto, presupuesto financiero, las

[5] Ms. Lorena Carmina Jiménez, Auditoria Informática, Pág. 38-51

fechas y la manera como se presentarán los informes de las actividades de cumplimiento del proyecto, basados en la realidad de la organización evaluada.[6]

2.2.1.6 EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA

La ejecución de la auditoría Informática radica de manera primordial en la recolección de información y evidencias suficientes, para posteriormente poder establecer los comentarios, conclusiones y recomendaciones con respecto a la Administración de Tecnologías de la Información, lo cual se realiza utilizando diversas técnicas como las siguientes:

- Entrevistas
- Simulación
- Cuestionarios
- Análisis de la información documental entregada por el auditado
- Revisión y Análisis de Estándares
- Revisión y Análisis de la información de auditorías anteriores

El análisis de la información obtenida mediante las técnicas anteriormente mencionadas deberá ser realizado utilizando el criterio profesional adquirido por la experiencia del equipo comisionado del Proyecto de Auditoría, identificando cuando las evidencias que se han logrado obtener son suficientes para acreditar el adecuado conocimiento de la organización.

La información recolectada debe ser completa y detallada para que pueda ser comprendida por el equipo de auditoría y así poder admitir la obtención de comentarios, conclusiones y recomendaciones, mediante su revisión.

La evidencia se clasifica de la siguiente manera:

a. Evidencia documental.

b. Evidencia física.

c. Evidencia analítica.

d. Evidencia testimonial.

[6] http://es.scribd.com/doc/53381984/10/Planificacion-de-la-auditoria-Informatica; Ing. Sandra Patricia Balseca Alcocer e Ing. Miguel Eduardo Cachimuel Querembás

Una vez que se ha obtenido una información confiable mediante la cual se logre evaluar a la organización, se debe proceder a examinar la manera en la que se han diseñado los controles en la empresa, razón por la cual el equipo de auditoría confirmará la información procesada por medios electrónicos y manipulará métodos especializados de informática.

Corresponde también considerar que antes de aportar una opinión favorable acerca de los sistemas y acordar su confiabilidad en el procesamiento de la información, es de vital importancia efectuar de forma necesaria una revisión de los controles generales del computador, debido a que en la confiabilidad de ellos se fundamenta el buen funcionamiento de los sistemas de aplicación.

2.2.1.7 FINALIZACIÓN DE LA AUDITORÍA INFORMÁTICA.

La deducción o resultado que arroja la auditoría Informática, deberá ser plasmada en un informe de conclusiones el mismo que se redactará, presentará y proporcionará a la administración de la organización para su evaluación, razón por la cual previo a la emisión del informe final se expedirán algunos apuntes, notas o borradores, que se examinarán, actividad que realizará en conjunto entre los auditores y la administración de la organización, para descubrir las posibles fallas en la evaluación de auditoría debido a la incorrecta comprensión de la organización por parte de los auditores.

2.2.1.8 PLAN DE AUDITORÍA INFORMÁTICA.

Es el esquema metodológico más importante del auditor informático, en él se describe todo sobre esta función y el trabajo que realiza.

Las partes que lo componen deben ser al menos las siguientes:

- Funciones.
- Procedimientos.
- Tipos de auditorías que realiza.
- Sistema de evaluación.
- Nivel de exposición.
- Lista de distribución de informes.
- Seguimiento de acciones correctoras.
- Plan de trabajo.

2.2.1.9 ASPECTOS GENERALES SOBRE LA ENTIDAD AUDITADA.

Para realizar la ejecución de un plan de auditoría informática en una entidad pública es necesario conocer ciertos datos generales sobre ella, tales como:

a) Una entrevista con el director de la Unidad de Tecnología y comunicación

Esta debe ser realizada de manera clara precisa y sencilla, por la persona encargada de ejecutar el manual de auditoría informática.

Posteriormente dependiendo de los resultados obtenidos en la entrevista, se debe proceder a entregar una solicitud formal de parte del auditor para que el director la firme y se extienda un documento formal que respalde la autorización, caso contrario no se puede ejecutar el plan de auditoría.

b) Luego de haber concluido satisfactoriamente los puntos antes mencionados, la persona encargada de la auditoría asignado(a) para realizar la ejecución de plan de auditoría informática; debe proceder a lo siguiente:

- Investigación sobre la historia y naturaleza de la entidad auditada. Lo que permitirá conocer de forma general el origen y naturaleza de la institución a ser auditada.
- Solicitar la estructura organizativa tanto de la entidad en general como de la Unidad De Tecnología De Información Y Comunicaciones.
- Se pretende conocer la forma de cómo están distribuidas las diferentes áreas de la entidad, así como también los niveles jerárquicos de cada área.

- Investigar la historia y naturaleza de La Unidad De Tecnología De Información Y Comunicaciones.
  Esta información a recopilar es parte fundamental en el desarrollo del proyecto de investigación, que permite verificar y conocer mejor el área de sistemas.
- Solicitud del inventario de equipo de cómputo y recurso tecnológico del Departamento de Sistemas.

Son datos fundamentales para conocer la situación actual de los equipos de cómputo y recursos tecnológicos; con que cuenta el Departamento de Sistemas.

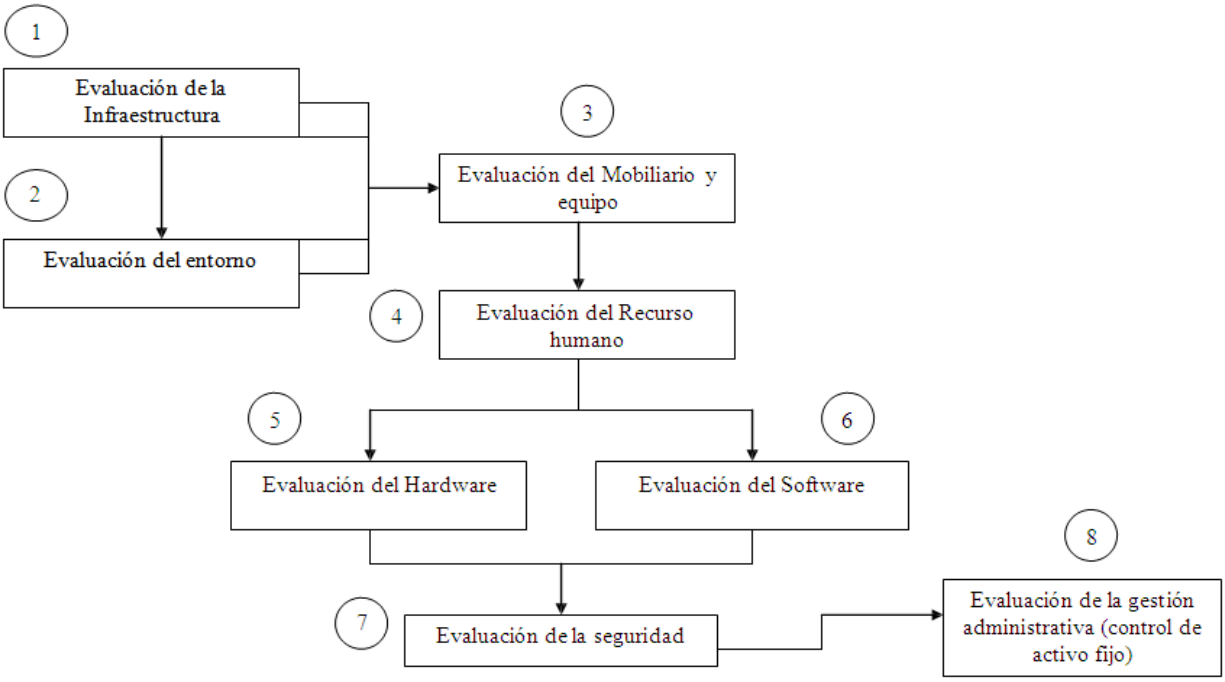
c) Ejecutar el plan de auditoría informática en el Departamento de Sistemas.

Teniendo en cuenta evaluar los siguientes aspectos:

- Infraestructura.
- Evaluacióndel Entorno.
- Mobiliario y equipo.
- Recurso humano.
- Hardware y Software.
- Seguridad.
- Gestión administrativa (control de activos fijo).

Todos estos aspectos básicos deberán ser estudiados por separado, según la estructura contemplada dentro del plan de auditoría informática.

2.2.1.10 ESTRUCTURA DEL MANUAL DE AUDITORÍA INFORMÁTICA.



2.2.1.10 Esquema 1.

2.2.1.10.1 EVALUACIÓN DE LA INFRAESTRUCTURA.

INFRAESTRUCTURA, es el conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una organización cualquiera, tanto de sus áreas como toda ella. Y esta puede ser de tipo: física, aérea, social, económica, otros.

Como primer paso se considera la evaluación de la infraestructura por ser la base donde se establece el funcionamiento principal de una empresa o departamento. Dentro de este aspecto corresponde evaluar todo lo relacionado con la infraestructura es decir: lo tangible como paredes, piso, techo e instalaciones eléctricas, su correspondiente mantenimiento y remodelaciones de la misma.

Así como también la forma como se controlan los problemas que se tengan con este aspecto, para su correspondiente solución y mejoramientos.

2.2.1.10.2 EVALUACIÓN DEL ENTORNO

ENTORNO es el ambiente, todo lo que nos rodea. Conjunto de condiciones extrínsecas que se necesitan para funcionar de la mejor manera dentro de una organizacióno departamentodeesta.

Es decir, todas aquellas situaciones que intervienen directa o indirectamente en el desarrollo de las actividades, aunque estas no se puedan ver o tocar, pero si se pueden medir (calor, ruido, otros) o sentir (la ergonomía o comodidad, espacio físico adecuado y mas).

Es otro de los aspectos a evaluar que interviene directamente en el área informática, pues es de gran importancia para el buen funcionamiento de estos.

Para la evaluación del entorno se toma en consideración aspectos como: la ubicación, espacio físico, condiciones ambiéntales, distribución del equipo de cómputo, la ergonomía si es el idóneo de acuerdo a las necesidades, problemas detectados, así como las posibles soluciones, y como afectan las distracciones a los usuarios, si el lugar es cómodo para las funciones que desempañan el personal administrativo y usuario.

2.2.1.10.3 EVALUACIÓN DEL MOBILIARIO Y EQUIPO.

MOBILIARIO Y EQUIPO es el conjunto de muebles de una casa u oficina o un área determinada, y el Grupo o Conjunto de aparatos y dispositivos que constituyen el material básico de esta.

Para el caso del mobiliario se estaría hablando de muebles como sillas, escritorios, mesas o muebles para computadoras y otros.

Y de los equipos tales como ventiladores, aires acondicionados, las mismas computadoras y todo los otros recursos tecnológicos como retro-proyectores, televisores, VHS y otros.

En cuanto a mobiliario y equipo, se evaluará los siguientes puntos: distribución del equipo, es adecuado el equipo de cómputo para el desarrollo de las práctica, es suficiente la cantidad de equipo de

cómputo, se están dejando de realizar actividades por falta de equipo de cómputo y recursos tecnológicos; o existen equipos de cómputo adicionales que sean reemplazados al ocurrir un daño, la existencia de lugares específicos para guardar papelería, herramientas, mantenimiento y seguridad para proteger el mobiliario, que se hace con el mobiliario dañado, sobre quien recae la responsabilidad del mobiliario y/o equipo y la frecuencia con que se renueva.

2.2.1.10.4 EVALUACIÓN DEL RECURSO HUMANO.

RECURSO, es el conjunto de elementos disponibles para resolver una necesidad o llevar a cabo una acción, procedimiento o trabajo. Estos pueden ser: Recursos naturales, hidráulicos, forestales, económicos, humanos, otros.

La importancia de la evaluación de los recursos dentro de una organización se debe a que son parte muy esencial para toda acción o trabajo a realizar dentro de esta.

Para la evaluación del recurso humano los aspectos a evaluar son los siguientes:

El proceso que se lleva a cabo para seleccionar el personal administrativo del área informática, las capacitaciones tanto a administradores como docentes, sugerencias del administrador, encargados e instructores para mejoramientos del área de cómputo, como se lleva a cabo la supervisión del recurso humano, si son presentadas las sugerencias al director de la institución para su mejora, si existe un sustituto para la realización de las funciones en caso de ausencia del personal, la realización de funciones adicionales del personal que labora en el área de informática es realizada en horas laborales o no laborales y las políticas para sancionar la indisciplina.

2.2.1.10.5 EVALUACIÓN DEL HARDWARE.

HARDWARE**.** Conjunto de los componentes que integran la parte material de una computadora, es decir, todo aquello que se puede tocar físicamente como por ejemplo: el monitor, el CPU, el teclado y más.

Son todos los dispositivos y componentes físicos que realizan las tareas de entrada y salida, también se conoce al hardware como la parte dura o física del computador.

- LA SEGURIDAD FÍSICA DEL HARDWARE.

La seguridad física del hardware es un punto a estudiar por un auditor de informática. Aquí la seguridad física se torna más ardua, puesto que los sistemas informáticos suelen estar cercanos al usuario final o al mismo administrador, por lo que están expuestos aun mayor peligro de mal uso o uso mal intencionado.

También dentro de esta categorías e incluyen los recursos tecnológicos como, Televisores, retroproyectores, cámaras, VHS y otros.

En cuanto a la evaluación del hardware los aspectos son: el comprobante de la adquisición, cantidad y estado del equipo de cómputo y recurso tecnológico, así como la actualización. Además la proporción de los servicios de mantenimiento el tipo que se le proporciona y con qué frecuencia. También si el hardware es adecuado a las necesidades de los usuarios, los problemas que se dan con mayor frecuencia, y el tiempo con que son resueltos.

2.2.1.10.6 EVALUACIÓN DEL SOFTWARE.

SOFTWARE: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas enunacomputadora.

La seguridad el software es un punto muy importante a estudiar por un auditor de informática, por ser uno de los recursos importantes y frágiles si no se cuenta con el control adecuado y necesario que lo proteja tales como: Seguridad por contraseña de acceso, protección por antivirus, eliminación o modificaciones no autorizadas entre otros.

Con este aspecto se evaluará: el licenciamiento y facturación del software, su actualización, servicios de mantenimiento, tiempo en el cual se da, los problemas relacionados con el congestionamiento de la información, así como la instalación innecesaria de programas, además si carecen de programas para la realización de alguna práctica, se toman en cuenta los problemas y el tiempo para ofrecerles la solución**.**

2.2.1.10.7 EVALUACIÓN DE LA SEGURIDAD

SEGURIDAD: Dicho de un mecanismo que asegura el buen funcionamiento, precaviendo que este falle, se frustre o se violente.

La seguridad informática generalmente consiste en asegurar que los recursos con los que se cuenta (Hardware; Todo lo material. Software todo los programas) en una empresa u organización sean utilizados de la manera posible y sin que estos sufran daños o perjuicios por el mal uso o intencionalmente por cualquier usuario.

Es decir, que la seguridad es uno de los aspectos de mayor importancia pues de aquí depende en gran parte la efectividad de los recursos (hardware, software, mobiliario y equipo, recurso humano, otros) y los aspectos como (infraestructura, gestión administrativa, otros) que rodean un área informática.

Para evaluar la seguridad se toman los siguientes aspectos: en primer lugar la vigilancia para salvaguardar los recursos tecnológicos como las instalaciones, así como los controles preventivos y de riesgo supervisando actividades, claves de acceso, alarmas, salidas de emergencias y seguros.

Pero la seguridad va más allá de los aspectos físicos, es decir, en informática también existe la seguridad a través de software que son programas diseñados específicamente para mantener un control de monitoreo de riesgo posibles en cuanto al mal uso de los recursos, sabotaje, etc. Para lo cual se recomienda algún software, estos pueden ser obtenidos a través de la red de Comercialización normal o de forma gratuita en Internet.

2.2.1.10.8 EVALUACIÓN DE LA GESTIÓN ADMINISTRATIVA (CONTROL DE ACTIVO FIJO).

GESTIÓNA DMINISTRATIVA: Acción y efecto de dirigir, ordenar, disponer, organizar, ejercer un cargo, oficio dentro de una organización o empresa.

En cuanto a la evaluación de la gestión administrativa, esta va enfocada específicamente a áreas informáticas, por ser éstas de gran importancia en la actualidad. Para las instituciones educativas, además de verificar que estos cuenten con manuales de procedimiento, su elaboración, revisión y aplicación.

Así como el control de activo fijo tales como: equipo de cómputo, recursos tecnológicos y como se lleva el control sobre estos, es decir, el préstamo, uso del equipo de cómputo, seguridad, inventario y mantenimiento.

También las limitantes y responsabilidades con las que cuenta el administrador, encargado e instructor para realizarlas actividades adecuadamente.[7]

2.2.2 LA TECNOLOGÍA DE INFORMACIÓN (TI)

La tecnología de información (IT), según lo definido por la asociación de la tecnología de información de América (ITAA) es “el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras.” Se ocupa del uso de las computadoras y su software para convertir, almacenar, proteger, procesar, transmitir y recuperar la información.

La tecnología de la información puede ser bastante amplia, cubriendo muchos campos. Cuando las tecnologías de computación y comunicación se combinan, el resultado es la tecnología de la información o “infotech”.

[7] http://www.univo.edu.sv:8081/tesis/018134/018134_Cap5.pdf

La Tecnología de la Información (IT) es un término general que describe cualquier tecnología que ayuda a producir, manipular, almacenar, comunicar, y/o esparcir información.

2.2.2.1 LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

Las tecnologías de la información y la comunicación (TIC) son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las organizaciones y personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

Las Tecnologías de la información y la comunicación, son un solo concepto en dos vertientes diferentes como principal premisa de estudio en las ciencias sociales donde tales tecnologías afectan la forma de vivir de las sociedades.

2.2.2.2 ¿QUÉ ES LA INFORMACIÓN?

La información puede ser definida como los datos que han sido recogidos, procesados, almacenados y recuperados con el propósito de tomar decisiones financieras y económicas o para el soporte de una producción y distribución eficientes de bienes y servicios.

2.2.2.2.1 INFORMACIÓN ESTRATÉGICA.

Este tipo de Información permite a la alta gerencia definir los objetivos de la organización, la cantidad y clase de recursos necesarias para alcanzar los objetivos y las políticas que gobiernan su uso. La alta gerencia tiene que tomar decisiones económicas importantes basadas en las condiciones de los cambiantes mercados e innovación tecnológica. Parte de esta información es externa.

2.2.2.2.2 INFORMACIÓN PARA EL CONTROL DE GESTIÓN.

Este tipo de información ayuda especialmente para tomar decisiones en el período actual, normalmente un año, para que sean consistentes con los objetivos estratégicos organizativos. Incluye comparaciones entre los resultados actuales y objetivos, presupuestos y medidas de rendimiento.

2.2.2.2.3 INFORMACIÓN TÉCNICA U OPERACIONAL.

Se produce por rutina, día a día e incluye datos de contabilidad, control de inventario, programación de la producción, planificación de necesidades de materiales, normas y gestión del personal, control del flujo de caja, logística, ingeniería, fabricación, recepción, distribución, ventas y todo el conjunto de operaciones que son necesarias para mantener la empresa en funcionamiento.

2.2.2.2.4 INFORMACIÓN CONTABLE Y FINANCIERA.

Es la información que se genera con el propósito de control e información financieros. Este tipo de información se recoge de acuerdo con Principios Contables Generalmente Aceptados y son aplicados por los profesionales contables.

2.2.2.3 ¿POR QUÉ ES VALIOSA LA INFORMACIÓN PARA LA TOMA DE DECISIONES?

La calidad de las decisiones tomadas depende directamente de la calidad de la información que las soporta. La toma de decisiones requiere:

1. Un profundo conocimiento de las circunstancias que rodean un problema.
2. Conocimiento de las alternativas disponibles y
3. Estrategias competitivas.

2.2.2.3.1 ATRIBUTOS DE LA INFORMACIÓN QUE LA HACEN VALIOSA PARA LA TOMA DE DECISIONES.

- Completa: Si la información se pierde u oculta al que toma la decisión, el resultado de la decisión será pobre.
- Exacta**:** Errores en la entrada, conversión o procesos puede dar como resultado conclusiones inválidas que darán lugar a decisiones erróneas.
- Autorizada: La información puede ser semánticamente correcta, pero representar transacciones inválidas o no autorizadas.
- Auditable**:** La información debe ser verificada a través del documento fuente o su ejecución seguida mediante sistemas de control monitorizado y pre verificados.
- Económica: El coste de producir la información debería no exceder su valor cuando se utiliza.
- Adecuada: Información específica que debe estar disponible solamente para aquellos que la necesitan para asegurar una gestión eficiente. Demasiada información irrelevante a disposición de quién debe tomar la decisión puede ocultar el proceso.
- Oportuna o Puntual: La información pierde su valor cuando a quién tiene que tomar la decisión, se le entrega después de que la necesita.
- Segura: La información debe ser protegida de su difusión a personas no autorizadas, sin ello puede dar lugar a pérdidas económicas en la organización. Debe estar protegida contra destrucciones accidentales o voluntarias.

2.2.2.4 ¿QUÉ HACE QUE LA INFORMACIÓN SEA UN RECURSO CRÍTICO PARA LA ORGANIZACIÓN?

- Los estudios realizados en diversas organizaciones y universidades revelan que en los sectores financieros, productivos y de servicios, una caída total de las redes y equipos informáticos de tres o cuatro días puede dar lugar a la pérdida del negocio.

- La pérdida de confidencialidad en las bases de datos puede proporcionar a los competidores una ventaja definitiva.

2.2.2.5 ¿CÓMO MEJORAR LA GESTIÓN Y EL CONTROL DE LAS T.I.?

Para ello es necesario que las organizaciones puedan disponer de:

- Una función de auditoría informática independiente.
- Una utilización correcta de la informática en la práctica de los distintos tipos de auditoría.
- La definición de unos objetivos de control de T.I.[8]

2.2.3 GOBIERNOS PROVINCIALES DEL ECUADOR

2.2.3.1 GOBIERNOS PROVINCIALES Y TECNOLOGÍAS.

En la ciudad de Guayaquil, durante los días 17, 18 y 19 de octubre de 1969, los Prefectos del país, constituyeron con carácter permanente al Consorcio de Consejos Provinciales del Ecuador, CONCOPE, como la entidad de derecho público, responsable de: velar por la solidaridad de todos los consejos provinciales; de defender la autonomía institucional; y, para cumplir los cometidos, hoy previstos en su Reglamento General, publicado en el R.O. N° 546 del 12 de octubre de 1994.

El Acta y Estatuto inicial del Consorcio fueron aprobados por el Ministerio de Gobierno y Municipalidades, mediante Acuerdo Ministerial N° 067 del 2 de marzo de 1970, conforme lo determina el Art. 118 (hoy 121) de la Ley Orgánica de Régimen Provincial.

Son miembros del Consorcio todos los Gobiernos Provinciales del Ecuador. La representación de éstos en el seno y organismos del CONCOPE, la ejercen los señores Prefectos Provinciales o quienes hagan las veces de ellos.

El Gobierno Electrónico Provincial genera altos beneficios como medio de creación de valor y conocimiento en información para las

[8] http://jrvargas.files.wordpress.com/2009/03/conceptos-basicos-de-auditoria-informatica.pdf; .Ms. Julio Rito Vargas Avilés

autoridades y funcionarios que tienen que tomar decisiones y apoyar su gestión institucional así como también a modo demecanismo de transformación gradual de la forma y contenido de las relaciones de los ciudadanos con el Gobierno Provincial.

2.2.3.1.1 SISTEMAS INFORMÁTICOS:

- Gestión Institucional**:** Plan/ Presupuesto, Financiero, Control de Proyectos, Gestión Documental, Control y Monitoreo de Vehículos.
- Gestión Territorial**:** Sistema de Información Geográfica bajo WEB, Sistema para Catálogo de Datos (Meta datos), Gestión Actores, Cooperación Internacional, Portal de Acceso para Pequeños Productores.

2.2.3.1.2 ÁREAS DE TRABAJO

- Implementación y adaptabilidad en los GP‘S: El análisis de los procesos y sus mejoras de acuerdo a la normativa constituye la razón de dichas automatizaciones.
- Mejoramiento continuo en base a estándares de calidad: El mejoramiento y adaptabilidad en función de los cambios en la normativa, requerimientos de los Gobiernos Provinciales así como los estándares de calidad (ISO), forma parte de éste proceso.
- Asistencia Técnica y capacitación a equipos provinciales para apoyar su correcto funcionamiento y sostenibilidad: La capacidad operativa para gestionar los sistemas y procesos son transferidos desde el inicio a los responsables de los Gobiernos Provinciales; a futuro se pretende contar con un sistema de soporte concurrente entre los Gobiernos Provinciales.
- Gestionar y fortalecer la red de conectividad.

La red se encuentra en operación, lo que significa que cualquier Gobierno Provincial autónomamente puede organizar eventos.

- Apoyar proyectos de tecnología de los GP'S: El diseño, ejecución y evaluación de proyectos de tecnología forma parte de éste proceso.
- Apoyar la identificación de fuentes de cooperación en tecnología: La identificación y gestión de financiamiento para la implementación de proyectos de tecnología es una actividad permanente.
- Intercambio de experiencias tecnológicas: Las buenas prácticas tecnológicas siempre son impulsadas a través de eventos, difusión y coordinación entre Gobiernos Provinciales.
- Establecimiento de Centro y Sistemas de Información en los GP's: Los centros y sistemas de información territorial son una de las principales actividades.

El Gobierno Electrónico, integrasistémicamente la información institucional con la territorial a través de herramientas informáticas que gestionan modularmente los procesos administrativos y territoriales.[9]

2.2.3.2 GOBIERNO PROVINCIAL DE LOS RÍOS

2.2.3.2.1 SITUACION ACTUAL DE LA UNIDAD DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES.

La Situación actual de La Unidad De Tecnología De Información Y Comunicaciones se encuentra integrada por un conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc.), software (sistemas operativos de Windows 7, bases de datos, herramientas de administración, etc.) y servicios (soporte técnico, seguros, comunicaciones, etc.) que en conjunto dan soporte a los sistemas informáticos del Gobierno Provincial de Los Ríos.

[9] http://www.concope.gob.ec/sites/default/files/OFERTATECNICA.pdf; Ing. Montgomery Sánchez Reyes

2.2.3.2.2 PLAN ESTRATEGICO DE LA UNIDAD DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES.

Esta unidad está destinada a mantener el funcionamiento óptimo de la infraestructura tecnológica institucional, haciendo eficientes las tareas de procesamiento de datos y de información.

RESPONSABLE**:** Coordinador Técnico.

ATRIBUCIONES Y RESPONSABILIDADES**:**

1. Administrar las operaciones del área de cómputo, redes locales y departamentales de la institución;

2. Desarrollar e Implementar Planes de Sistemas de Información y Tecnologías Informáticas, considerando capacitación y formación de usuarios;

3. Desarrollar manuales de procedimientos, metodologías y estándares informáticos para buenas prácticas de servicios;

4. Proveer de servicios informáticos a las unidades del Gobierno Provincial;

5. Desarrollar y mantener Software de base a medida y utilitarios para hacer eficiente el trabajo de las diferentes unidades de la institución y redes locales;

6. Coordinar con la dirección de planificación en la elaboración de planes y proyectos de tecnología de información y comunicaciones TICs;

7. Realizar estudios Periódicos para provisión de equipos, programas y servicios computacionales, según las necesidades de todas las unidades departamentales;

8. Instalar, operar, controlar y mantener el hardware, software y redes de cómputo;

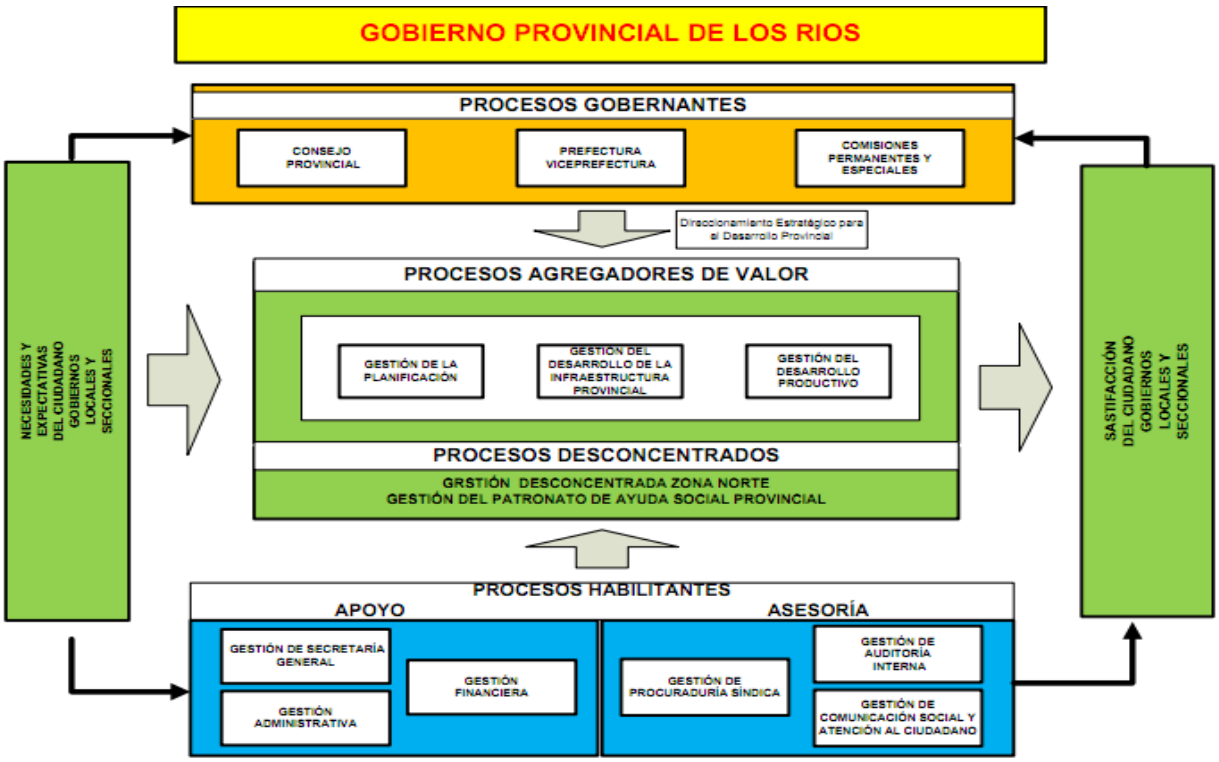
9. Mantener el inventario físico actualizado de las configuraciones computacionales y de comunicación;

10. Analizar el rendimiento óptimo de recursos consumibles de información (tintas, tóneres, cintas, etc.)

11. Apoyar a la mejora continua de procesos para fortalecer la institución.

La unidad para cumplir su misión contará con las áreas de: Planificación y seguridad informática, base de datos y aplicaciones, soporte técnico ymantenimiento, redes y comunicación de datos, áreas que tendrán un Supervisor Técnico.[10]

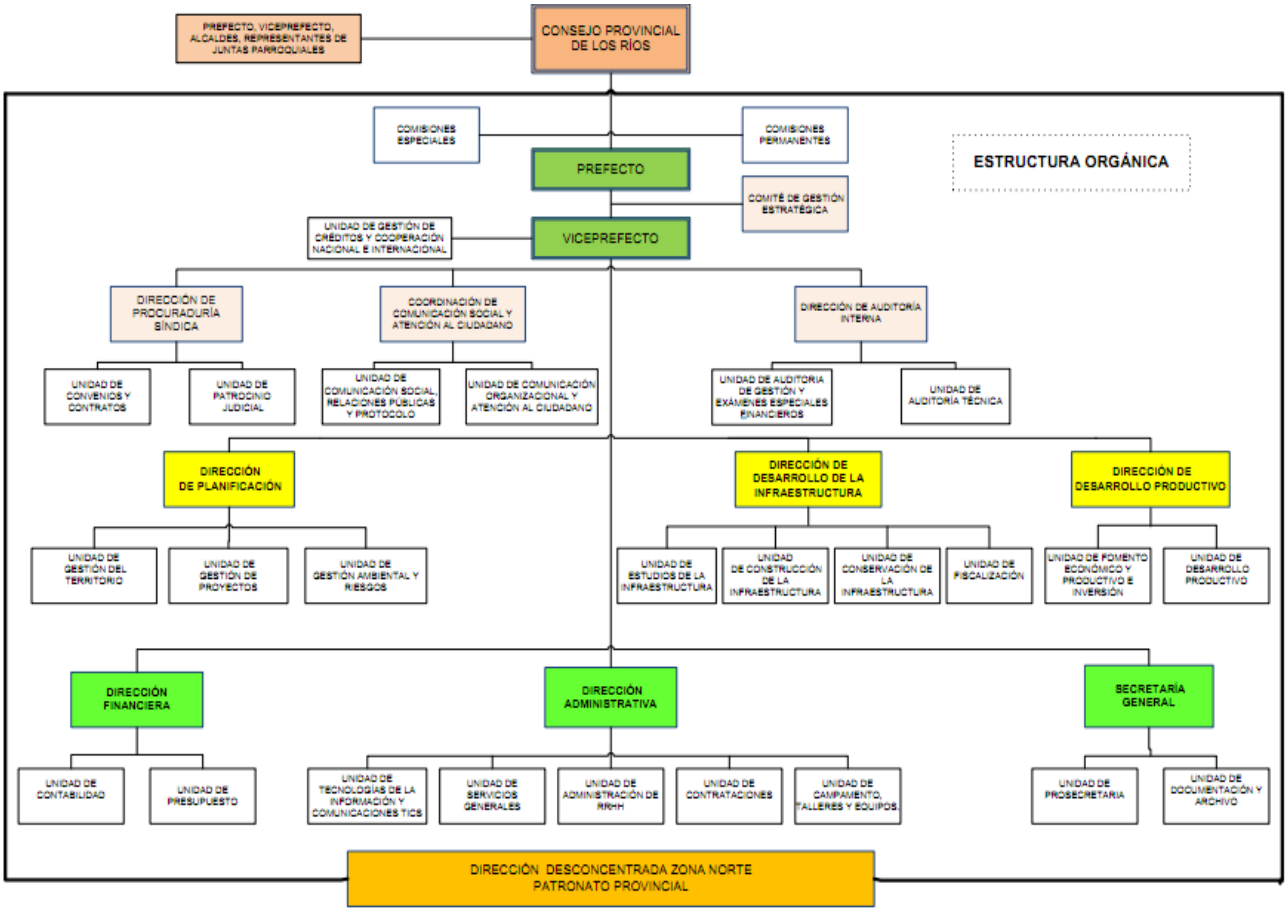
2.2.3.2.3 ESTRUCTURA ORGANIZACIONAL DEL GPLR



2.2.3.2.3 Esquema 2. Estructura Organizacional del GPLR

www.los-rios.gov.ec

[10]http://www.los-rios.gov.ec/documentos/organico.pdf; Unidad de Administración de Recursos Humanos, Pág. 80.81



Esquema 3. Estructura Organizacional del GPLR

www.los-rios.gov.ec

2.2.3.2.4 INFRAESTRUCTURA TECNOLÓGICA

La infraestructura tecnológica es la base primordial de cualquier empresa y permite la optimización de sus recursos, el aumento del valor de su empresa y una respuesta más rápida a los requerimientos del mercado.

La unidad de tecnología de informacióny comunicaciones del Gobierno Provincial de Los Ríoscuenta con lo siguiente:

- Sistemas de cómputo de alto rendimiento simple o distribuido
- Servidores para todo tipo de servicios
- Sistema de respaldo y restauración de datos críticos.

- Estaciones de trabajo de alto rendimiento para todo tipo de labor específica
- Networking y conectividad para todo tipo de demanda.

2.2.4 PLANES DE CONTINUIDAD DE NEGOCIOS

2.2.4.1 ¿QUÉ ES UN PLAN DE CONTINUIDAD DE NEGOCIOS?

Un Plande Continuidad de Negocio tiene como objetivo el mantenimiento de servicios y procesos críticos, así como la reducción de impactos ante imprevistos de indisponibilidad o desastres para en un plazo razonable y con uncoste acotado.

Este servicio está orientado a la obtención de un plan global que garantice la cobertura técnica y organizativa adecuada de las áreas críticas de negocio.

El Plan de Continuidad de Negocio se compone de varias fases que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan a la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Un Plan de Continuidad de Negocio, a diferencia de una Plan de Contingencia, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.

En el desarrollo de un Plan de Continuidad de Negocio existen dos preguntas clave:

• ¿Cuáles son los recursos de información relacionados con los procesos críticos del negocio de la compañía?

• ¿Cuál es el período de tiempo de recuperación crítico para los recursos de información en el cual se debe establecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o aceptables?

Un Plan de Continuidad reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores.

El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

La activación de un Plan de Continuidad debería producirse solamente en situaciones de emergencia y cuando las medidas de seguridad hayan fallado.[11]

2.2.4.2 ALCANCE DE UN PLAN DE CONTINUIDAD DE NEGOCIOS

El Plan de Continuidad de Negocios puede ser desarrollado para toda la organización, un área o un proceso crítico de la misma.

En primer lugar será preciso identificar cuáles serán los departamentos que estarán incluidos en el plan; luego definir cuáles son las amenazas más probables y descartar algunas que podrían ser posibles pero que la posibilidad de su ocurrencia es extremadamente baja.

El Plan de Continuidad de Negocios planea implementar nuevas estrategias y procedimientos que permitan asegurar los recursos de la empresa y operaciones, de tal manera que si existe impacto, sea mínimo ante una eventualidad.

El BCP debe ser diseñado con la finalidad de instaurar una condición de preparación que brinde una respuesta o resultado inmediato diseñado mediante una serie de situaciones estudiadas y definidas previamente.

[11] Guía de Desarrollo de un Plan de Continuidad de Negocio,Ing. Laura del Pino

2.2.4.3 OBJETIVOS DEL PLAN

Los objetivos del plan de continuidad de negocio son:

- ·Salvaguardar los intereses de sus clientes y socios además del negocio y la imagen de la organización.
- Identificar los puntos débiles en los sistemas de la organización.
- Analizar las comunicaciones e infraestructuras.
- Conocer la logística para restablecer los servicios, independientemente de los sistemas.
- Ofrecer alternativas viables a todos los procesos críticos del negocio.

2.2.4.4 BENEFICIOS

Un Plan de Continuidad de Negocios brinda los siguientes beneficios:

- Economiza tiempo además de dinero al momento de confrontar los desastres, interrupciones y contingencia.
- Perfecciona la imagen, progreso y revalorización de la confianza en la organización por parte de la administración, empleados, clientes y todas aquellas personas que se benefician de la empresa al mostrarles que se toman medidas diarias que resultan útiles para garantizar la continuidad del negocio.
- Identifica los diferentes acontecimientos que podrían ser la causa de un impacto sobre lacontinuidad de las actividades y su impacto financiero, humano y de reputación sobre la organización.
- Precisa el conocimiento de las temporadas críticas de recuperación para disponerse a retornar a la situación anterior al desastre sin afectar a la organización.
- Evita las pérdidas para el negocio en caso de calamidades, de no poder evitarlas, minimiza dichas pérdidas.

- Estructura y organiza los activos con la finalidad de prevalecer la protección de los mismos en caso de desastre.
- Brinda a la empresa ventajas competitivas frente a la competencia.
- Implica al personal de recursos humanos de la compañía en las actividades de continuidad.

2.2.4.5 ¿QUIÉN DEBE TENER UN PLAN DE RECUPERACIÓN?

Una pregunta que podemos hacernos es si el tamaño de una organización determina la necesidad o no de tener un Plan de Continuidad.

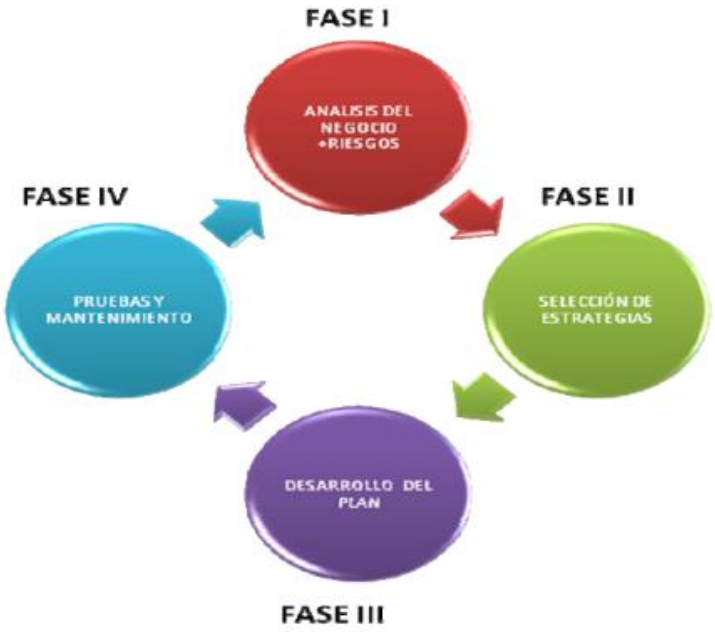
Se puede responder a esta pregunta diciendo que NO. Si una organización es muy grande, con beneficios millonarios, con grandes edificios y gran número de empleados, o si se trata de una persona trabajando en una pequeña oficina con 5 empleados, ambos necesitan asegurar la disponibilidad de su negocio.

De hecho, debido a los pocos recursos y a las pocas opciones de respuesta ante un desastre, en algunos casos sería más vital desarrollar un Plan de Recuperación de Negocio para los pequeños negocios que para las grandes corporaciones.[12]

[12]Guía de Desarrollo de un Plan de Continuidad de Negocio, Ing. Laura del Pino Pág. 6

2.2.4.6 FASES DE UN PLAN DE CONTINUIDAD DE NEGOCIOS.

Podemos dividir un Plan de Continuidad de Negocios en cuatro Fases:



2.2.4.6 Esquema 4. Fases del Plan de Continuidad

Guía de desarrollo del plan de continuidad de negocios

2.2.4.6.1 ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS.

Para desarrollar un Plan de Continuidad con garantía de éxito, lo primero es conocer y entender cuáles son los procesos de negocio que son esenciales dentro de la compañía en la que se va a desarrollar el Plan, con el objetivo de asegurar la continuidad de la actividad en caso de contingencia. Para ello debemos empezar por responder a cuestiones tales como:

- ¿Cuáles son las actividades más importantes para la compañía?
- ¿Cómo afectaría económicamente una interrupción de los servicios a medida que va pasando el tiempo sin reanudar el servicio?

- ¿Cuál sería la capacidad operativa de la empresa a medida que pasa el tiempo?
- ¿Cuál es el plazo máximo para volver a la normalidad sin llegar a incurrir en graves pérdidas?

Las actividades/procesos que se clasifican como esenciales dentro de una compañía suelen ser en su mayoría los Operacionales.

Estos procesos interactúan directamente con los clientes o con otras organizaciones externas a la compañía (Dpto. de Ventas, Dpto. Atención al Cliente, etc.).

También es posible, que estos procesos dependan de otros internos, que también deben ser analizados.

Para conocer cuáles son las necesidades de la compañía en cuanto a estrategias de continuidad, vamos a utilizar dos mecanismos de análisis:

2.2.4.6.1.1 ANÁLISIS DE IMPACTO

Nos permitirá identificar la urgencia de recuperación de cada función de negocio, determinando el impacto en caso de interrupción. Esta información nos permitirá seleccionar cuál es la estrategia más adecuada.

Dentro del Análisis de Impacto podemos distinguir las siguientes actividades:

- Obtención de la Relación de Procesos**:** Establecer los procesos de negocio que se realizan en la compañía.
- Obtención de la Relación de Aplicaciones: Establecer la relación de aplicaciones que soportan los procesos de la compañía.
- Relación de Departamentos y Usuarios**:** Se identifican los departamentos que hay en la empresa y el nombre de las personas que la componen y que intervienen en los procesos.
- Determinar cuáles son los Procesos Críticos: Pueden darse dos valoraciones, una basada en la importancia para la compañía de los procesos cuya ausencia tendría un impacto alto en la

actividad de la compañía (valoración cualitativa). La otra, se referiría a las pérdidas económicas por período debido a la ausencia de los procesos (valoración cuantitativa).

- Período Máximo de Interrupción: El acumulado de pérdidas suele ir creciendo linealmente a medida que pasan los días y las actividades están interrumpidas. No obstante, a partir de un momento que denominaremos Período Máximo de Interrupción, las pérdidas sufren un aumento significativo y las funciones no podrían ser reasumidas.

2.2.4.6.1.2 ANÁLISIS DE RIESGOS

El Objetivo de un análisis de riesgos es identificar y analizar los diferentes factores de riesgo que potencialmente podrán afectar a las actividades que queremos proteger.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el impacto que supondría para la organización. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles.

De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

El objetivo de un Análisis de Riesgos es poner de manifiesto aquellas debilidades actuales que por su situación o su importancia pueden poner en marcha, antes de lo deseable, el Plan de Recuperación de Negocio.

El Análisis de Riesgo debe centrarse en los procesos/actividades del negocio que se han considerado críticos, aunque también puede extenderse a aquellos que no lo son.

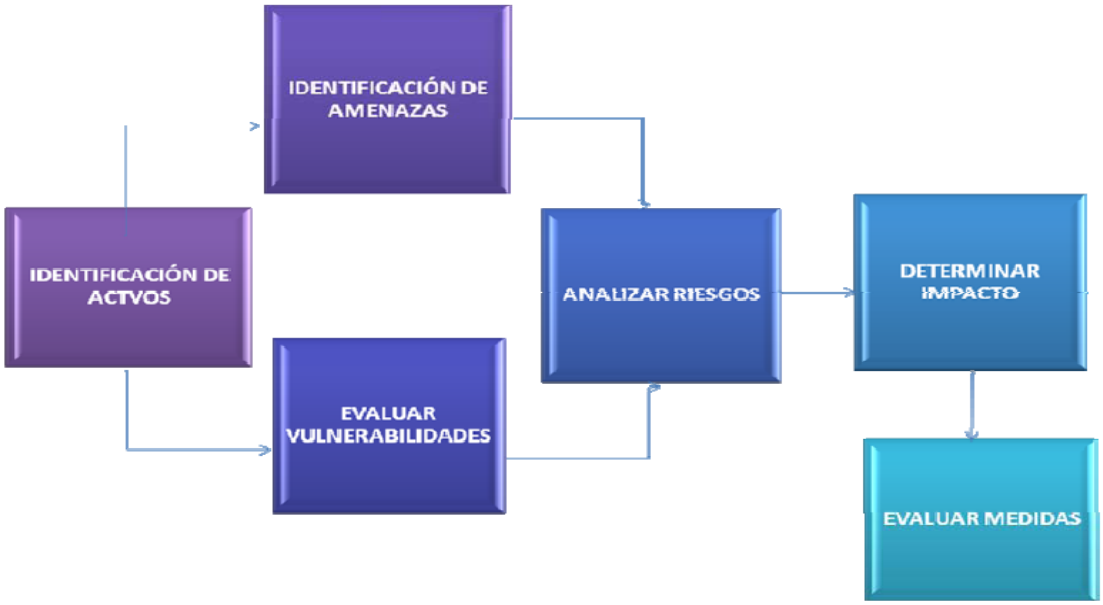
La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles.

De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

En lo fundamental, la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Qué se intenta proteger?
- ¿Cuál es su valor para uno o para la organización?
- ¿Frente a qué se intenta proteger?
- ¿Cuál es la probabilidad de un ataque?

2.2.4.6.1.2 Esquema 5. Análisis de riesgo



Guía de desarrollo del plan de continuidad de negocios

2.2.4.6.1.2.1 IDENTIFICAR ACTIVOS

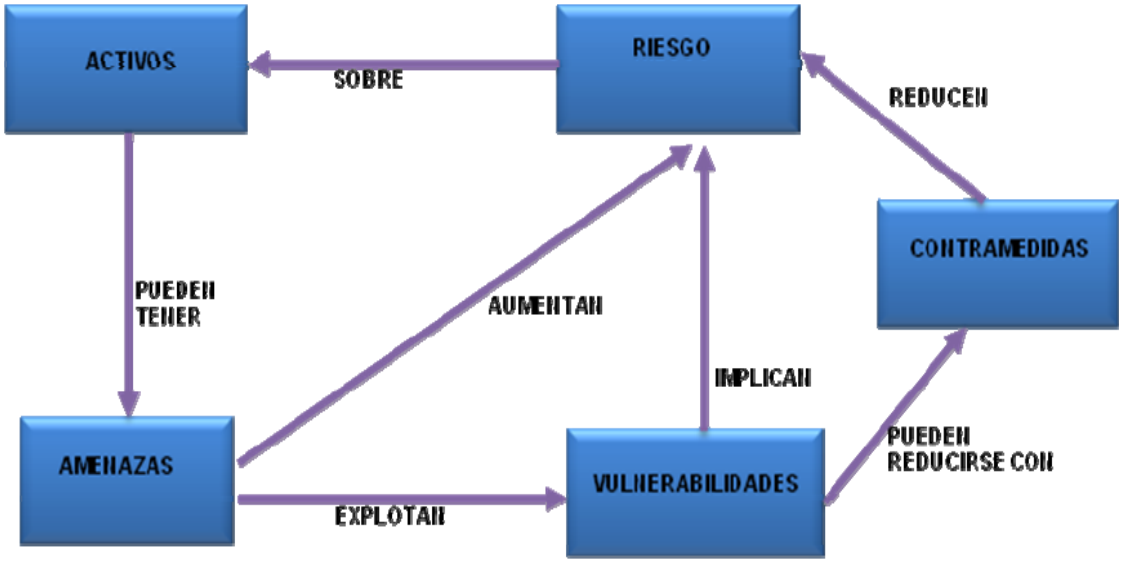
Para cada uno de los procesos críticos de la compañía es necesario realizar un inventario de los activos involucrados en el proceso.

Los activos se definen como los recursos de una compañía que son necesarios para la consecución de sus objetivos de negocio.

Ejemplos de activos de una compañía pueden ser:

- Información
- Equipamiento
- Conocimiento
- Sistemas

A continuación se incluye un esquema con la relación existente entre los diferentes elementos que intervienen en el Análisis de Riesgos.



2.2.4.6.1.2.1 Esquema 6. Componente del análisis de riesgo.
Guía de desarrollo del plan de continuidad de negocios

2.2.4.6.1.2.2 IDENTIFICAR AMENAZAS

Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios.

A la hora de analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir de las más diversas fuentes. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales.

2.2.4.6.1.2.2 Esquema 7. IDENTIFICAR AMENAZAS

2.2.4.6.1.2.3 EVALUAR VULNERABILIDADES

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

Las vulnerabilidades en sí mismas no causan daño alguno, sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo.

2.2.4.6.1.2.4 EVALUACIÓN DEL IMPACTO

Los incidentes causan un impacto dentro de la organización, que también deberá tomarse en cuenta a la hora de calcular los riesgos. La valoración del impacto puede realizarse de forma cuantitativa, estimando las pérdidas

económicas, o de forma cualitativa, asignando un valor dentro de una escala (alto, medio, bajo).

Por ejemplo, el robo de información confidencial de la compañía puede causar un impacto alto si ésta cae en malas manos.

En otro caso, podemos estimar las pérdidas económicas de equipos tangibles valorando el coste de reposición y puesta en marcha.

2.2.4.6.1.2.5 EVALUACIÓN DEL RIESGO

Riesgo es la posibilidad de que se produzca un impacto determinado en la organización. El riesgo calculado es simplemente un indicador ligado al par de valores calculados de vulnerabilidad y el impacto, ambos ligados a su vez de la relación entre el activo y la amenaza a la que el riesgo calculado se refiere.

PROBABILIDAD DE INCIDENTES= AMENAZA X VULNERABILIDAD

RIESGO = PROBABILIDAD DE INCIDENTES X IMPACTO

2.2.4.6.1.2.6 EVALUAR CONTRAMEDIDAS

Para reducir riesgos se utilizan los denominados controles o medidas de seguridad. Podemos clasificar los controles en:

- CONTROLES PREVENTIVOS

  Identifican potenciales problemas antes de que ocurran y previenen errores, omisiones o actos maliciosos.

Ejemplos:

- Realizar copias de seguridad de los archivos.
- Contratar seguros para los activos.
- Establecer procedimientos / políticas de seguridad.
- Establecer control de acceso a la información.
- Establecer control de acceso físico.

- CONTROLES DETECTIVOS

  Identifican y “reportan” la ocurrencia de un error, omisión o acto malicioso ocurrido.

Ejemplos:

- Monitorización de eventos.
- Auditorías internas.
- Revisiones periódicas de procesos.
- Sensores de humo.
- Detección de virus (Antivirus).

- CONTROLES CORRECTIVOS

Minimizan el impacto de una amenaza; Solucionan errores encontrados por controles detectivos e identifican la causa de los problemas con el objeto de corregir errores producidos.

Además modifican los procedimientos para minimizar futuras ocurrencias del problema.

Ejemplos:

- Parches de seguridad.
- Corrección de daños por virus.
- Recuperación de datos perdidos.

Las medidas seleccionadas para disminuir riesgos deben mantener una proporción entre el esfuerzo y coste necesarios para su implantación y el riesgo que mitigan (evaluación del coste-beneficio).

Uno de los objetivos del Plan de Continuidad es evitar en la medida de lo posible que se produzcan incidentes que hagan necesaria su ejecución. Por ello, es importante que la compañía conozca sus riesgos y ponga las medidas adecuadas para corregir el mayor número de vulnerabilidades que puedan provocar un incidente grave.

La evaluación de riesgos debe ser periódica y de acuerdo con el modelo de gestión de riesgos de la organización y en función de la evolución del negocio (crecimiento), de cambios importantes en la organización (procesos internos), nuevas obligaciones legales, etc.

2.2.4.6.2 SELECCIÓN DE ESTRATEGIAS.

Existen diferentes estrategias para mitigar el impacto de una interrupción. Cada una de estas estrategias tiene unos parámetros de tiempo, disponibilidad y costes asociados que serán más o menos apropiados dependiendo de las funciones de negocio.

A continuación se describen diferentes estrategias para reubicación funcional:

- No hacer nada**:** Este tipo de actuación podría utilizarse en aquellas funciones o actividades que se han clasificado como "no urgentes" en el Análisis de Impacto. En este tipo de estrategia se asume el riesgo.
- Utilización de espacios propios**:** Espacios existentes en la compañía tales como salas de formación, cafeterías, etc. Este tipo de estrategia requiere una planificación minuciosa.
- Reutilización de recursos**:** Reubicación de personal con funciones no urgentes en tareas que requieren una mayor prioridad. En este caso se debe poner cuidado en convertir la función no urgente en urgente por ser desatendida durante demasiado tiempo.
- Trabajo Remoto o Teletrabajo**:** Posibilidad de trabajar desde ubicaciones exteriores a la compañía mediante conexión remota.
- Acuerdos Recíprocos**:** Acuerdos entre dos organizaciones (o dos unidades de negocio de la propia compañía diferentes) con características de equipamiento/espacio similares que permitiría a cada una de las partes recuperar funciones en la otra localización. En este caso es importante definir las condiciones de uso y la realización de pruebas periódicas para asegurar las condiciones pactadas.
- Sitio alternativo subcontratado a terceros**:** Contratación con compañías especializadas de espacios alternativos para la recuperación de la actividad. En este caso hay que asegurar que estas compañías pueden proporcionar unos tiempos de recuperación acordes con las necesidades de la organización.

Este tipo de compañías pueden proporcionar diferentes de soluciones:

- Espacio dedicado**:** Se garantiza la disponibilidad inmediata del espacio. En contrapartida este servicio es más caro que otras alternativas.
- Espacio compartido**:** Se comparte el espacio con otras compañías. Es más barato que un centro dedicado.
- Espacios móviles**:** Se pueden utilizar rápidamente, pero tienen un espacio limitado.
- Módulos prefabricados**:** Pueden tardar unos días en estar disponibles para su uso.

• Localizaciones diversas**:** Se traslada la operación pero no el personal.

• Centro replicado**:** Solución que permite trasladar de forma inmediata la operación y continuar la actividad rápidamente. También puede denominarse “centro espejo”. Esta solución es normalmente la más cara, pero también la mejor solución en el caso de que se necesite una recuperación muy rápida de la operación.

Además deberá considerarse factores como:

- Ubicación y superficie requerida
- Espacio suficiente
- Zonas acondicionadas para acoger a personal

RECURSOS TÉCNICOS NECESARIOS**:**

- Hardware
- Software
- Comunicaciones
- Datos de respaldo

RECURSOS HUMANOS REQUERIDOS

RECURSOS MATERIALES Y DE INFRAESTRUCTURA

- Servicios auxiliares necesarios
- Tiempos de activación
- Coste

Una vez tomada la decisión sobre el tipo de estrategia que se utilizará como respaldo en caso de interrupción del negocio, pasaremos a desarrollar todos los procedimientos, funciones y actividades que permitirán restablecer los procesos de negocio en unos plazos razonables.

2.2.4.6.3 DESARROLLO DEL PLAN

A partir de aquí desarrollaremos “nuestro Plan de Continuidad”. Para ello definiremos:

- Los equipos necesarios para el desarrollo del Plan.
- Las responsabilidades y funciones de cada uno de los equipos.
- Las dependencias orgánicas entre los diferentes equipos.
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.
- Los procedimientos de actuación ante incidentes.
- La estrategia de vuelta a la normalidad.

2.2.4.6.3.1 ORGANIZACIÓN DE LOS EQUIPOS

Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollarse en las distintas fases del Plan.

Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, a continuación se muestran algunos ejemplos de los equipos que pueden formar parte del Plan:

- Comité de Crisis**:** Encargado de dirigir las acciones durante la contingencia y recuperación.
- Equipo de Recuperación**:** Su función es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.).
- Equipo Logístico: Responsable de toda la logística necesaria en el esfuerzo de recuperación.
- Equipo de las Unidades de Negocio: Encargados de la realización de pruebas que verifiquen la recuperación de los sistemas críticos.
- Equipo de Relaciones Públicas: Encargado de las comunicaciones a los medios de comunicación y clientes.

El personal asignado a cada uno de los equipos puede variar dependiendo del tamaño de la organización y de la estrategia de recuperación seleccionada. Una persona puede pertenecer a más de un equipo, siempre y cuando no existan incompatibilidades en las tareas a realizar.

2.2.4.6.3.1.1 EQUIPO DIRECTOR O COMITÉ DE CRISIS

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 “clave” durante los incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndoles 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.

2.2.4.6.3.1.2 EQUIPO DE RECUPERACIÓN

El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación.

Esto incluye todos los servidores, PC's, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio.

2.2.4.6.3.1.3 EQUIPO LOGÍSTICO

Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:

- Transporte de material y personas (si es necesario) al lugar de recuperación.
- Suministros de oficina.
- Comida.
- Reservas de hotel, si son necesarias.
- Contacto con los proveedores.

Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas.

2.2.4.6.3.1.4 EQUIPO DE RELACIONES PÚBLICAS Y ATENCIÓN A CLIENTES

Se trata de canalizar la información que se realiza al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son:

- Elaboración de comunicados para la prensa.
- Comunicación con los clientes.

Uno de los valores más importantes de una compañía son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación.

2.2.4.6.3.1.5 EQUIPO DE LAS UNIDADES DE NEGOCIO

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

Cada equipo deberá configurar las diferentes pruebas que deberán realizar para los sistemas.

2.2.4.6.3.2 DESARROLLO DE PROCEDIMIENTOS

Una vez que hemos definido los equipos y se han establecido las funciones que debe desempeñar cada equipo, tenemos que desarrollar los procedimientos que van a seguir, y su actuación en cada una de las fases de activación del Plan de Continuidad.

2.2.4.6.3.2.1 FASE DE ALERTA

La Fase de Alerta define los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos. Dividiremos esta fase en tres partes:

- NOTIFICACIÓN**:** Define cómo y quién debe ser informado en primera instancia de lo ocurrido.

	EVENTO	ACCIÓN
1	Situación de contingencia/incidente detectado por algún empleado de la compañía. (Fuego, inundación, virus, etc.).	Aviso inmediato con el **máximo detalle posible** al Responsable de Personal de turno o a Seguridad.
2	El responsable de turno o de seguridad conoce que ha sucedido una contingencia.	Aviso a la persona de contacto del Comité de Crisis. Aviso a los equipos de emergencia (si procede).

2.2.4.6.3.2.1 Tabla 1. Fase de Notificación

Guía de Desarrollo de Plan de Continuidad

- **Evaluación**: Análisis de la situación y valoración inicial de los daños. Definición de estrategias.

	EVENTO	ACCIÓN
3	Conocimiento por algún miembro del Comité de incidente ocurrido.	El equipo del Comité se reunirá en un **lugar acordado previamente** y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad. Será necesario informar de la situación a los siguientes responsables: • Responsable de Seguridad. • Comité de Dirección de la Empresa. • Relaciones Públicas. • Equipo de Recuperación. • Responsable de los Equipos.

2.2.4.6.3.2.1 Tabla 2. Fase de Evaluación
Guía de Desarrollo de Plan de Continuidad

- **Ejecución del Plan:** Decisión del equipo director de disparar el Plan debido al alcance de los daños.

	EVENTO	ACCIÓN
4	Consideración por parte del Comité de Crisis y ejecución del Plan.	Iniciar el árbol de llamadas. Informar al Comité de Dirección.
5	Paso a la Fase de Transición.	

2.2.4.6.3.2.1 Tabla 3. Fase de Ejecución
Guía de Desarrollo de Plan de Continuidad

2.2.4.6.3.2.2 FASE DE TRANSICIÓN

La Fase de Transición es la fase previa a la de recuperación de los sistemas. Es importante que en esta fase exista una coordinación entre los diferentes dispositivos y equipos de logística, ya que son éstos los encargados de que todo esté disponible para comenzar la recuperación en el menor tiempo posible.

Podemos dividir la fase de transición en dos partes principalmente:

- PROCEDIMIENTOS DE CONCENTRACIÓN Y TRASLADO DE PERSONAS Y EQUIPOS.

Dependiendo de la solución final que se decida como estrategia de respaldo, este procedimiento puede variar. Realizaremos una descripción general de los procedimientos, que podrá completarse una vez que se tome una solución definitiva.

Una vez avisados los equipos y puesto en marcha el Plan, deberán acudir al centro de reunión. En el caso de que la emergencia se declare en horas de trabajo, se tomará como punto de encuentro los lugares designados en el Plan de Emergencia. Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como centro de respaldo, o cualquier otro designado por el Comité de Dirección de Crisis.

Además del traslado de personas al centro de recuperación (si es necesario) hay que realizar una importante labor de coordinación para el traslado de todo el material necesario para poner en marcha el centro de recuperación (cintas de backup, material de oficina, documentación...)

- PROCEDIMIENTOS DE PUESTA EN MARCHA DEL CENTRO DE RECUPERACIÓN.

Una vez concentrados los distintos equipos que van a intervenir en la recuperación, y con todos los elementos necesarios disponibles para comenzar la recuperación, hay que poner en marcha este centro, estableciendo la infraestructura necesaria, tanto de software como de comunicaciones, etc.

2.2.4.6.3.2.3 FASE DE RECUPERACIÓN.

Una vez que hemos establecido las bases para comenzar la recuperación, se procederá a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suele precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados.

Podemos dividir esta fase en dos:

• Procedimientos de Restauración

Estos procedimientos se refieren a las acciones que se llevan a cabo para restaurar los sistemas críticos.

• Procedimientos de Gestión y Soporte.

Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el negocio con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

2.2.4.6.3.2.4 FASE DE VUELTA A LA NORMALIDAD

Una vez con los procesos críticos en marcha y solventada la contingencia, debemos plantearnos las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento.

Para ello vamos a dividir esta fase en diferentes procedimientos:

• Análisis del impacto.

El análisis de impacto pretende realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad.

• Procedimientos de vuelta a la normalidad.

Una vez determinado el impacto deben establecerse los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total de funcionamiento.

Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

2.2.4.6.4 PRUEBAS Y MANTENIMIENTO.

2.2.4.6.4.1 TIPOS DE PRUEBAS

Las pruebas de un Plan de Continuidad deben tener dos características principales:

- Realismo**:** La utilidad de las pruebas se reduce con la selección de escenarios irreales. Por ello es importante reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.
- Exposición Mínima**:** Las pruebas deben diseñarse de forma que impacten lo menos posible en el negocio, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, debe realizarse una ventana de tiempo que impacte lo menos posible en el negocio.

En algunos casos puede resultar complicado realizar una prueba completa del Plan de Continuidad de Negocios. Por ello, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal se han ensayado durante un período de tiempo.

2.2.4.6.4.2 MANTENIMIENTO DEL PLAN DE CONTINUIDAD

Por la propia dinámica de 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 quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.[13]

[13]Guía de Desarrollo de un Plan de Continuidad de Negocio, Ing. Laura del Pino, Pág. 7 - 36

2.2 HIPÓTESIS Y VARIABLES

2.3.1 HIPÓTESIS

Con la realización de una auditoría Informática brindaremos y garantizaremos la continuidad de negocios en el Gobierno Autónomo Descentralizado de la Provincia de Los Ríos

2.3.2 VARIABLES

Variable Independiente: Auditoría Informática

Variable Dependiente: Plan de Continuidad de Negocios y Contingencia

CAPITULO III

3. MARCO METODOLÓGICO

3.1 MODALIDAD DE LA INVESTIGACIÓN

El presente estudio es netamente investigativo, un proyecto basado en la modalidad cualitativa que es la descripción de las cualidades de un fenómeno, mediante ella buscaremos explicar el por qué y el cómo se tomó una decisión, en contraste con la investigación cuantitativa la cual busca responder preguntas tales como cuál, dónde, cuándo proporcionándonos un mejor enfoque de la información obtenida a través de los instrumentos de la auditoría (entrevistas, encuestas, etc.)

3.2 TIPOS DE INVESTIGACIÓN

3.2.1 Bibliográfica

Llevaremos a cabo una investigación bibliográfica ya que es la etapa en la que se explora lo que se ha escrito en la comunidad científica sobre el tema Auditoría Informática.

3.2.2 De Campo

En la investigación de campo nos enfocaremos en informaciones que provienen entre otras, de entrevistas, cuestionarios, encuestas y observaciones con el fin de describir de qué modo o porque causas se produce una situación o acontecimiento particular. Esta investigación se realiza en el mismo lugar de los hechos, es decir donde se desarrolla o producen los sucesos, en contacto directo con quien o quienes son los gestores del problema que se investiga.

3.2.3 Descriptiva

Por el objetivo que se persigue, será indispensable este tipo de investigación, ya que se busca describir el fenómeno o una situación mediante su estudio, en una circunstancia tiempo – espacio determinado, la investigación descriptiva se caracteriza por enfatizar aspectos de categorías bien definidas del fenómeno observado.

3.3 POBLACIÓN Y MUESTRA

La población se define como "el conjunto para el cual serán válidas las conclusiones que se obtengan a los elementos o unidades a las cuales se refiere la investigación"

Para el efecto de esta investigación, la población estará conformada por los empleados y funcionarios de los distintos departamentos del Gobierno Provincial de los Ríos.

Para obtener la muestra que necesitaremos con la finalidad de conocer el número de personas con quienes nos entrevistaremos, se desarrolla la siguiente fórmula:

$$n = \frac{Z * P}{(P - 1)(Z^2 \div 2^2) + Z}$$

SIMBOLOGÍA.

N = Tamaño de muestra

Z= Valor de Confianza (de 0.05)

P = Población. (Funcionarios y empleados).

La cantidad de empleados que laboran en el Gobierno Provincial de Los Ríos, se muestra en el siguiente recuadro:

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE LOS RÍOS	
EMPLEADOS	**VALOR**
CON NOMBRAMIENTO	230
CONTRATADOS	352
Total	582

3.3 Tabla 4. Cantidad de empleados del GPLR

Tomando en consideración los datos anteriores, determinaremos la muestra:

$$n = \frac{Z * P}{(P-1)(Z^2 \div 2^2) + Z}$$

$$n = \frac{0{,}05 * 582}{(582-1)(0{,}05^2 \div 2^2) + 0{,}05}$$

$$n = \frac{29{,}1}{(581)(0{,}0025 \div 4) + 0{,}05}$$

$$n = \frac{29{,}1}{(581)(0{,}000625) + 0{,}05}$$

$$n = \frac{29{,}1}{(0{,}363125) + 0{,}05}$$

$$n = \frac{29{,}1}{0{,}413125}$$

$$n = 70{,}4387292$$

En base al resultado que hemos obtenido, el número de personas a encuestar será 70.

3.4 MÉTODOS, TÉCNICAS E INSTRUMENTOS

3.4.1 MÉTODOS Y TÉCNICAS

La metodología aplicada consiste en un proceso que va desde obtener el entendimiento de la empresa, identificación de posibles eventos, su impacto y valoración, definición de estrategias, elaboración del plan, desarrollo de una cultura, hasta la prueba, mantenimiento y auditoría del BCP; todo con el propósito de garantizar una respuesta flexible, suficiente y capaz a los eventos de riesgo en que puede verse involucrada la empresa.

Los métodos y técnicas a utilizar en el análisis del objeto de estudio en este proyecto investigativo son los siguientes:

- Diagnósticos
- Evaluaciones Diagnosticas
- Aplicación de Metodologías
- Estudios Comparados
- Análisis Estadísticos
- Estrategias investigativas

3.4.2 INSTRUMENTOS

En la medida en que la Gerencia de Riesgos alcance un desarrollo importante dentro de la empresa, necesitará de instrumentos y ayudas para su gestión, estos instrumentos o herramientas son indispensables para el desarrollo del BCP en las diferentes situaciones definidas dentro del plan. Es necesario, para una eficaz y ágil puesta en marcha del plan, que la información de continuidad de negocio de las diferentes unidades, se pueda actualizar directamente y vía web por los diferentes implicados y responsables.

A continuación visualizamos uno de los instrumentos a utilizar:

Dirigido a: Empleados con nombramiento y contratados del GPLR

Objetivo: Identificar el grado de necesidad de un Plan de Continuidad de Negocios y Contingencia en el Gobierno Autónomo Provincial de Los Ríos.

PREGUNTAS	RESPUESTAS
1. ¿Considera adecuada la infraestructura de la unidad de TIC's, que actualmente posee el GPLR?	Si ( ) No ( )
Porqué _____ _____	
2. ¿En caso de existir medidas de seguridad para proteger el equipo, considera que éstas medidas son las correctas?	Si ( ) No ( )
Porqué _____ _____	
4. ¿Qué tipo de mantenimiento se les da a las computadoras?	Preventivo ( ) Correctivo ( ) Ambos ( )
Porqué _____ _____	
5. ¿Cuenta la institución con las respectivas licencias del Software adquirido?	Si ( ) No ( )
6. ¿Existen algún tipo de alarma para:	Detectar Fuego () Detectar fuga de agua ( ) De desalojar el edificio en caso de desastres ( )
7. ¿Existen salidas de Emergencia?	Si ( ) No ( )
8. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?	Si ( ) No ( )
Porqué_____ _____	
9. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?	Si ( ) No ( )

Porqué_____ _____	
10. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?	Si ( ) No ( )
Porqué_____ _____	
11. ¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?	Si ( ) No ( )
Porqué_____ _____	
12. ¿Considera que la aplicación de un manual de auditoría informática le ayudaría a mejorar la gestión administrativa del GPLR?	Si ( ) No ( )
Porqué_____ _____	

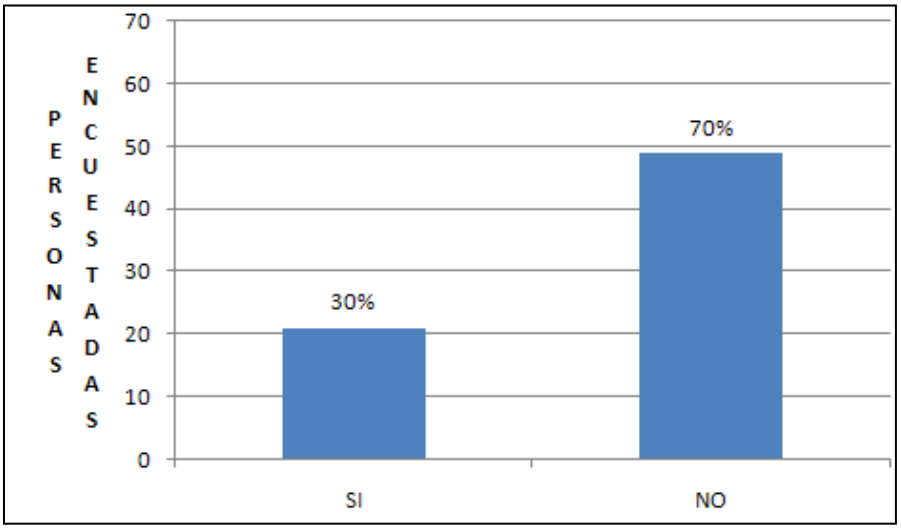
3.5 INTERPRETACIÓN DE LOS RESULTADOS

3.5.1 Interpretación de los resultados de las encuestas realizadas a los empleados del Gobierno Provincial de Los Ríos.

A la muestra de 582 empleados se les realizó el siguiente análisis:

1. ¿Considera adecuada la infraestructura de la unidad de TIC's, que actualmente posee el GPLR?

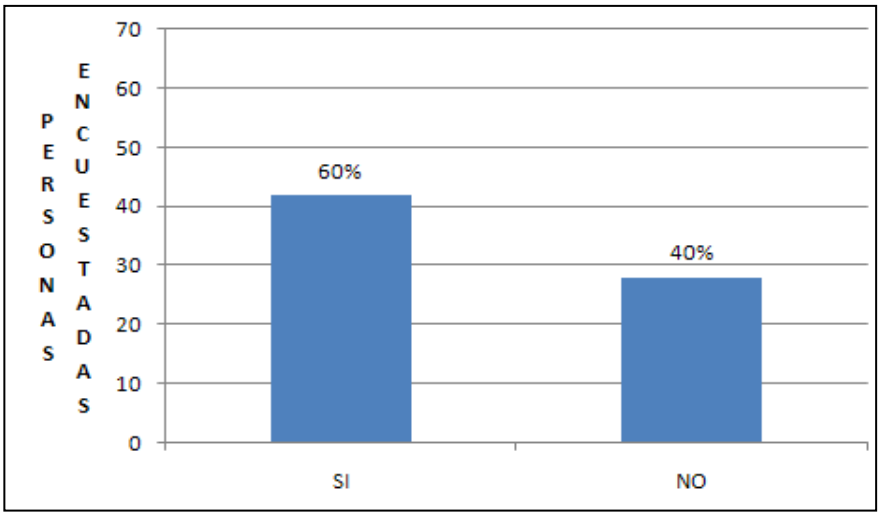
RESPUESTAS	CANTIDAD
SI	21
NO	49



Podemos observar que más de un 50% de los empleados del Gobierno Provincial de Los Ríos no cree que la infraestructura la Unidad de Tecnologías y Comunicaciones sea la adecuada para el rol tan importante que desempeña en ésta organización.

2. ¿Existe servicio de mantenimiento para el mobiliario y equipo?

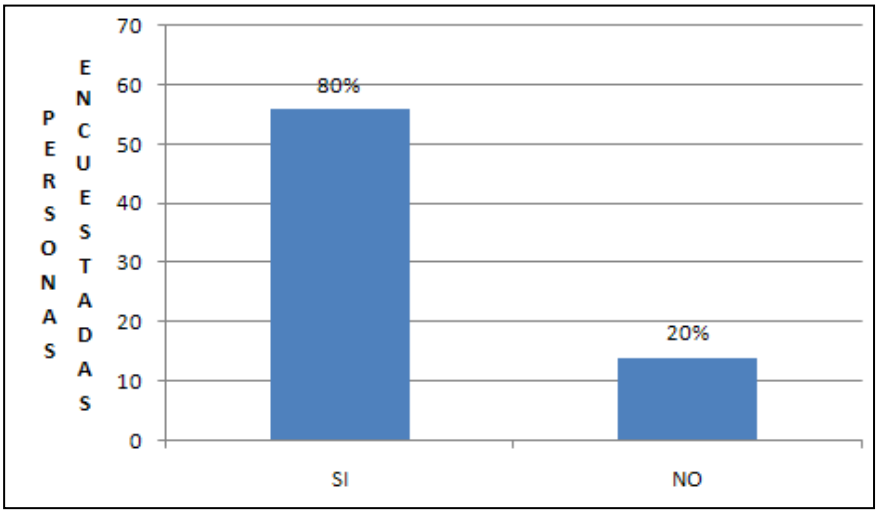
RESPUESTAS	CANTIDAD
SI	42
NO	28



Con una diferencia del 20% en su mayoría los empleados confirman la existencia de un servicio de mantenimiento de mobiliario y equipo, a pesar de ser 28 personas las que consideran que no existe este mantenimiento, podría indicar que no en toda la organización se lleva a cabo dicho servicio.

3. ¿En caso de existir medidas de seguridad para proteger el mobiliario y equipo, considera que éstas medidas son las correctas?

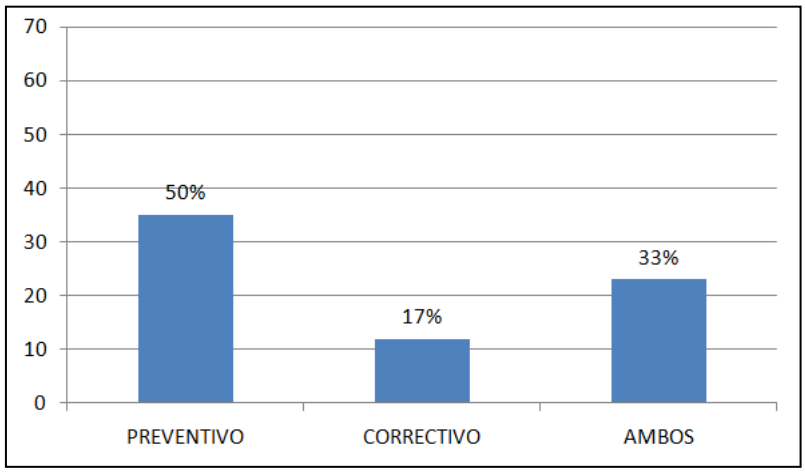
RESPUESTAS	CANTIDAD
SI	56
NO	14



Resulta fácil notar que más de la mitad delaspersonas encuestadas están de acuerdo con las medidas de seguridad que tenga la empresa con la finalidad de proteger el mobiliario y equipo aunque por la versión de los demás empleados tal vez deberían realizarse algunas modificaciones o reforzar dichas medidas.

4. ¿Qué tipo de mantenimiento se les da a las computadoras?

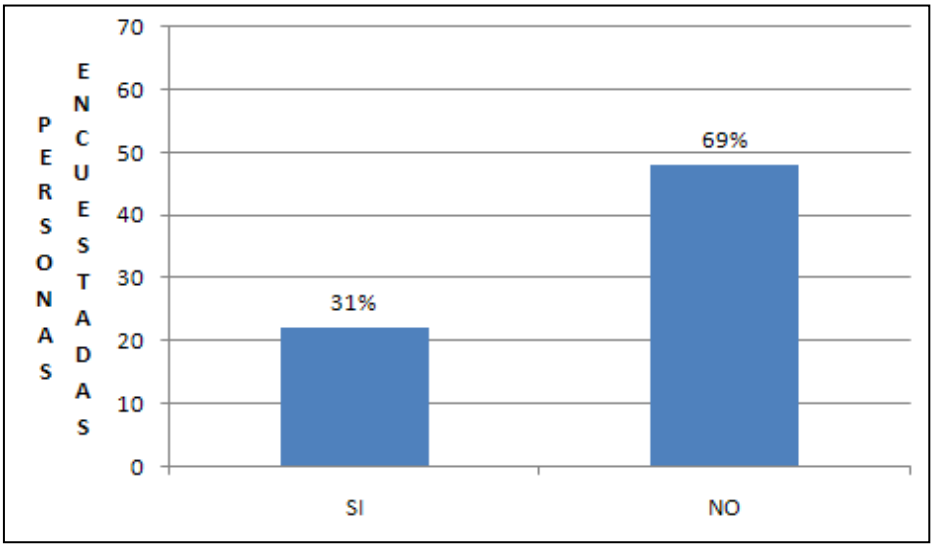
RESPUESTAS	CANTIDAD
PREVENTIVO	35
CORRECTIVO	12
AMBOS	23



Debido a los datos proporcionados conocemos que exactamente la mitad de las personas encuestadas indican que el tipo de mantenimiento que se brinda a las computadoras es preventivo, también se nos ha dado a saber que además se llevan a cabo ambos tipos de mantenimiento aunque en un menor porcentaje.

5. ¿Cuenta la institución con las respectivas licencias y facturación del Software adquirido?

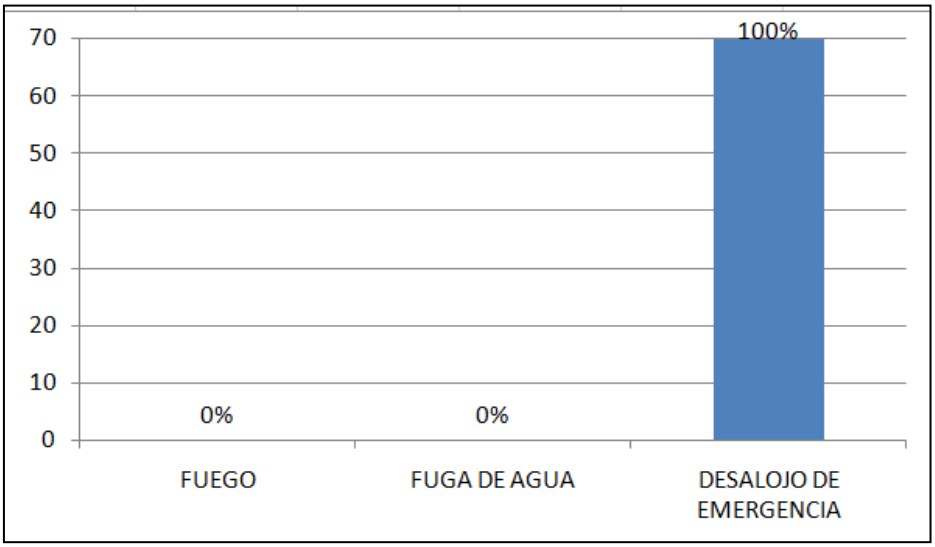
RESPUESTAS	CANTIDAD
SI	22
NO	48



Éste sería un buen punto de estudio ya que un mayor porcentaje de empleados nos indican que la organización no cuenta con licencias y facturación de software, lo que significa que no están cumpliendo con leyes establecidas o simplemente los empleados no están al tanto de todas las políticas de la institución caso que podría generar confusiones, malos entendidos e incluso problemas a la misma.

6. ¿Existen algún tipo de alarma para:

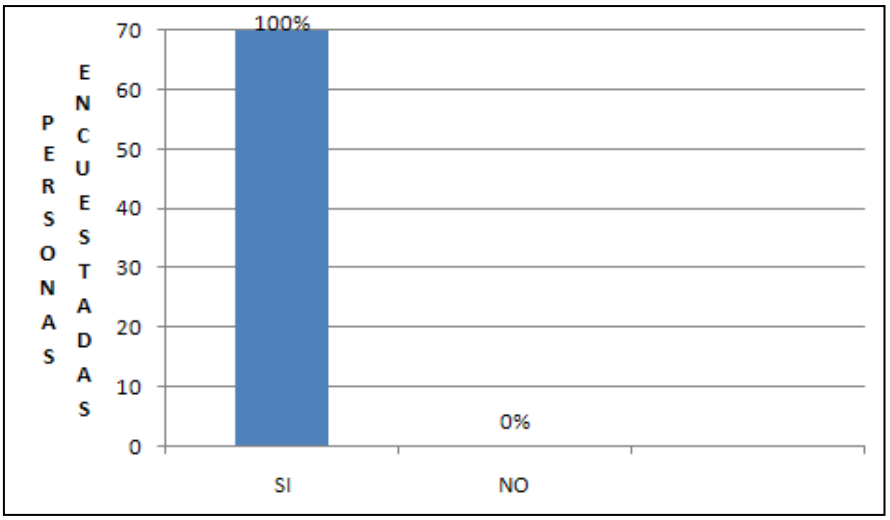
RESPUESTAS	CANTIDAD
FUEGO	0
FUGA DE AGUA	0
DESALOJO DE EMERGENCIA	70



Como podemos visualizar la totalidad de los empleados encuestados afirman que existe una alarma que indica el desalojo de emergencia, al parecer la organización no cuenta con alarmas para fuego o fuga de agua, lo que posiblemente se deba a que no han tenido inconvenientes en temporadas anteriores que requieran de éstas alarmas, sin embargo son de mucha utilidad.

7. ¿Existen salidas de Emergencia?

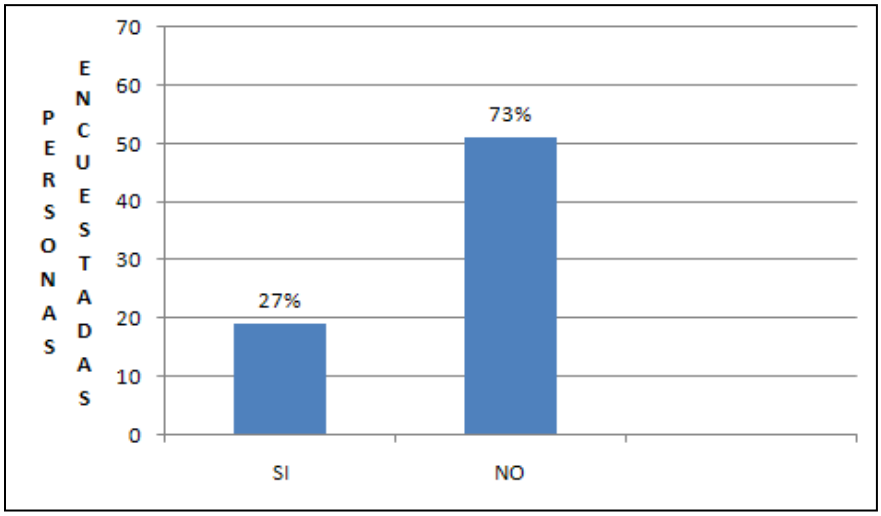
RESPUESTAS	CANTIDAD
SI	70
NO	0



En este caso no hay mucho que argumentar, de acuerdo a los resultados que se han obtenido se nos indica que el Gobierno Provincial de Los Ríos cuenta con salidas de emergencia que se consideran muy importantes en toda organización.

8. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

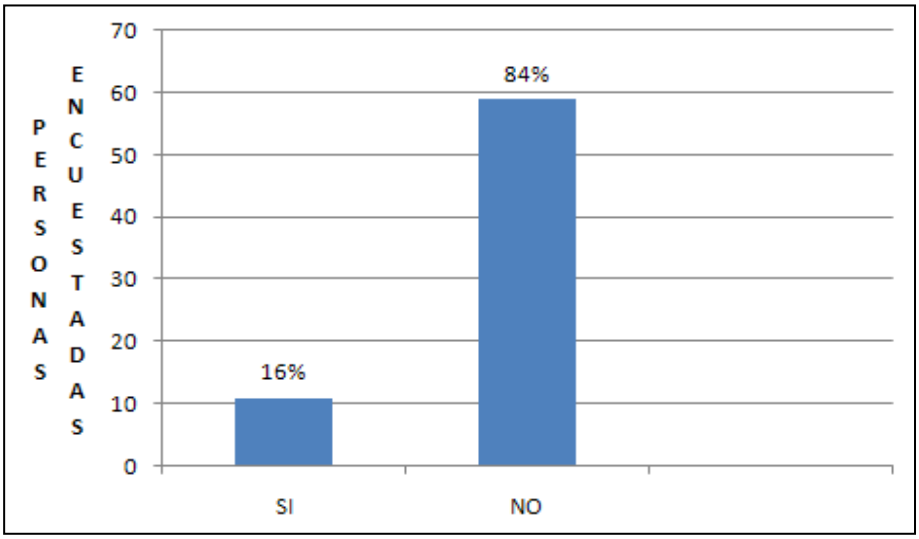
RESPUESTAS	CANTIDAD
SI	19
NO	51



Tal parece que no todos los empleados del GPLR consideran que exista la protección y etiquetado de interruptores puesto que la mayoría de ellos así lo afirman en sus respuestas, aunque un menor porcentaje asegura lo contrario, tal vez se deba a que si existe la debida protección en ciertas áreas y posiblemente se ha descuidado otras de ellas.

9. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?

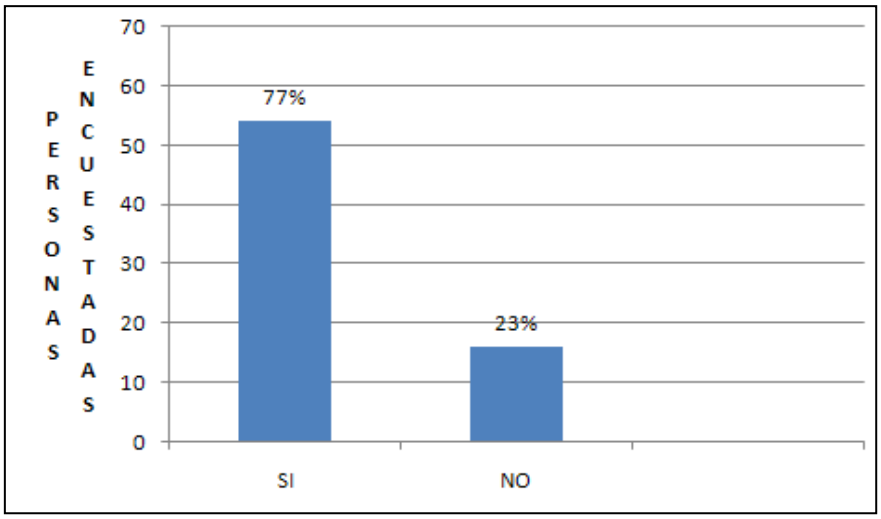
RESPUESTAS	CANTIDAD
SI	11
NO	59



En muchas ocasiones resulta necesario el ingreso de programadores, analistas y operadores a los programas y archivos de la organización, sin embargo notamos que en su mayoría no está permitido, lo que probablemente podría tratarse de una medida de seguridad en la que solo puedan acceder a ciertas áreas con restricciones.

10. ¿Existen procedimientos escritos para la recuperación del sistema en caso de las fallas?

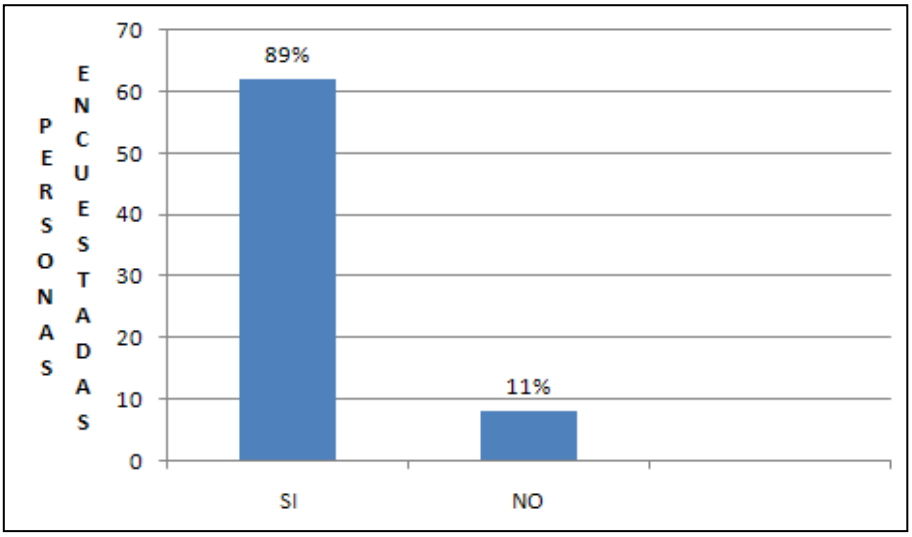
RESPUESTAS	CANTIDAD
SI	54
NO	16



La precaución que se tiene en la organización en cuanto a respaldos de información por parte de la mayoría de los empleados es evidente, pero también es notable que no todos crean las copias de los archivos en un lugar distinto al de la computadora.

11. ¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?

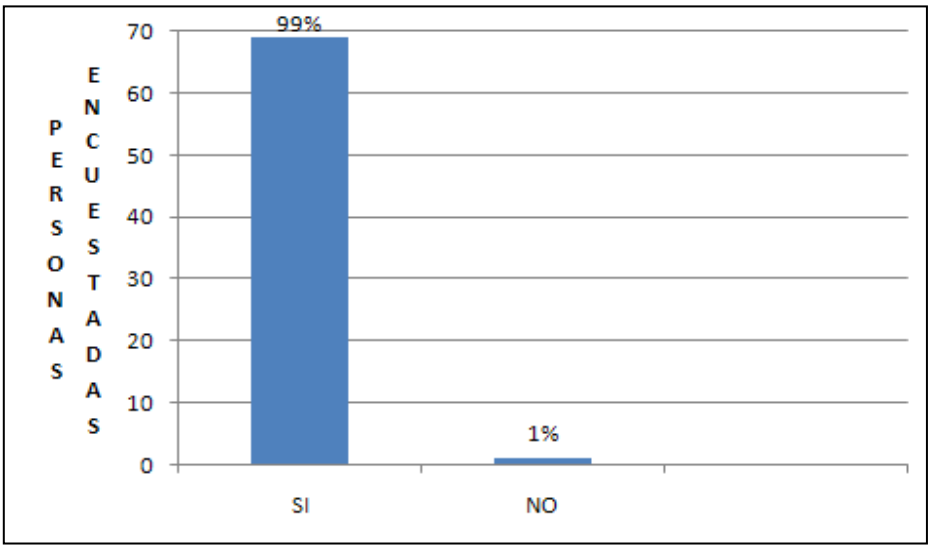
RESPUESTAS	CANTIDAD
SI	62
NO	8



En un porcentaje bastante alto, con muy poca diferencia los empleados tienden a asegurar el respaldo de mantenimiento y asistencia técnica, ya que la organización cuenta con un personal capacitado en servicio técnico informático, lo que consideran de vital importancia para evitar serios inconvenientes a futuro como retrasos, baja productividad e incluso la paralización total de su actividad empresarial.

12. ¿Considera que la aplicación de un manual de auditoría informática le ayudaría a mejorar la gestión administrativa del GPLR?

RESPUESTAS	CANTIDAD
SI	69
NO	1



Como podremos observar casi en su totalidad los empleados encuestados consideran que la aplicación de un manual de auditoría informática ayudaría a mejorar la gestión administrativa y mejor aún asegurar la continuidad de negocios mediante un Plan de Contingencia.

3.6 CONCLUSIONES Y RECOMENDACIONES

3.6.1 CONCLUSIONES

Actualmente la informática sirve como apoyo para la sistematización de las áreas de negocio tales como: la administración, el manejo de la contabilidad y la nómina, lo cual causa como efecto que sea necesaria la realización periódica de un ejercicio práctico y formal de la auditoría en informática que permita asegurar que los recursos informáticos se están utilizando de manera adecuada para lograr los objetivos de la institución auditada.

El ámbito de auditoría ofrece gran cantidad de herramientas y modelos que se pueden tomar como referencia para definir la manera en la que se debe actuar para administrar adecuadamente los recursos y operaciones de los sistemas informáticos.

Considerando los resultados de la encuesta realizada y basándonos en la interpretación de los mismos, creemos que existen varios temas de gran interés por estudiar y dar a conocer a todo el personal que labora en el Gobierno Autónomo Descentralizado de la Provincia de Los Ríos, ya que es necesario que ellos deban estar enterados al máximo sobre reglas, normas o políticas de la organización e incluso que deban contribuir para lograr mejorar la gestión de la misma.

3.6.2 RECOMENDACIONES

Es recomendable la adopción de herramientas adecuadas en las que se base el personal de la de Tecnología de Información y Comunicaciones para la administración de los recursos tecnológicos.

Se debe poner gran énfasis a los procedimientos de control y seguridad de la información puesto que hoy por hoy se ha constituido en un bien sumamente importante, por ende debe realizarse el análisis de las diferentes técnicas que pueden utilizarse para la detección, mitigación de riesgos y aseguramiento de la información.

Sería importante que el GADPLR adopte como una buena práctica, la planificación y la realización de ejercicios periódicos de auditoría informática, los cuales además de evaluar los sistemas de información deben hacer un seguimiento de recomendaciones señaladas por consultores externos para mejorar su situación actual.

Teniendo en cuenta el rol tan importante que desempeña ante la sociedad el Gobierno Autónomo Descentralizado de la Provincia de Los Ríos y el peligro al que toda organización se encuentra expuesta en la actualidad tales como delitos informáticos, pérdida de información, etc., recomendamos al Prefecto Provincial Sr. Marcos Troya F. o funcionarios encargados se nos solicite el desarrollo de un Plan de Continuidad que nos permita brindarles y garantizarles la Continuidad de negocios o actividades de la organización.

CAPÍTULO IV

4. MARCO PROPOSITIVO

4.1 INTRODUCCIÓN

La evolución de los sistemas de información y comunicación en nuestro País y a nivel mundial, ha generado la necesidad de implementar la gestión de sistemas en las diferentes instituciones; para obtener seguridad, confiabilidad y escalabilidad en todos los ámbitos que a estas conciernen. La velocidad con que los medios de comunicación progresan, han hecho que las empresas cada vez necesiten de más control sobre sus datos y los sistemas que estas utilizan, provocando con ello el que el procesamiento de la información y la rapidez con la que se realiza se vuelva de vital importancia.

El Gobierno Provincial de Los Ríos y su Unidad de Tecnología de la Información y Comunicación, ejecutan proyectos relacionados con el área informática con el fin de apoyar a las distintas actividades que se desarrollan dentro de ella, por lo que se vuelve indispensable controlar que se entreguen los servicios requeridos, que exista una correcta capacitación para su uso y un adecuado soporte que permita la continuidad de las operaciones en caso de suscitarse cualquier tipo de problema o incidente. Ésta resulta ser una motivación para que el Gobierno Autónomo Descentralizado de la Provincia de Los Ríos haya puesto en consideración el desarrollo de una auditoría informática ya que es de vital importancia para el buen desempeño de los sistemas de información proporcionando controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.Conociendo que el principal objetivo de una auditoría informática es emitir una opinión sobre los procesos claves de control que se manejan dentro de la organización podremos manifestar que nuestro propósito es hacer el correcto uso de ésta opinión, la misma que nos permitirá otorgar al Gobierno Provincial de Los Ríos un Plan de Continuidad de Negocios diseñado para crear situaciones de preparación que proporcionen una respuesta inmediata en función de una serie de incidentes o escenarios previamente definidos.

4.2 OBJETIVOS DE LA PROPUESTA

4.2.1 OBJETIVO GENERAL

Garantizar la continuidad de negocios en el Gobierno Autónomo Descentralizado de la Provincia de Los Ríos, mediante el desarrollo de una Auditoría Informática que arroje resultados necesarios para crear un Plan de Continuidad de Negocios y Contingencia, planteado para dar soluciones a las necesidades e incidentes que podrían suscitarse en dicha organización.

4.2.2 OBJETIVOS ESPECÍFICOS

- Desarrollar una Auditoría basada en las necesidades analizadas previamente en el GPLR.
- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones de la organización.
- Proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier interrupción, evitando confusión y reduciendo situaciones de tensión.
- Comprobar el control interno de la entidad verificando sus puntos fuertes y débiles.
- Verificar el cumplimiento de normas, políticas y procedimientos que rigen las tecnologías de la información.
- Comprobar una seguridad razonable de los recursos cumpliendo con los objetivos de control y generales de la empresa.
- Evaluar si la información que se procesa es oportuna y confiable.
- Presentar un informe para dar a conocer los resultados y recomendaciones.
- Verificar la aceptación del Gobierno Provincial de Los Ríos para con los resultados que han proporcionado la investigación ejecutada.

4.3 METODOLOGÍA DE DESARROLLO UTILIZADA

La metodología para el desarrollo e implantación de la Auditoría Informática es verdaderamente importante ya que brinda un camino estructurado que permite llevar a cabo tareas, actividades, revisiones, funciones, etc., es conveniente recalcar que la metodología requiere además de un buen dominio de: Técnicas, Herramientas de Productividad, Conocimientos Técnicos y Administrativos, Experiencia en campos de Auditoría e Informática, etc.

La Metodología de Desarrollo que utilizaremos está basada en el análisis de necesidades en un entorno distribuido empleando técnicas y herramientas como Cuestionarios, Entrevistas, Checklist, etc., de los cuales se destaca el análisis de datos, ya que para la organización el conjunto de datos o información es de vital importancia para su verificación y comprobación, lo que nos permitirá obtener el producto final conocido como “Informe Final”, donde se verán plasmadas todas las recomendaciones con el objetivo de que las funciones realizadas en el Gobierno Autónomo Descentralizado Provincial de Los Ríos se realicen de una manera más eficiente y eficaz, y al mismo tiempo disminuya el riesgo de interrupción de las mismas o conocer cómo controlar y solucionar la situación en caso de que ésta exista.

4.4 ANÁLISIS PREVIO

Para hacer una adecuada planeación de la auditoría informática hemos llevado a cabo un análisis previo de los requerimientos del cliente tales como Continuidad de negocios para:

- Sistema Contable
- Servidor de Internet
- Página Web
- Firewall
- Servidor de Archivos
- Servidor de Correo Electrónico

Considerando los requerimientos establecidos anteriormente, nuestro análisisindicaque para satisfacer éstas necesidades debemos cumplir varias normas de auditoría.

Las normas de auditoría son requerimientos de calidad relativos a la personalidad del trabajo, al trabajo que desempeña y a la información que rinde como resultado de dicho trabajo, los cuales se derivan de la naturaleza profesional de la actividad de auditoría y de sus características especificas.

Las NAGAS, tiene su origen en los Boletines (StatementonAuditing Estándar – SAS) emitidos por el Comité de Auditoría del Instituto Americano de Contadores Públicos de los Estados Unidos de Norteamérica en el año 1948

- NORMAS GENERALES O PERSONALES
    - Entrenamiento y Capacidad Profesional: La Auditoría debe ser efectuada por personal que tiene el entrenamiento técnico y pericia como Auditor.
    - Independencia: En todos los asuntos relacionados con la Auditoría, el auditor debe mantener independencia de criterio.
    - Cuidado y Esmero Profesional.: Debe ejercerse el esmero profesional en la ejecución de la Auditoría y en la preparación del dictamen.

- NORMAS DE EJECUCIÓN DEL TRABAJO.
    - Planeamiento y Supervisión: La Auditoría debe ser planificada apropiadamente y el trabajo de los asistentes del auditor, si los hay, debe ser debidamente supervisado.
    - Estudio y Evaluación del Control Interno: El auditor debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirvan de base para determinar el grado de confianza que va depositar en el.
    - Evidencia Suficiente y Competente: el auditor debe obtener evidencia comprobatoria suficiente y competente en el grado que requiera suministrar una base objetiva para su opinión.

- NORMAS DE PREPARACIÓN DEL INFORME

Estas normas regulan la última fase del proceso de Auditoría, es decir la elaboración del informe, para lo cual, el auditor habrá acumulado en grado suficiente las evidencias, debidamente respaldada en sus papeles de trabajo.

- Aplicación de los Principios de Contabilidad Generalmente Aceptados:

  El dictamen debe expresar si los estados financieros están presentados de acuerdo a principios de contabilidad generalmente aceptados.

- Consistencia:

  Los usos de la información contable requieren que se sigan procedimientos de cuantificación que permanezcan en el tiempo.
  Este principio se refiere tanto a la consistencia en la aplicación de criterios contables de valuación de partidas y demás criterios (capitalización o no capitalización de desembolsos relacionados con activos fijos; tratamiento contable de los planes de pensiones a persona, tratamiento de mejoras de arrendamientos, etc.)

Como a la consistencia en cuanto a la clasificación de partidas dentro de los estados financieros.

Razones financieras equivocadas se obtendrán si en un ejercicio una partida se clasifica como crédito diferido y en otro se clasifica como cuenta de complementaria de activo (caso de Intereses por Realizar en ventas y en Abonos).

- Revelación Suficiente:

  Establece que todo estado financiero debe tener la información necesaria y presentada en forma comprensible de tal manera que se pueda conocer claramente la situación financiera y los resultados de sus operaciones.

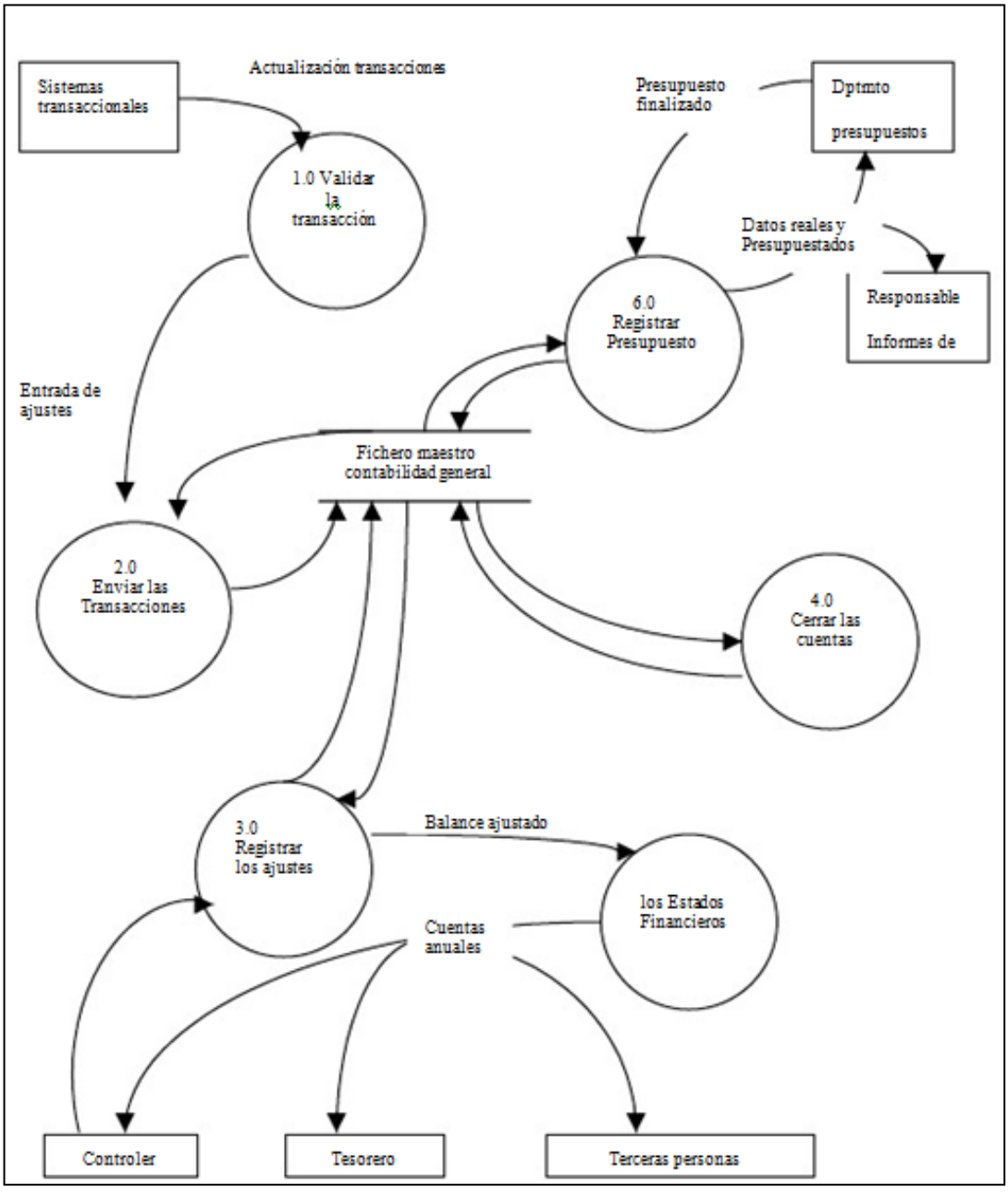
  Por esta razón la revelación puede darse a través de las cifras de los estados financieros o en las notas correspondientes.

- Opinión del Auditor:
  - Opinión Limpia o Sin Salvedades.
  - Opinión con Salvedades o Calificada.
  - Opinión Adversa o Negativa.
  - Abstención de Opinar.

4.5 DISEÑO

4.5.1 DIAGRAMAS NARRATIVOS

4.5.1.1 DIAGRAMA DE SISTEMA COTABLE

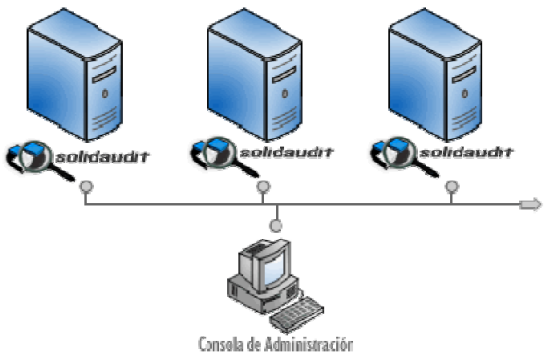


4.5.1.1 Esquema 8. Diseño del diagrama de Sistema Contable

4.5.1.2 DIAGRAMA DEL SERVIDOR DE INTERNET

A continuación se muestran algunos diagramas representativos de las funcionalidades o diferentes métodos de utilización:

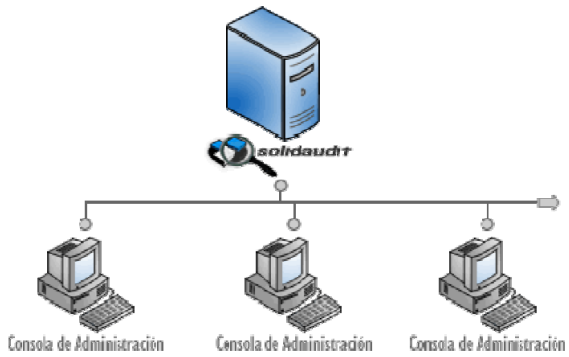
- **Múltiples Servidores Administrados Desde Una Misma Consola**



4.5.1.2 Esquema 9. Diseño del diagrama de Servidor de Internet

La consola de administración permite auditar múltiples servidores en forma simultánea desde una misma consola.

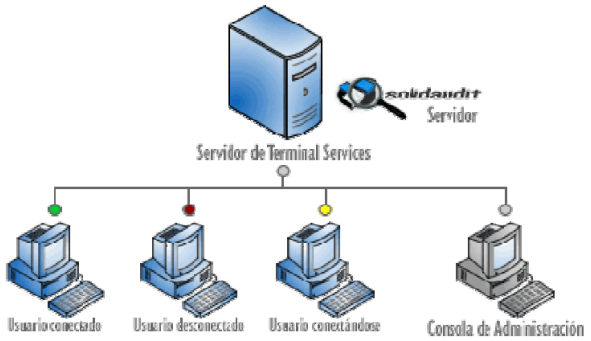
- **Múltiples Consolas De Administración Conectadas A Un Mismo Servidor**



4.5.1.2 Esquema 10. Diseño del diagrama de Servidor de Internet

El servidor permite múltiples conexiones de consolas en forma simultánea.

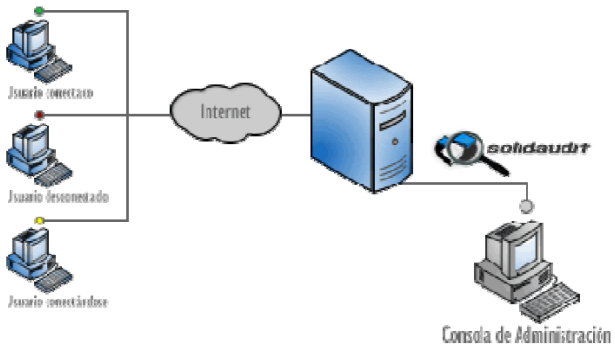
- **Monitoreo de conexiones**



4.5.1.2 Esquema 11. Diseño del diagrama de Servidor de Internet

El sistema monitorea las conexiones en tiempo real de las terminales que se conectan al servidor de Terminal Services.

- **Monitoreo de conexiones a través de Internet o VPN**



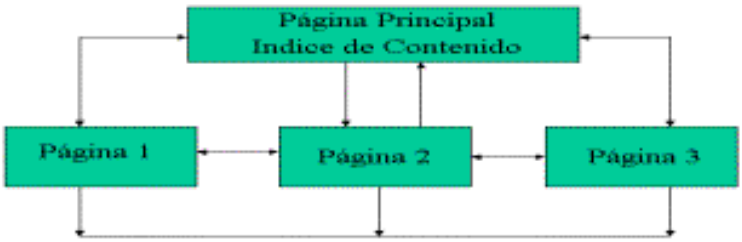
4.5.1.2 Esquema 12. Diseño del diagrama de Servidor de Internet

Además de monitorear las conexiones en tiempo real de las terminales en una red local, el sistema registra aquellas conexiones que se realizan a través de una VPN o de Internet registrando la dirección de IP real del cliente.

4.5.1.3 DIAGRAMA DE PÁGINA WEB

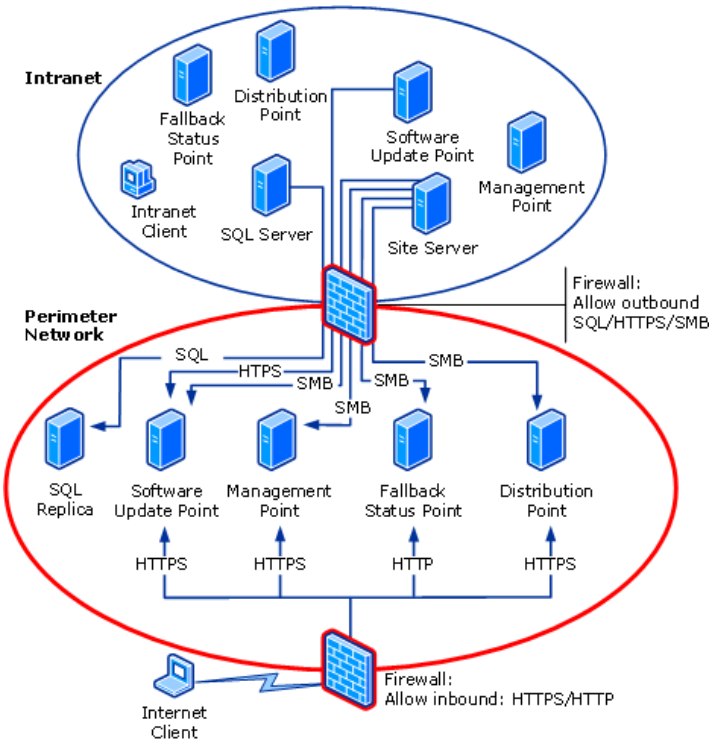
A continuación debes planificar cómo van a desplazarse los usuarios por ellas. Se debe realizar un diagrama de flujo claro para definir los índices principales, las páginas secundarias y las ramificaciones de todos los documentos.

Si utilizas una sola página WEB y esta es muy extensa deberá poner enlaces a las diferentes partes del documento al principio y al final de tu página y de esta forma facilitar la lectura de la misma, sin tener que depender tanto de las barras de desplazamiento.



4.5.1.3 Esquema 13. Diseño del diagrama de Página Web

4.5.1.4 DIAGRAMA DE FIREWALL

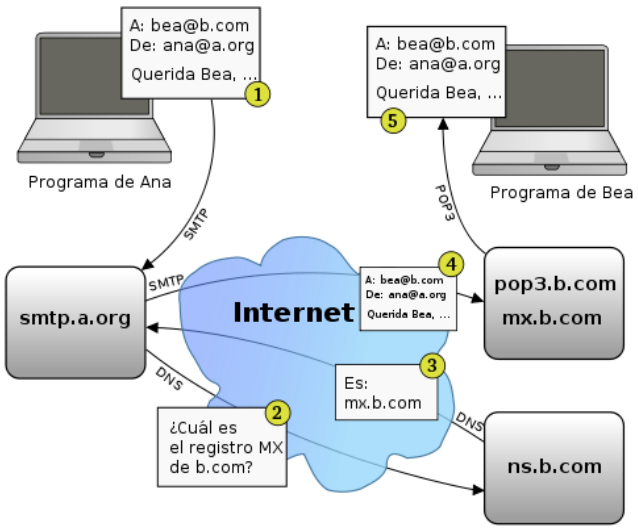


4.5.1.4 Esquema 14. Diseño del diagrama de Firewall

4.5.1.5 DIAGRAMA DEL SERVIDOR DE ARCHIVOS

4.5.1.5 Esquema 15. Diseño del diagrama de Servidor de Archivos

4.5.1.6 DIAGRAMA DEL SERVIDOR DE CORREO ELECTRÓNICO



4.5.1.6 Esquema 16. Diseño del diagrama de email server

Cada persona está en un servidor distinto (una en a.org, otra en b.com), pero éstos se pondrán en contacto para transferir el mensaje. Por pasos:

1. *Ana* escribe el correo en su programa cliente de correo electrónico. Al darle a *Enviar*, el programa contacta con el servidor de correo usado por *Ana* (en este caso, smtp.a.org). Se comunica usando un lenguaje conocido como protocolo SMTP. Le transfiere el correo, y le da la orden de enviarlo.
2. El servidor SMTP ve que ha de entregar un correo a alguien del dominio b.com, pero no sabe con qué ordenador tiene que contactar. Por eso consulta a su servidor DNS (usando el protocolo DNS), y le pregunta quién es el encargado de gestionar el correo del dominio b.com. Técnicamente, le está preguntando el registro MX asociado a ese dominio.
3. Como respuesta a esta petición, el servidor DNS contesta con el nombre de dominio del servidor de correo de *Bea*. En este caso es mx.b.com; es un ordenador gestionado por el proveedor de Internet de *Bea*.
4. El servidor SMTP (smtp.a.org) ya puede contactar con mx.b.com y transferirle el mensaje, que quedará guardado en este ordenador. Se usa otra vez el protocolo SMTP.
5. Más adelante (quizás días después), *Bea* aprieta el botón "*Recibir nuevo correo*" en su programa cliente de correo. Esto empieza una conexión, mediante el protocolo POP3 o IMAP, al ordenador que está guardando los correos nuevos que le han llegado. Este ordenador (pop3.b.com) es el mismo que el del paso anterior (mx.b.com), ya que se encarga tanto de recibir correos del exterior como de entregárselos a sus usuarios. En el esquema, *Bea* recibe el mensaje de *Ana* mediante el protocolo POP3.

Ésta es la secuencia básica, pero pueden darse varios casos especiales:

- Si ambas personas están en la misma red (una Intranet de una empresa, por ejemplo), entonces no se pasa por Internet. También es posible que el servidor de correo de *Ana* y el de *Bea* sean el mismo ordenador.

- *Ana* podría tener instalado un servidor SMTP en su ordenador, de forma que el paso 1 se haría en su mismo ordenador. De la misma forma, *Bea* podría tener su servidor de correo en el propio ordenador.
- Una persona puede no usar un programa de correo electrónico, sino un webmail. El proceso es casi el mismo, pero se usan conexiones HTTP al webmail de cada usuario en vez de usar SMTP o IMAP/POP3.
- Normalmente existe más de un servidor de correo (MX) disponible, para que aunque uno falle, se siga pudiendo recibir correo.

Si el usuario quiere puede almacenar los mensajes que envía, bien de forma automática (con la opción correspondiente), bien sólo para los mensajes que así lo desee. Estos mensajes quedan guardados en la carpeta "Enviados".

4.6 Plan de continuidad de negocio para el Gobierno Autónomo Descentralizado de la Provincia de Los Ríos

El Plan de Continuidad de Negocio no es más que un conjunto de estrategias, procedimientos preventivos y reactivos que permiten un rápido retorno a una situación normalizada, dicho conjunto de estrategias y procedimientos son creados para que la actividad de la institución se recupere en un nivel aceptable después de una interrupción no prevista de sus sistemas de información, y de la situación normal de funcionamiento.

La información es uno de los activos más importantes para las organizaciones, donde los sistemas de información y disponibilidad de estos juegan un rol preponderante para la continuidad de un negocio, por lo cual las organizaciones desarrollan e implementan lo que se conoce como Plan de Continuidad de Negocio el objetivo de mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia. Esto implica que un Plan de Continuidad de Negocio debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio.

Un Plan de Continuidad de Negocio tiene como objetivo el mantenimiento de estos servicios y procesos críticos, así como la reducción de impactos ante imprevistos de indisponibilidad o desastres para en un plazo razonable y con un coste acotado.

Tradicionalmente se venía considerando la seguridad informática como un área donde bastaba con dar una solución tecnológica a los problemas y necesidades que planteaba. Sin embargo, cada vez más somos todos conscientes de que cuando hablamos, no ya de seguridad informática sino de seguridad de la información, nos referimos a cuestiones relativas a organización y control interno.

En definitiva, estamos hablando de la buena administración de la empresa que permita la continuidad y la supervivencia del negocio. Elemento clave de esta concepción de la seguridad de la información es el plan de continuidad de negocio.

La gestión de la continuidad de negocio es: “La acción de prever aquellos incidentes que afectan a funciones o procesos críticos para la organización y que asegura que la respuesta a todos ellos se ejecuta de una manera organizada y consecuente.”

El principal objetivo del plan es proporcionar mecanismos que provean a una entidad de capacidad de reacción ante posibles interrupciones de sus servicios para proteger los procesos considerados críticos ante la ocurrencia de fallos o desastres. A grandes rasgos, un plan de continuidad del negocio debe llevarse a cabo siguiendo una serie de fases, unas de ellas se deben repetir en el tiempo de forma cíclica, otras se deben llevar a cabo de forma continua.

El objetivo de esa redundancia es garantizar que el plan se mantenga vigente en el tiempo, esté adecuadamente actualizado y que sea útil a la entidad en caso de fallos relevantes o desastres.

En el entorno empresarial actual, los sistemas de información son cada vez más críticos, lo que convierte en imprescindible que exista una continuidad en la operación de estos sistemas para el mantenimiento de sus tareas y negocios.

Los sistemas de información son los que sustentan los procesos de negocio de las organizaciones. Por este motivo es necesario que cuenten con un nivel de continuidad que permita a la organización ejecutar sus procesos de negocio sin ningún tipo de pérdida.

4.7 Objetivos

4.7.1 Objetivo General

- Desarrollar una estrategia que le permita continuidad de operaciones al Gobierno Autónomo Descentralizado de la Provincia de Los Ríos.

4.7.2 Objetivos Específicos

- Proveer un panorama general acerca de la implementación de un Plan de Continuidad de Negocios y Contingencia.
- Describir los puntos críticos para la implementación de un proyecto de este tipo.
- Proveer de ideas y beneficios por el uso de la metodología para el análisis y la selección de diferentes alternativas de seguridad con las que cuenta el Gobierno Autónomo Descentralizado Provincial de Los Ríos.

4.8 Descripción de Componentes del Plan

Un plan de continuidad del negocio es el conjunto de procedimientos formales que posee una compañía para enfrentar una situación de contingencia que inhabilita o impide la entrega de servicios a sus clientes, permitiéndole recuperar los elementos críticos de operación y servicio, para disminuir el impacto económico y de imagen generado.

Este plan está compuesto por los siguientes elementos:

- Procedimientos detallados de operación.
- Procedimientos detallados de recuperación de infraestructura (hardware y software).
- Procedimientos detallados de recuperación de datos.
- Recuperación de sitios de trabajo.
- Definición de equipos de recuperación.
- Estructura de escalamiento.
- Planes de comunicación (internos y externos).
- Plan de mantenimiento y pruebas de los elementos antes mencionados.

4.9 ANÁLISIS SITUACIONAL

4.9.1 DESCRIPCIÓN DE LA EMPRESA

4.9.1.1 GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE LOS RÍOS

Los Gobiernos autónomos descentralizados gozan de autonomía política, administrativa y financiera y se rigen por los principios de solidaridad, subsidiaridad, equidad territorial, integración y participación ciudadana.

Conforme a la Constitución Política de la República del Ecuador, los Gobiernos seccionales autónomos son ejercidos por los Gobiernos Provinciales, los Gobiernos Municipales, las Juntas Parroquiales y los organismos que

determine la ley para la administración de las circunscripciones territoriales indígenas y afro ecuatorianas.

El GPLR es una organización dedicada a formular y ejecutar planes, programas y proyectos, que garanticen el desarrollo social, económico y productivo de la Provincia y el País.

Para el cumplimiento de éstas actividades, se requiere regular el funcionamiento de sus diferentes dependencias, definiendo, delimitando y jerarquizando la naturaleza y ámbito de las funciones, deberes y derechos de cada una de las unidades administrativas de la Institución.

4.9.1.2 MISIÓN, VISIÓN, OBJETIVOS ESTRATÉGICOS Y VALORES DEL GOBIERNO PROVINCIAL DE LOS RÍOS

4.9.1.2.1 MISIÓN DEL GPLR

Mejorar la calidad y el nivel de vida de la población riosense, mediante la implementación de programas y proyectos con participación directa y efectiva de los actores sociales, en un marco de planificación, transparencia, respeto al medio ambiente, preservando su identidad cultural y con un capital humano altamente competitivo.

4.9.1.2.2 VISIÓN DEL GPLR

El Gobierno Provincial de Los Ríos en los próximos cuatros años, se constituirá en un ejemplo de desarrollo de la región y contará con una organización interna altamente eficiente, que garantice productos y servicios compatibles con la demanda ciudadana, y con capacidad de asumir los nuevos roles establecidos en la Constitución, asegurando el desarrollo y la calidad de vida de la población.

4.9.1.2.3 OBJETIVOS ESTRATÉGICOS DEL GPLR

1. Hacer del Gobierno Provincial una entidad planificadora y transparente, involucrada con la ciudadanía para mejorar sus condiciones y calidad de vida;
2. Dotar a la Provincia de la infraestructura vial, con los más altos estándares de calidad contribuyendo al desarrollo económico sustentable, la conectividad y la integración provincial;
3. Dotar a la Provincia de la infraestructura de riego, necesaria para su desarrollo agrícola;
4. Fomentar las actividades productivas con calidad y eficiencia, facilitando el acceso al crédito y proveyéndola de asistencia técnica y tecnológica.
5. Implementar políticas de ordenamiento territorial potenciando y generando nuevos polos de desarrollo.
6. Implementar políticas de gestión ambiental y de riesgos, para hacer de Los Ríos un territorio seguro.
7. Buscar la cooperación nacional e internacional en todas las áreas de intervención del Gobierno Provincial.

4.9.1.2.4 VALORES DEL GPLR

Los valores del GPLR se presentan a continuación:

Se pretende ser una empresa innovadora, que goce del orgullo de sus empleados y merezca la confianza permanente de quienes la integran.

Estos procesos son los responsables directos de la ejecución de los objetivos, políticas y planes propuestos por el Gobierno Provincial para cumplir sus competencias y está integrado por:

1. DIRECCIÓN DE PLANIFICACIÓN, con las unidades de: Gestión del Territorio, Gestión de Proyectos y Gestión Ambiental y Riesgos.

2. DIRECCIÓN DEL DESARROLLO DE LA INFRAESTRUCTURA, conformada por las unidades de: Estudios Técnicos; Construcciones, Conservación, Fiscalización.

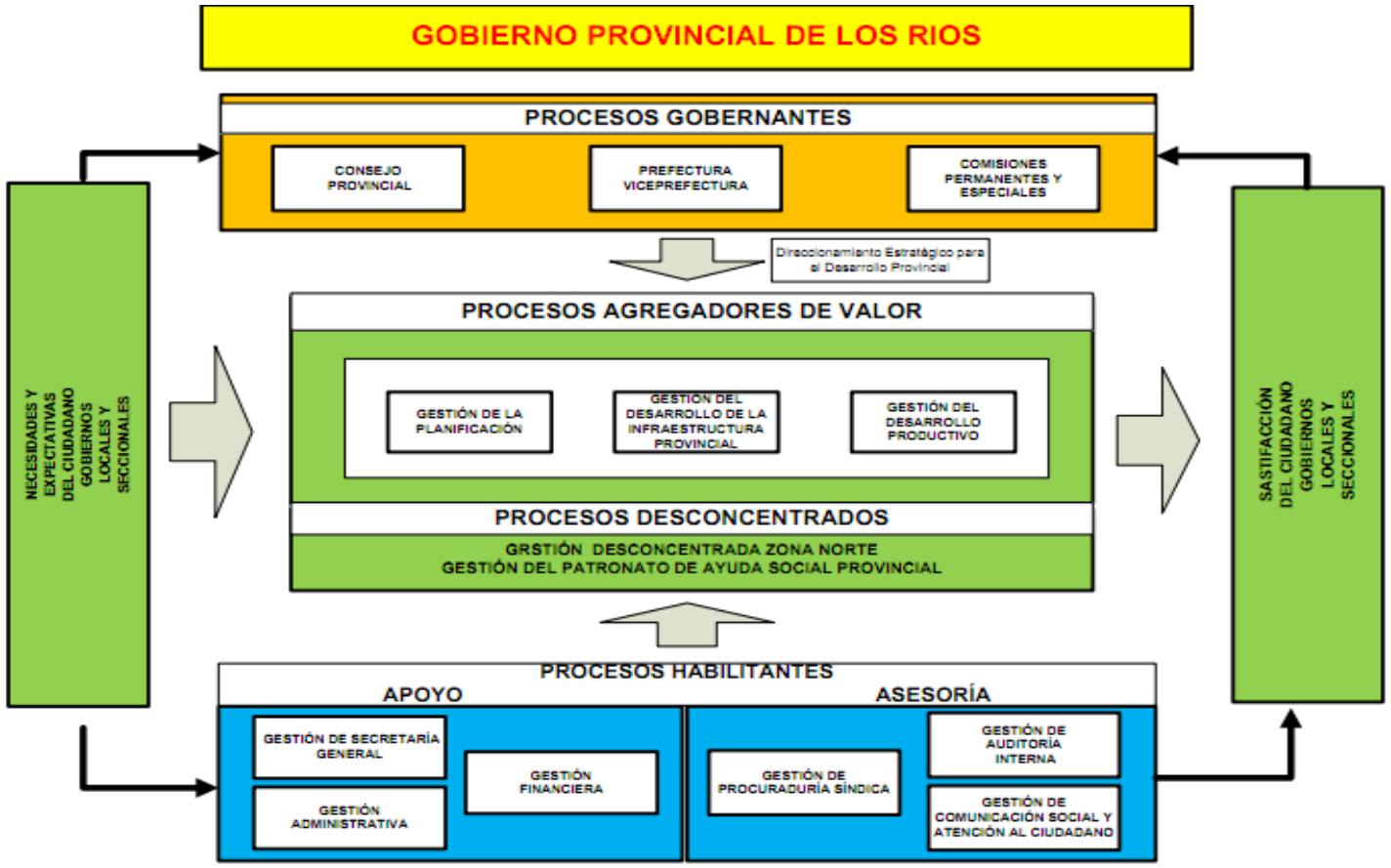
3. DIRECCIÓN DE DESARROLLO PRODUCTIVO, con las unidades de Fomento Productivo Promoción e Inversión y Desarrollo Productivo.

4.9.2 PRESENCIA DEL GOBIERNO PROVINCIAL DE LOS RÍOS EN ECUADOR

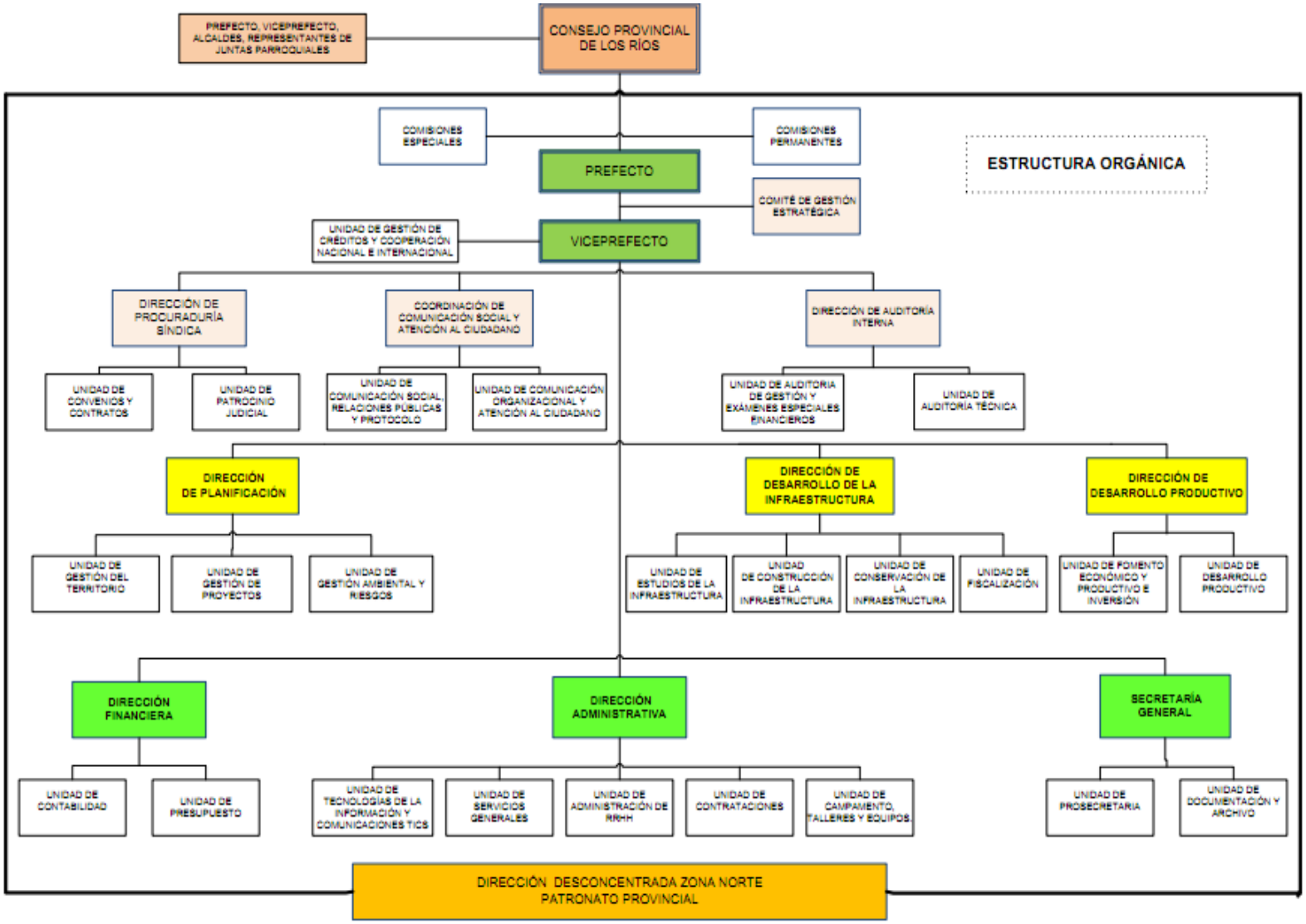
El Gobierno Autónomo Descentralizado Provincial de Los Ríos se localiza en la ciudad de Babahoyo en Av. Universitaria y Primera Transversal - Babahoyo – Ecuador.

Cuenta en la actualidad con la colaboración de aproximadamente 582 empleados quienes en su mayoría residen en la ciudad.

4.9.3 ESTRUCTURA ORGANIZACIONAL DEL GPLR



4.9.3 Esquema 17. Estructura Organizacional del Gobierno Descentralizado de la Provincia de Los Ríos



4.9.3 Esquema 18. Estructura Organizacional del Gobierno Descentralizado de la Provincia de Los Ríos

4.10 ANÁLISIS FODA

4.10.1 ANÁLISIS FODA DEL DEPARTAMENTO DE TIC's

Tomando en cuenta el alcance del presente proyecto de titulación se enfoca al análisis FODA única y exclusivamente al Departamento de TIC's del Gobierno Provincial de Los Ríos.

El análisis FODA del Departamento de TIC's ha sido elaborado con la colaboración de los miembros del Departamento de TIC's y se detalla de la siguiente manera:

Fortalezas

- Se cuenta con personal calificado para administrar tanto los equipos como las aplicaciones requeridas por la empresa.
- Los miembros del Departamento de TIC's tienen buena aceptación y percepción por parte de los usuarios.
- Se siguen estándares para los procedimientos que se realizan dentro del departamento de TIC's.
- Los miembros del Departamento de TIC's tienen acceso a capacitaciones constantes.
- Se tiene apertura para adoptar nuevas tecnologías de forma rápida.

Oportunidades

- El Departamento de TIC's del GPLR es partícipe de todos los proyectos que se desarrollan a través de la organización.
- Tener acceso a tecnología de punta por los convenios que se tiene con diferentes empresas proveedoras de hardware y software.
- Tener acceso a capacitación de nuevas tecnologías con el fin de dar mejores soluciones al Departamento de TIC's.

Debilidades

- Poca Capacitación
- Transportación
- Bajo compromiso y entendimiento por parte de los directivos (Las TIC's ayudan a fortalecer institucionalmente)

Amenazas

- Naturales y Ambientales
    - Fuego
    - Tormenta eléctrica
    - Terremoto
    - Inundación
    - Sequía
    - Volcán
    - Tsunami
- Humanas
    - Accidentales
        - Omisión
        - Error
    - Intencionales
        - Omisión
        - Error
        - Fuego
        - Robo
        - Sabotaje
        - Vandalismo
        - Huelga
        - Ciber-amenaza
    - De Infraestructura
        - Daño estructural
        - Comunicaciones
        - Sistemas de seguridad
        - Potencia eléctrica
        - Calefacción/aire

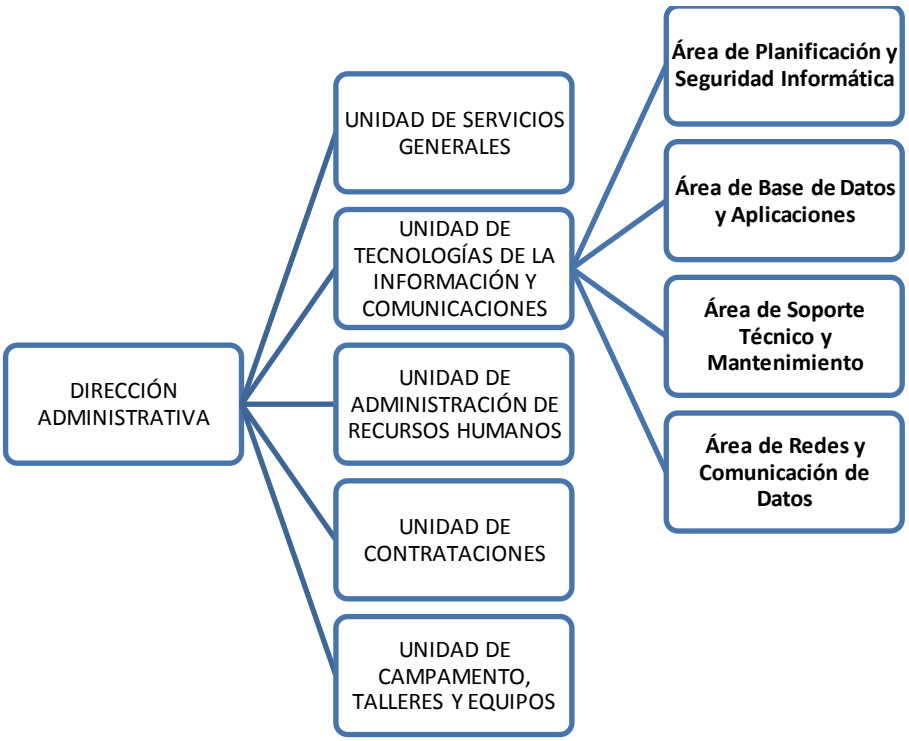
4.11 PROCESOS Y FUNCIONES DEL DEPARTAMENTO DE TIC's EN LA ORGANIZACIÓN

4.11.1 EL DEPARTAMENTO DE TIC's EN LA ORGANIZACIÓN

La Unidad De Tecnología De Información Y Comunicaciones se encuentra integrada por un conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc.), software (sistemas operativos de Windows 7, bases de datos, herramientas de administración, etc.) y servicios (soporte técnico, seguros, comunicaciones, etc.) que en conjunto dan soporte a los sistemas informáticos del Gobierno Provincial de Los Ríos.

Esta unidad está destinada a mantener el funcionamiento óptimo de la infraestructura tecnológica institucional, haciendo eficientes las tareas de procesamiento de datos y de información.

4.11.2 ESQUEMA ORGANIZACIONAL DEL DEPARTAMENTO DE TIC's



4.11.2 Esquema 19. Departamento de TIC´s del GPLR

4.11.3 AREAS ADMINISTRATIVAS DEL DEPARTAMENTO DE TIC's

El Departamento de TI en EL GPLR se divide en cuatro áreas importantes para desarrollar sus actividades:

- Área de Planificación y Seguridad Informática
- Área de Base de Datos y Aplicaciones
- Área de Soporte Técnico y Mantenimiento
- Área de Redes y Comunicación de Datos

4.11.4 DESCRIPCIÓN DE LOS SERVICIOS QUE SOPORTA EL DEPARTAMENTO DE TIC's

Esta unidad está destinada a mantener el funcionamiento óptimo de la infraestructura tecnológica institucional, haciendo eficientes las tareas de procesamiento de datos y de información. Los servicios que soporta el Departamento de TIC's a través de sus áreas administrativas se detallará en el mapeo de servicios que se muestra en el (punto 3.3.5 - tabla #).

4.11.5 MAPEO DE SERVICIOS QUE SOPORTA EL DEPARTAMENTO DE TIC's A LAS ÁREAS DEL NEGOCIO

AREA	PRODUCTOS Y SERVICIOS
Área de Planificación y Seguridad Informática	Plan Estratégico de la Unidad implementado y socializado.
	Plan Operativo Anual del área.
	Informes semestrales de evaluación del Plan Operativo Anual.
	Poner en práctica normas para la seguridad de la información (ISO-27001).
	Procedimientos técnicos y metodologías sobre seguridad en aplicaciones y sistemas informáticos.
	Plan de Capacitación Informática e informe de evaluación trimestral de Capacitación Informática.
	Propuestas de políticas de gestión tecnológica.

	Informes de implementación, administración y mantenimiento de aplicaciones y sistemas informáticos.
	Términos de referencia y especificaciones técnicas.
	Proyectos para la adquisición de software propietario y software libre.
	Informes de soporte informático y capacitación en aplicaciones y sistemas de información.
	Procedimientos para accesos a recursos de información.
	Informe de seguridad y confidencialidad de identificaciones de usuario y contraseña.
	Informes de monitoreo de violaciones de seguridad.
	Informes periódicos de políticas de seguridad.
	Informe de cumplimiento de procesos establecidos.
	Informes de pruebas o revisiones de software.
	Políticas de Seguridad de la información y comunicación.
	Informes de aseguramiento y calidad de software.
	Test de penetración al sistema operativo.
	Test de penetración de redes y comunicaciones.
	Afinamiento a los sistemas operativos.
	Informe de implementación de antivirus.
	Gestión de la seguridad de los sistemas y de la continuidad empresarial.
	Encriptación de datos.
	Análisis de la integridad y fiabilidad de la información.
	Gestión de Backup Periódicos de la Información y Datos de la organización
	Informes de administración de licencias de programas informáticos comerciales (software).

	Propuestas de gestión e implementación de mejoras e innovaciones en los procesos, procedimientos y normatividad relacionado con la unidad. (pasa a auditoria).
Área de Base de Datos y Aplicaciones	Informe de cambio de la información física de datos.
	Implementación de herramientas de optimización de datos y acceso a la información.
	Implementación de controles de definición, acceso, actualización y concurrencia de datos.
	Informes de monitoreo de las bases de datos.
	Informes de Auditoría de base de datos en coordinación con la sub unidad de planificación y Seguridad Informática.
	Informes de actualización de la estructura de base de datos.
	Gestión de la migración de datos a otras plataformas operativas y/o servidores.
	Registro de la generación de respaldos.
	Informes de verificación de la integridad de datos.
	Controles de acceso a los datos definidos e implementados.
	Planes de capacitación a programadores e ingenieros para utilizar eficientemente la base de datos.
	Informes de actividades y proyectos de desarrollo de sistemas de información en función de cumplir el Plan Operativo Informático (POI).
	Informes de ejecución de proyectos de desarrollo de sistemas informáticos aplicando estándares de desarrollo establecidos.
	Plan Anual de Mantenimiento de Sistemas de información.
	Informe de ejecución de actividades de mantenimiento de sistemas informáticos.
	Especificaciones técnicas de los servicios de desarrollos informáticos y aplicativos.
	Informe de evaluación y monitoreo de la ejecución de proyectos de desarrollo de sistemas informáticos realizados por terceros.

	Informes de asistencia técnica sobre soluciones tecnológicas puestas a consideración por terceros.
	Propuestas de tecnologías de información en los procesos del Gobierno Provincial como resultado de investigaciones de carácter tecnológico.
	Informes de administración técnica de los sistemas informáticos y los manuales de usuarios de cada sistema informático del Gobierno Provincial.
	Informes de los proyectos de desarrollo informático ejecutados y en ejecución.
	Informes de asesoría a las unidades orgánicas en la identificación de soluciones que involucren el desarrollo o aplicación de sistemas informáticos.
	Portal Web del Gobierno Provincial actualizado y administrado eficientemente.
Área de Soporte Técnico y Mantenimiento	Inventario de equipos de cómputo (hardware).
	Realizar mantenimiento preventivo y correctivo del hardware de la institución (impresoras, computadoras y otros equipos de tecnología informática).
	Asistencia técnica presencial y telefónica a los usuarios de recursos de información del Gobierno Provincial de Los Ríos.
	Charlas técnicas de uso de aplicaciones puntuales.
	Capacitación a usuarios en utilización de nuevo hardware para su eficiente aprovechamiento.
	Informes de administración del servicio de asistencia al usuario (“Helpdesk”).
	Informes de mantenimiento preventivo y correctivo de los equipos de cómputo.
	Informes de administración de Activos Informáticos.
	Reporte de actualizaciones de sistemas operativos de los usuarios.
	Estadísticas de malware (virus, etc.).
	Registros de actualización de antivirus.
	Monitoreo de software no licenciado, en conjunto con la sub unidad de Planificación y Seguridad Informática.
	Informes de ejecución de proyectos de infraestructura tecnológica relacionados con redes y telecomunicaciones.

Área de Redes y Comunicación de Datos	Propuestas de aplicación de tecnologías de comunicaciones en los procesos del Gobierno Provincial, como resultados de investigaciones de carácter tecnológico.
	Especificaciones técnicas de procesos de selección referidos a servicios o proyectos de telecomunicaciones.
	Informes de supervisión de proyectos por terceros, relacionados con equipos de redes y comunicaciones.
	Registros de la red de datos (administración de usuarios, servidores y dispositivos de comunicaciones).
	Registros de la administración de accesos a la intranet e internet.
	Gestión del enlace de datos WAN entre diferentes unidades desconcentradas.
	Informes de administración de la red de telefonía.
	Políticas de seguridad informática en redes.
	Informes de ejecución de actividades orientadas al cumplimiento de la normatividad gubernamental en materia de telecomunicaciones y protección de la propiedad intelectual.
	Administración del Correo Electrónico Institucional.

4.11.6 LISTADO DE PROCESOS QUE DESARROLLA EL DEPARTAMENTO DE TIC's

- Administrar las operaciones del centro de cómputo, redes locales y departamentales de la institución;
- Desarrollar e Implementar Planes de Sistemas de Información y Tecnologías Informáticas, considerando capacitación y formación de usuarios ;
- Desarrollar manuales de procedimientos, metodologías y estándares informáticos para buenas prácticas de servicios;
- Proveer de servicios informáticos a las unidades del Gobierno Provincial;

- Desarrollar y mantener Software de base a medida y utilitarios para hacer eficiente el trabajo de las diferentes unidades de la institución y redes locales;

- Coordinar con la dirección de planificación en la elaboración de planes y proyectos de tecnología de información y comunicaciones TICs;
- Realizar estudios Periódicos para provisión de equipos, programas y servicios computacionales, según las necesidades de todas las unidades departamentales;
- Instalar, operar, controlar y mantener el hardware, software y redes de computo;
- Mantener el inventario físico actualizado de las configuraciones computacionales y de comunicación;
- Analizar el rendimiento óptimo de recursos consumibles de información (tintas, tóneres, cintas, etc.)
- Apoyar a la mejora continua de procesos para fortalecer la institución.

4.12 PLAN DE CONTINUIDAD Y CONTINGENCIA

4.12.1 PRIORIZACIÓN

En algún momento de toda planificación o metodología de mejora, es necesario decidir que es más importante hacer para la organización y cuando realizarlo, es decir establecer prioridades.
Nuestro proyecto se basa en la importancia vital que tiene un plan de continuidad y contingencia dentro de una organización para lo cual hemos tomado en consideración los diferentes componentes de dicho plan, los cuales se detallan a continuación:

- PROCEDIMIENTOS DETALLADOS DE OPERACIÓN: Información detallada que permite realizar la operación de las unidades de negocio en el sitio alterno.

- PROCEDIMIENTOS DETALLADOS DE RECUPERACIÓN DE INFRAESTRUCTURA (HARDWARE Y SOFTWARE): Información detallada que permite recuperar y poner a punto los elementos de infraestructura (HW y SW) de la organización en el sitio alterno.
- PROCEDIMIENTOS DETALLADOS DE RECUPERACIÓN DE DATOS: información detallada que permite recuperar los datos operativos, analíticos y de gestión para habilitar los sistemas de la organización en el sitio alterno.
- RECUPERACIÓN DE SITIOS DE TRABAJO: habilitación de sitios físicos de operación que permiten realizar las actividades operativas y de gestión necesarias para operar los servicios de la organización en el sitio alterno.
- DEFINICIÓN DE EQUIPOS DE RECUPERACIÓN: estructura organizativa responsable de llevar a cabo las actividades necesarias para habilitar los servicios de la compañía en el sitio alterno.
- ESTRUCTURA DE ESCALAMIENTO: estructura que soporta a la organización para la toma de decisiones en los momentos de contingencia.
- PLANES DE COMUNICACIÓN (INTERNOS Y EXTERNOS): estrategias de comunicación que permiten enviar mensajes relevantes a los diferentes stakeholders de la organización durante la operación del plan.
- PLAN DE MANTENIMIENTO Y PRUEBAS DE LOS ELEMENTOS ANTES MENCIONADOS: estrategia y actividades necesarias que permiten mantener actualizados y probados a los elementos antes mencionados.

Cabe indicar que se priorizaron los procedimientos tomando como criterio la importancia del proceso en la continuidad del negocio.

4.13 PLAN DE CONTINUIDAD DE NEGOCIOS Y CONTINGENCIA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE LOS RÍOS.

4.13.1 FASE 1: ANALISIS Y EVALUACIÓN DE RIESGOS

La fase de análisis y evaluación de riesgos consiste en la identificación y priorización de las amenazas que por su probabilidad e impacto afectasen a la continuidad de las operaciones y se revisará los controles establecidos y los próximos pasos a seguir.

4.13.1.1 Identificación de riesgos

El objetivo de esta fase es identificar y determinar las amenazas a las que está expuesto el proceso de abastecimiento de la empresa, para en un posterior análisis identificar cuáles son las amenazas que podrían afectar a la continuidad del mismo.

Para identificar los riesgos se consideró un listado estándar de amenazas, las cuales están divididas en categorías generales, en este listado se procede a seleccionar las amenazas que se ajusten a la realidad del Ecuador en especial de Babahoyo que es lugar de análisis.

Como método de identificación se procede a realizar entrevistas a los encargados del proceso con la experiencia sobre el tema, además se tomó en consideración los informes realizados por la auditoría.

Se unificó el listado de amenazas estándar con las de la organización, en el análisis se incluyó las amenazas de TIC's debido a que los sistemas se consideran parte importante del análisis.

4.13.1.2 Análisis y evaluación de riesgos

La finalidad de esta fase es dar prioridad a las amenazas identificadas con base en la probabilidad de ocurrencia de los mismos y el impacto en las operaciones de la empresa. Se escoge el análisis cualitativo por ser el que más se ajusta a la organización, debido a que no existe la información estadística necesaria para identificar la probabilidad de ocurrencia y el impacto.

Se tomaron medidas cualitativas de probabilidad e impacto y los resultados se muestran en las tablas 5 y 6 del análisis y evaluación de riesgos.

Probabilidad	Nivel	Descripción
Alta	5	Puede ocurrir en la mayoría de las circunstancias.
Media	3	Podría ocurrir en algún momento.
Baja	1	Puede ocurrir solo en circunstancias excepcionales.

4.13.1.2 Tabla 5 *Medidas cualitativas de Probabilidad BCP Abastecimiento de la Empresa*

Impacto	Nivel	Descripción
Alto	5	Proceso no controlado que ocasionaría pérdida de información, pérdida financiera alta o afecta en su totalidad la continuidad de la organización.
Medio	3	Proceso no controlado que puede ocasionar pérdida de información, pérdida financiera media o que afecta en parte a la continuidad de la organización.
Bajo	1	Proceso con un control ineficaz que no ocasionaría pérdida de información, pérdida financiera baja y no afecta en la continuidad dela organización.

4.13.1.2 Tabla 6. *Medidas cualitativas de Impacto BCP Abastecimiento dela Empresa*

Con el establecimiento de las medidas cualitativas de análisis se procederá a realizar los talleres con los encargados del departamento de TIC's para identificar el nivel de exposición al riesgo, de acuerdo a la experiencia que poseen, el resultado de los talleres realizados se los muestra en la tabla 7.

Cabe indicar que se evaluó la posibilidad real de ocurrencia existente para cada una de las amenazas identificadas desde la perspectiva de frecuencia e impacto sobre los activos, operaciones, personas y medio ambiente.

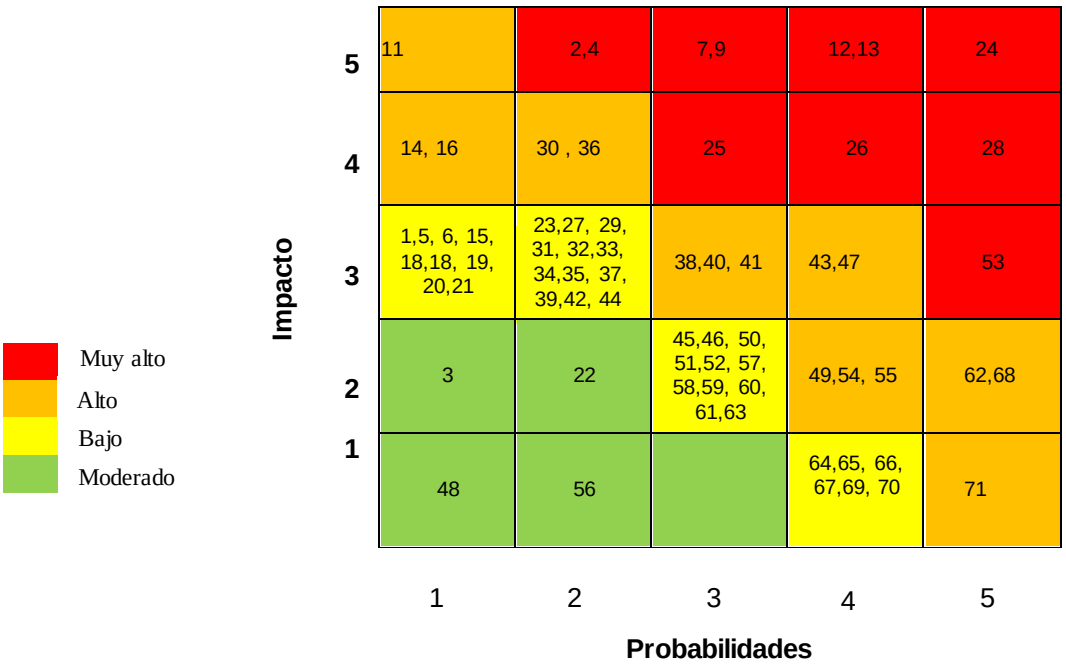
CÓDIGO	AMENAZAS Categorías	Probabilidad	Impacto	PxI	Exposición al riesgo
	Compras				
1	Especificaciones para compra no claros	3.00	2.00	6	
2	Falta de planificación para la compra de ítems	3.00	5.00	15	
3	No se revisa stocks ni presupuestos para comprar	1.00	2.00	2	
4	Demora en la compra local y de importación	3.00	4.00	12	
5	Conflicto de intereses	2.00	3.00	6	
6	Falta de experiencia de negociadores	1.00	3.00	3	
7	No realizar los contratos a tiempo	3.00	4.00	12	
8	Falta de personal para la negociación	3.00	3.00	9	
9	Falta de escalamiento y seguimiento en compras atrasadas	3.00	4.00	12	
10	Demora en pago a proveedores	2.00	4.00	8	
	Bodegas				
11	Artículos solicitados y no retirados de bodega por mucho tiempo	3.00	3.00	9	
12	Descoordinación entre las áreas para la recepción de mercaderías	3.00	4.00	12	
13	Espacio físico de bodegas limitado	3.00	4.00	12	
14	Horarios de atención en bodega no adecuados	2.00	4.00	8	
15	Movimientos de bodega sin ser regularizados en el Sistema	2.00	3.00	6	
16	Manejo inadecuado de ítems al momento de la recepción	2.00	4.00	8	
17	Recepción de ítems que no se encuentren especificaciones requeridas	1.00	3.00	3	
	Tecnológicos				
18	Falta de equipos informáticos	2.00	3.00	6	
19	Accesos no autorizados	2.00	3.00	6	
20	Contraseñas compartidas	2.00	3.00	6	
21	Corte de energía eléctrica	2.00	3.00	6	
22	Daño de escáner, fax, impresora	1.00	2.00	2	
23	Daños en equipos de computación	2.00	3.00	6	
24	Falla central telefónica	2.00	5.00	10	
25	Falla de Sistema	3.00	4.00	12	
26	Falla de correo	3.00	4.00	12	
27	Fallas o inexistencias de UPS y paso de energía	2.00	3.00	6	
28	Falta de respaldos de la información	2.00	5.00	10	
29	Información no confiable	1.00	3.00	3	
30	Robo de información de la empresa o mal uso de esta	1.00	4.00	4	
31	Virus y Gusanos Informáticos	2.00	3.00	6	
32	Filtraciones de agua a computadores y/o en centro de computo	1.00	3.00	3	
33	Claves genéricas	2.00	3.00	6	
34	Fallas en Hardware	2.00	3.00	6	
35	Fallas en Software	2.00	3.00	6	
36	Fallas en comunicaciones	2.00	4.00	8	
37	Falta de manuales precisos de operación y recuperación	2.00	3.00	6	
	Desastres Naturales				
38	Condiciones de clima muy inestables	2.00	4.00	8	
39	Derrumbe	2.00	3.00	6	
40	Erupción Volcánica	2.00	4.00	8	
41	Explosión	1.00	4.00	4	
42	Granizo	1.00	3.00	3	
43	Incendio	2.00	4.00	8	
44	Inundación	2.00	3.00	6	
45	Rayo	2.00	3.00	6	
46	Temblor	2.00	3.00	6	
47	Terremoto	2.00	4.00	8	

CÓDIGO	AMENAZAS Categorías	Probabilidad	Impacto	PxI	Exposición al riesgo
	Humanos				
48	Adicción al juego de apuestas, etc.	1.00	2.00	2	
49	Bomba	1.00	4.00	4	
50	Consumo de drogas, alcohol por parte del empleado	2.00	3.00	6	
51	Empleados con antecedentes y/o comportamiento violento	1.00	3.00	3	
52	Empleados con comportamiento doloso(fraude, soborno, corrupción)	2.00	3.00	6	
53	Huelga	2.00	5.00	10	
54	Robo	2.00	4.00	8	
55	Saqueo	1.00	4.00	4	
56	Apagado accidental de equipo	2.00	2.00	4	
57	Derrame de líquidos sobre equipos	2.00	3.00	6	
58	Errores de digitación	2.00	3.00	6	
59	Escritorios con información sensible	2.00	3.00	6	
60	Falla por fatiga del personal	2.00	3.00	6	
61	Pérdida de información	2.00	3.00	6	
62	Caza o robo de talentos	3.00	3.00	9	
63	Consecuencias legales por negligencia y accidentes	2.00	3.00	6	
64	No cumplimiento de procedimientos	2.00	3.00	6	
65	Faltad capacitación	2.00	3.00	6	
	Físicos				
66	Ausencia de identificación de salidas	2.00	3.00	6	
67	Falta de sitios para recurrir en caso de contingencia	2.00	3.00	6	
	Seguridad Física				
68	Asalto a los camiones (proveedores)	3.00	3.00	9	
69	Carga cambiada	1.00	3.00	3	
70	Falta de mantenimiento de vehículos	2.00	3.00	6	
71	Transporte de ítems inadecuado	3.00	3.00	9	

4.13.1.2 Tabla 7. *Amenazas desde la perspectiva de frecuencia e impacto sobre los activos, operaciones, personas y medio ambiente.*

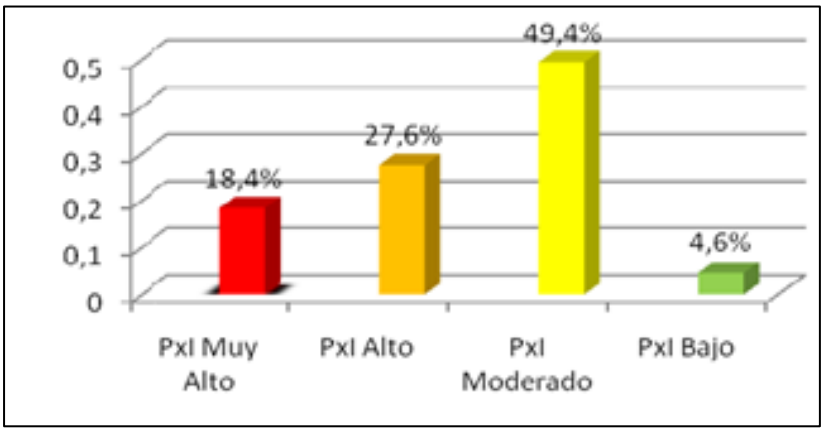
Luego de identificado el grado de exposición al riesgo con referencia a las amenazas, se procede a ubicar en la matriz, dichas amenazas de acuerdo al mayor puntaje obtenido en la probabilidad y el impacto, esto se visualiza en la figura 1.

4.13.1.2 Figura 1 *Matriz de riesgos- BCP Abastecimiento de la Empresa*



En la figura 2 se muestra el porcentaje de amenazas con una exposición al riesgo muy alto, alto, moderado y bajo.

4.13.1.2 Figura 2. Porcentaje de amenazas de acuerdo a la exposición al riesgo



Del análisis del gráfico se puede concluir que el 46% de las amenazas tienen una ponderación muy alta y alta, por lo cual, a estas amenazas se requerirá revisar los controles existentes y recomendar otros, como próximos pasos a seguir.

4.13.1.3 Identificación de controles

La finalidad de esta fase es de analizar las amenazas calificadas con mayor probabilidad e impacto y revisar los controles establecidos. En caso de no existir se debe identificar, con los encargados del proceso, los próximos pasos a seguir. Para tener una idea clara de los controles a continuación se muestran los conceptos:

Controles existentes

Describen las medidas de control existentes, son controles que se están aplicando o se haya aplicado para reducir la incidencia del riesgo.

Controles recomendados

Son los controles que deben ser implementados, estos son seleccionados con base en las mejores prácticas.

Para identificar los controles existentes y los próximos pasos se propone utilizar un formulario durante las entrevistas con los encargados y ejecutores del proceso.

Luego de realizar las entrevistas respectivas para revisar los controles existentes y los controles recomendados como próximos pasos para las amenazas con un PxI muy alto y alto, se procede a realizar el resumen que lo muestra la tabla 8

Establecimiento de controles

AMENAZAS Categorías	PxI	Exposición al riesgo	Controles existentes	Controles recomendados (Próximos Pasos)
Compras				
Falta de planificación para la compra de ítems	15		Autorización de compras fuera de planificación por parte de la Gerencia de área	Migrara un ERP que permita una mejor planificación con datos más reales
Demora en la compra local y de importación	12		Ajuste en el tiempo de los acuerdos de servicio entre compras y área usuaria	Revisión de los acuerdos deservicio por lo menos semestralmente

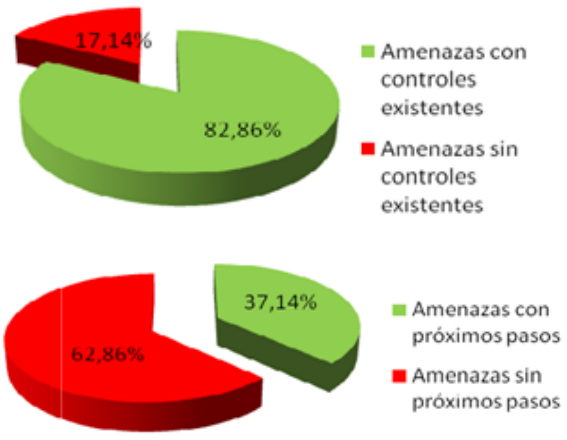
AMENAZAS Categorías	PxI	Exposición al riesgo	Controles existentes	Controles recomendados (Próximos Pasos)
No realizar los contratos a tiempo	12			Establecer un lead time entre legal y compras para la entrega de contratos
Falta de escalamiento y seguimiento en compras atrasadas	12		Se creó un aplicativo para que el usuario de seguimiento a su requerimiento	Reuniones con áreas para establecer prioridades
Falta de personal para la negociación	9		Indicadores de cumplimiento	Liberación de carga operativa mediante la automatización de algunos procesos
Demora en pago a proveedores	8			Establecer prioridades de pago
Bodegas				
Descoordinación entre las áreas para la recepción de mercaderías	12			Áreas involucradas deben revisar fecha de llegada de ítem
Espacio físico de bodegas limitado	12		Se está construyendo una bodega con mayor espacio para el almacenaje de materia prima	
Artículos solicitados y no retirados de bodega por mucho tiempo	9			Sacar reporte de artículos y establecer sanciones para usar lo que no hizo uso
Horarios de atención en bodega no adecuados	8		Para materia prima existe atención todo el día y los365díasdel año	
Manejo inadecuado de Ítems al momento de la recepción	8		Establecimiento de sanciones	
Tecnológicos				
Falla de Sistema	12		Se tiene un RTO de sistema en el DRP de Sistemas	
Falla de correo	12		Se tiene un RTO de correo en el DRP de Sistemas	
Falla central telefónica	10		Se tiene un RTO de central telefónica en el DRP de Sistemas	
Falta de respaldos de la información	10			Establecimiento de información Relevante para tener el Backup en cintas

AMENAZAS Categorías	PxI	Exposición al riesgo	Controles existentes	Controles recomendados(Próximos Pasos)
Fallas en comunicaciones	8		Los enlaces entre la empresa y el proveedor de comunicaciones es redundante	
Robo de información de la empresa o mal uso de esta	4		Usuarios solo tienen activados sus perfiles solo para lo estrictamente necesario	
Desastres Naturales				
Condiciones de clima muy inestables	8		Se tiene un programa de Manejo de Incidentes y resolución de crisis	
Erupción Volcánica	8		Se tiene un programa de Manejo de Incidentes y resolución de crisis	
Incendio	8		La empresa posee equipos para controlar incendios y brigadistas	
Terremoto	8		Se tiene un programa de Manejo de Incidentes y resolución de crisis	
Explosión	4		Se tiene un programa de Manejo de Incidentes y resolución de crisis	
Humanos				
Huelga	10		Está prohibido la formación de sindicatos, los sueldos en la empresa con respecto a la Industria son relativamente buenos	TTHH debe hacer un análisis de necesidades del personal
Caza o robo de talentos	9		Los sueldos en la empresa con respecto a la Industria son relativamente buenos	Tener incentivos por buen desempeño no necesariamente económicos
Saqueo	4		Se contrató una empresa de seguridad la cual tiene dispositivos de control de última tecnología	
Seguridad Física				
Asalto a los camiones (proveedores)	9		Los contratos con proveedores poseen cláusulas de protección	
Transporte de ítems inadecuado	9		En los contratos con proveedores se obliga a que se realice un mantenimiento periódico	

4.13.1.3 Tabla 7. Establecimiento de controles

La figura 3 muestra en que porcentaje las amenazas tienen establecidos controles y próximos pasos.

Figura 3 *Porcentaje de amenazas que tienen establecidos controles y próximos pasos*



En conclusión, se puede visualizar en la figura 3.5 que el porcentaje de amenazas consideradas que tienen un riesgo alto y que pueden afectarla continuidad del negocio están en el 44,3%, por lo cual se puede detectar la necesidad de un BCP para el Gobierno Provincial de Los Ríos.

El 55,7% de las amenazas están consideradas como de exposición al riesgo moderado a bajo por lo que es necesario que se realice constantes evaluaciones para revisar si por el constante cambio en el medio pueden llegar a considerarse amenazas de un impacto alto.

De las amenazas con mayor impacto sólo están establecidos controles el 83%, por lo que el 13% de amenazas restantes pueden poner a la empresa en un estado de vulnerabilidad alta.
La empresa solo tiene identificados un 37,14% de los próximos pasos a seguir ante las amenazas de mayor impacto.

4.13.2 FASE 2: Definición de escenarios y estrategias de recuperación

En la fase anterior se realizó un análisis de riesgos RA, según este parámetro a los más altos riesgos que afecten a la continuidad del negocio se procede a determinar las estrategias de recuperación ante un incidente. Cabe indicar que para definir el escenario es mejor analizar con el peor escenario debido a que con esto se cubre cualquier incidente que pudiera ocurrir.

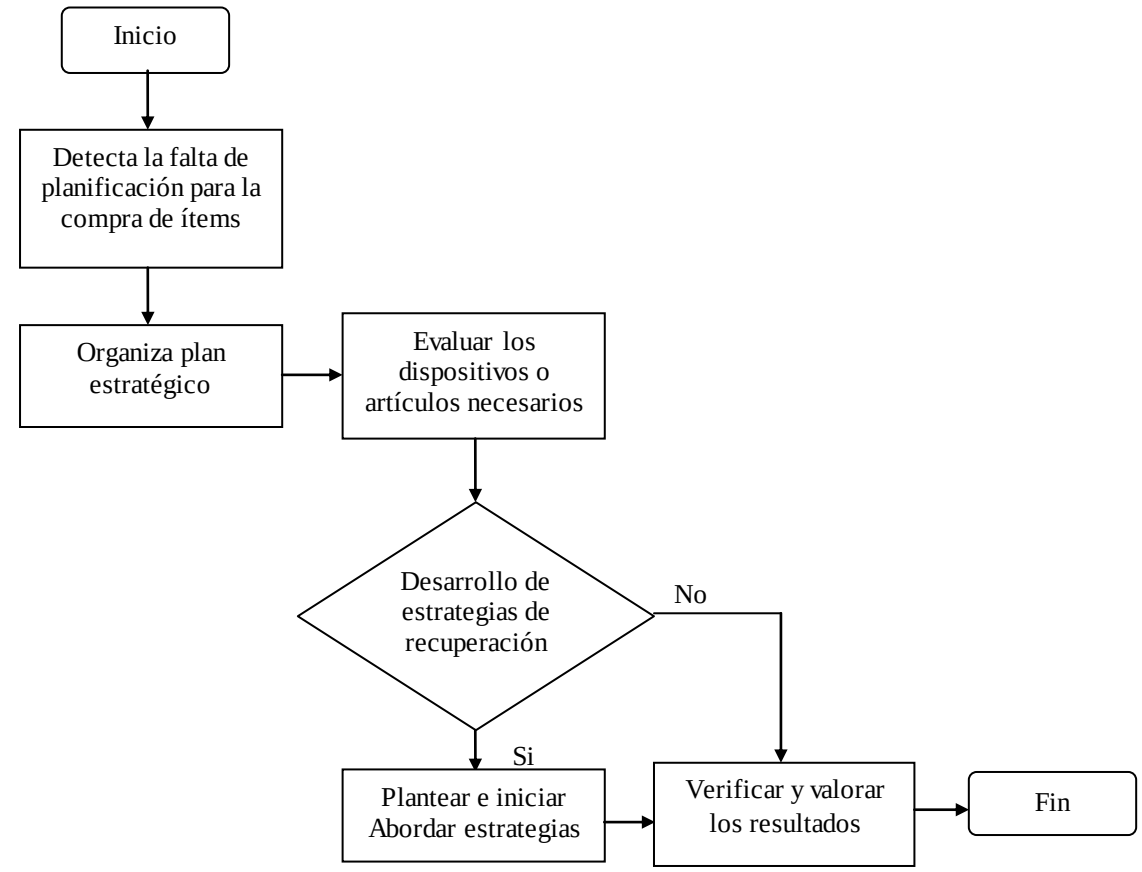
Para reducir el nivel del riesgo se puede bajar la probabilidad de ocurrencia a través de implementar los controles o transferir el riesgo lo cual implica cambiar la responsabilidad de un riesgo de una organización a otra como seguros y aceptar el riesgo que es cuando el costo de tratamiento es mayor al de su impacto.
Para la definición del escenario representativo y de mayor impacto se realizaron reuniones con los encargados y ejecutores del proceso los cuales vieron varios escenarios de alto impacto.

ESCENARIO 1: FALTA DE PLANIFICACIÓN PARA LA COMPRA DE ÍTEMS.

La falta de un plan estratégico es lo que ha forzado a la empresa a plantear nuevas estrategias para minimizar o anular amenazas, circunstancias sobre las cuales tienen una capacidad insuficiente para adquirir los productos necesarios.

Estrategias:

- Administración adecuada de inventarios para minimizar pérdidas de mercancía.
- Capacidad suficiente para albergar inventarios.
- Existencias de inventario en el momento en que se necesiten.
- Convenios y reuniones con proveedores para lograr mejorar los precios y un mejor crédito.
- Debe ser administrada bajo la lógica de un almacén. Esto implica ingreso y salida de medios magnéticos (sean cartuchos, disco removible, CD, etc.), obviamente teniendo más cuidado con la salida.
- Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.
- El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

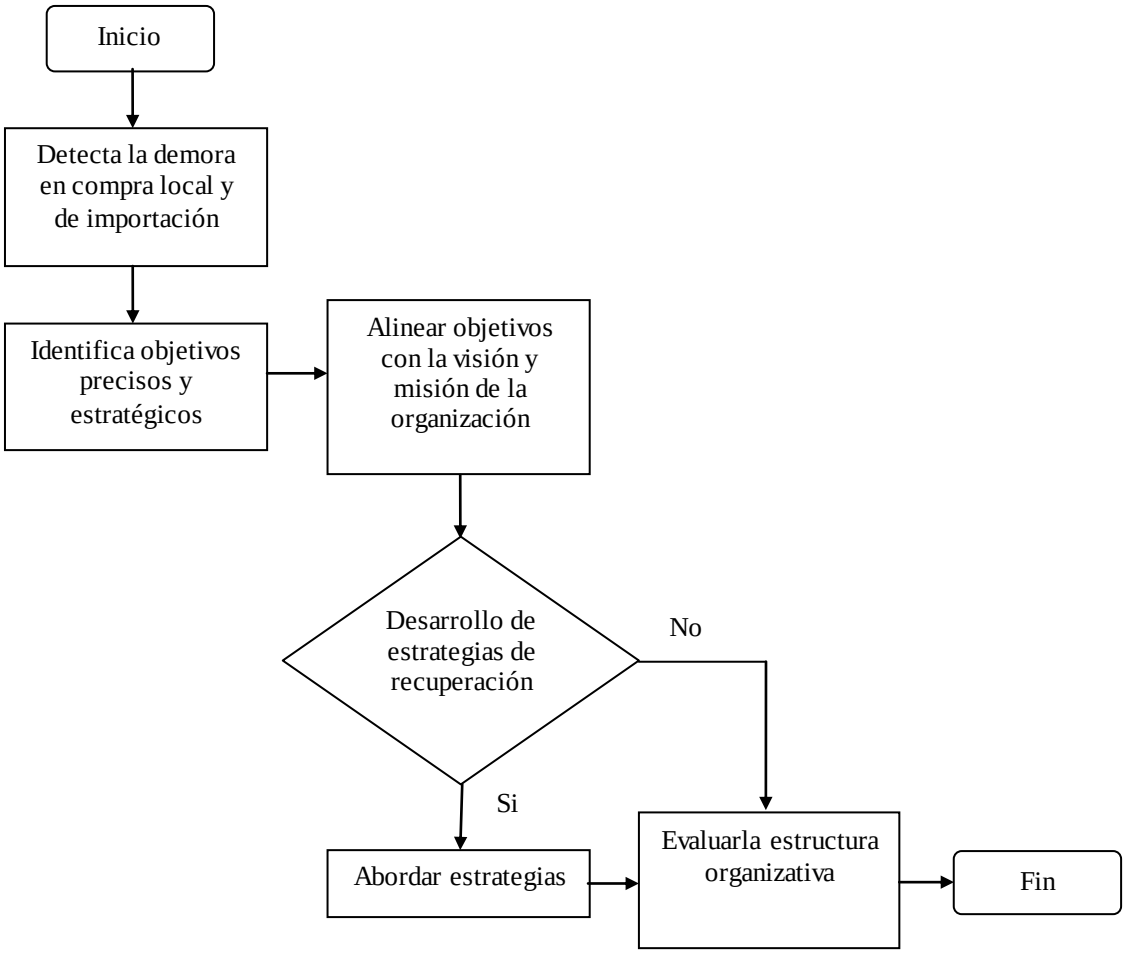


4.13.2 Esquema 20 Estrategia para solucionar la falta de planificación para la compra de ítems

ESCENARIO 2: DEMORA EN LA COMPRA LOCAL Y DE IMPORTACIÓN.

Considerando que la empresa no posee indicadores de gestión, no tiene identificado objetivos precisos a nivel de los trabajadores, ni los objetivos estratégicos alineados con la misión, visión, la empresa tiene una estructura organizativa flexible.

- Es necesario diseñar un sistema de control de gestión de tal manera que permita medir y controlar la gestión de esta importante empresa**.**
- Además debería disminuir el tiempo de demora en la compra local y de importación, para de esa manera lograr obtener cero demoras en la compra de productos.



4.13.2 Esquema 21 Estrategia para solucionar la demora en la compra local y de importación

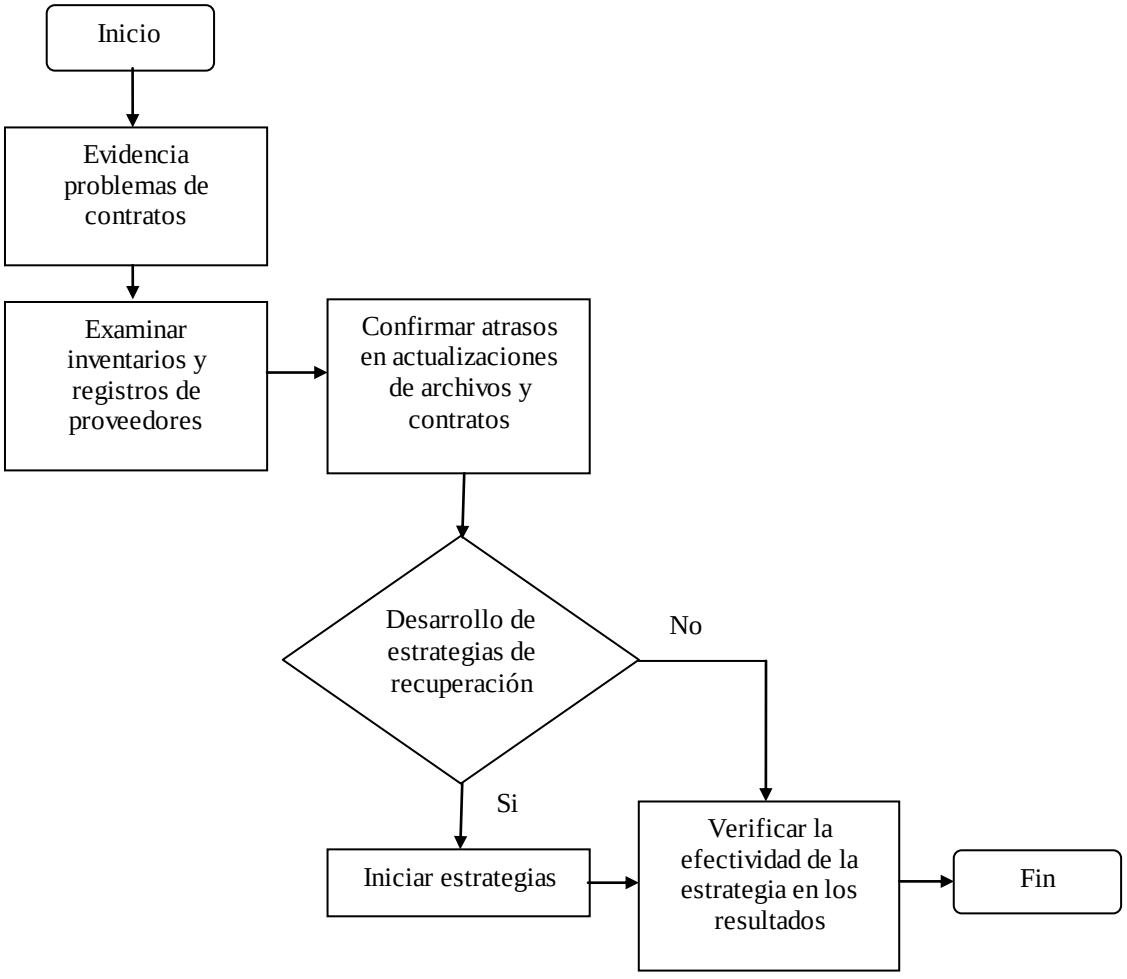
ESCENARIO 3. NO REALIZAR LOS CONTRATOS A TIEMPO.

En resumen del análisis se obtuvo lo siguiente:

- Falta de planeación operacional.
- Falta de control adecuado en inventarios.
- Atraso en actualización de archivos de proveedores.

Las estrategias a utilizar en esta situación son las siguientes:

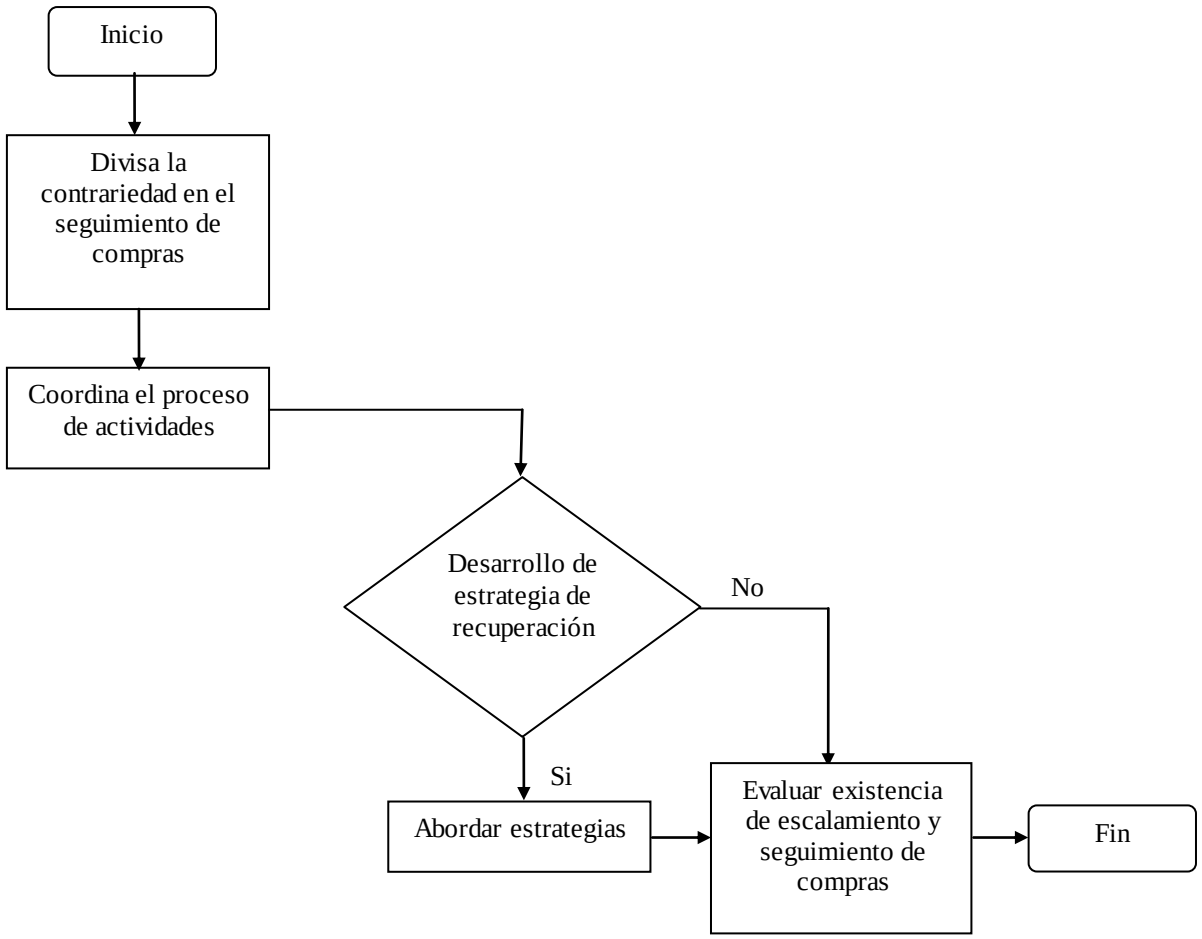
- El Departamento encargado de las compras debería tener un inventario en el momento en que se necesiten.
- Buscar nuevos proveedores, sin dejar a los ya existentes.
- Conviene actualizar periódicamente el inventario de los bienes de un negocio e informar a la compañía aseguradora sobre esos cambios así en caso de una emergencia la póliza cubra todas las pérdidas.
- Establecer un tiempo de espera entre el inicio y la ejecución de la compra para la entrega de contratos.



4.13.2 Esquema 22 Estrategia para realizar contratos a tiempo en el GPLR

ESCENARIO 4: FALTA DE ESCALAMIENTO Y SEGUIMIENTO EN COMPRAS ATRASADAS.

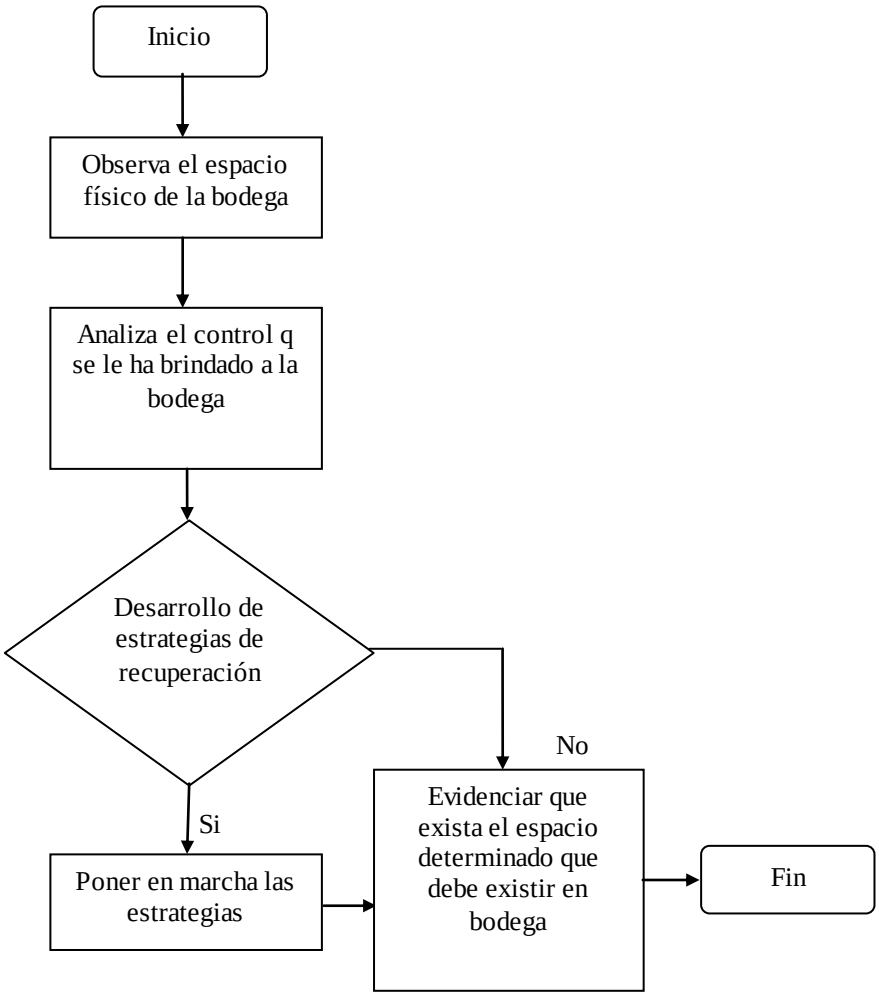
- Manejo de una caja chica o cuenta de emergencia para asuntos tecnológicos.



4.13.2 Esquema 23 Estrategia para regular escalamiento y seguimiento en compras

ESCENARIO 5: ESPACIO FÍSICO DE BODEGAS LIMITADO

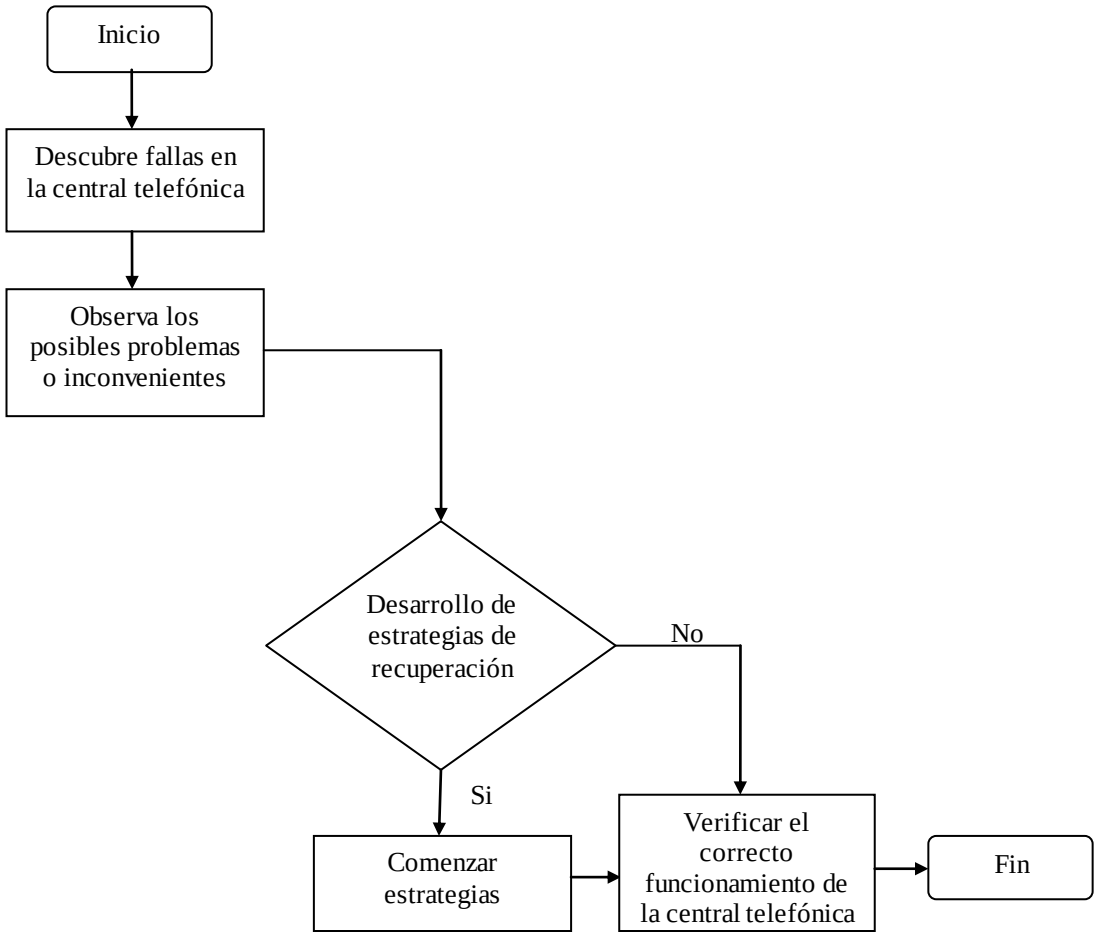
- La bodega se debe controlar para que siempre haya determinado grado de temperatura y humedad



4.13.2 Esquema 24. Estrategia para controlar el espacio físico de bodegas

ESCENARIO 6: FALLA CENTRAL TELEFÓNICA

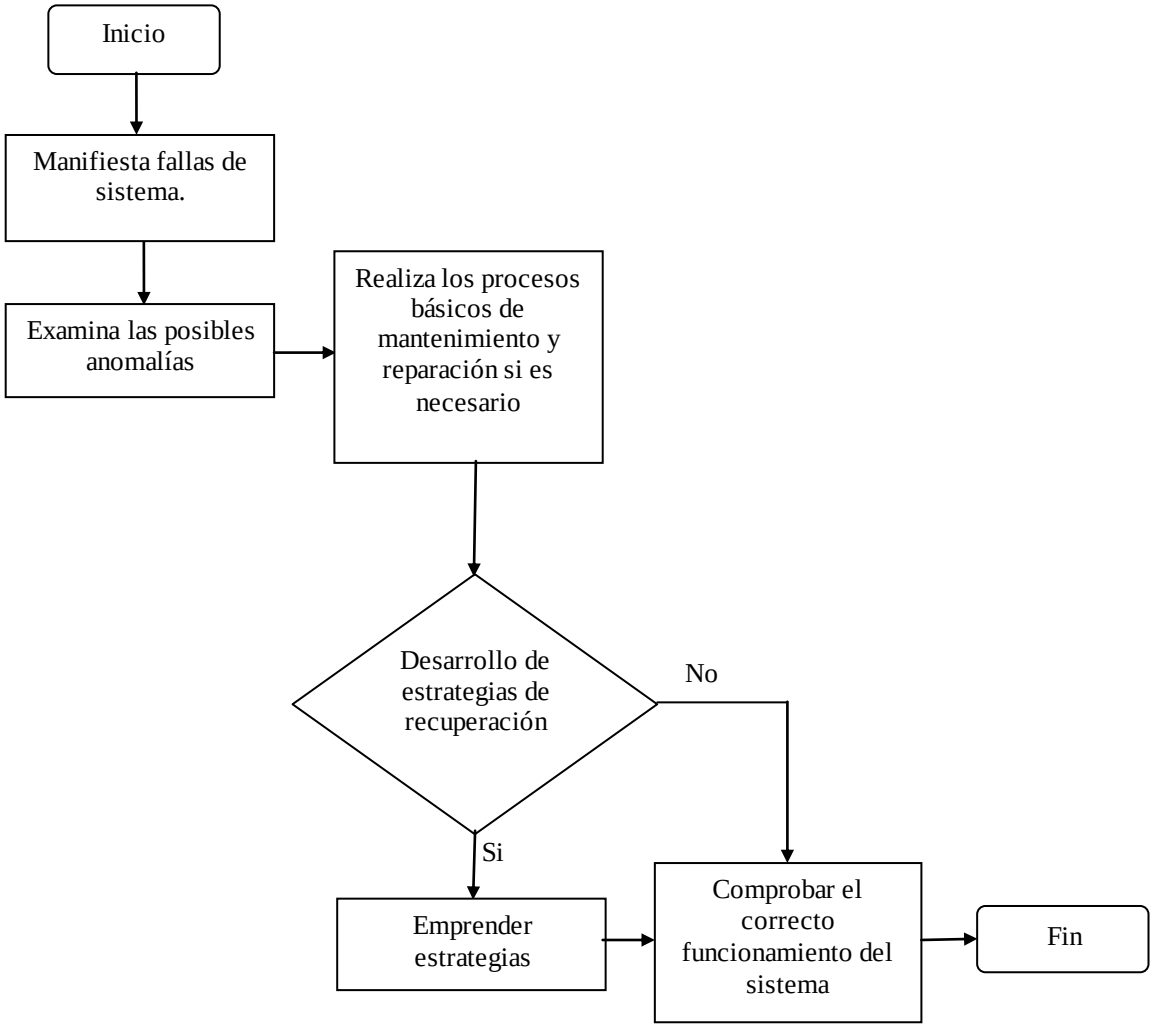
- La Central telefónica deberá contar con un sistema de VoIP reducir el uso de telefonía celular y tener como Backup un server adicional de VoIP.



4.13.2 Esquema 25. Estrategia para solucionar fallas de central telefónica

ESCENARIO 7: FALLA DE SISTEMA

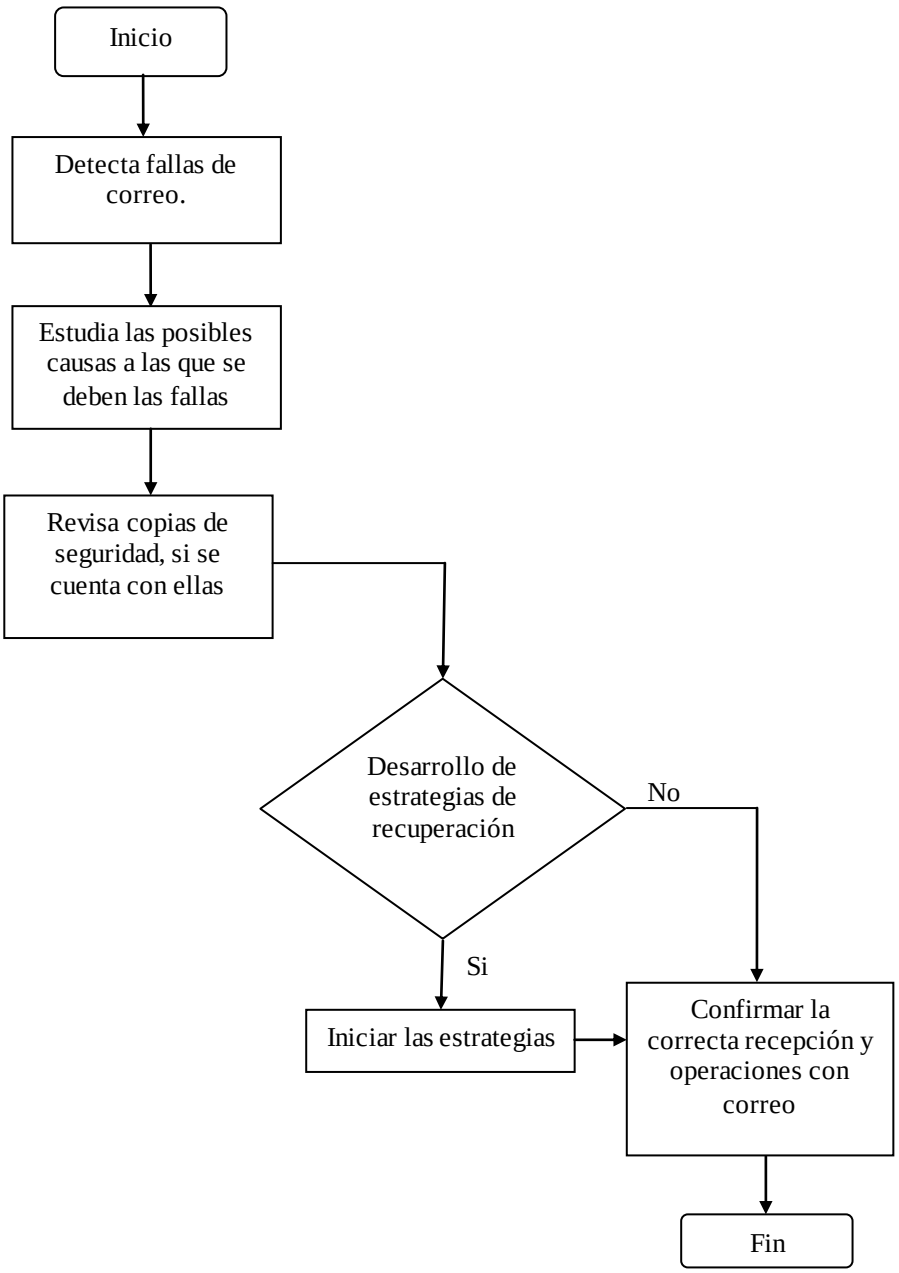
- Restaurar imágenes de sistemas operativos completos



4.13.2 Esquema 26. Estrategias para resolver fallas de sistema

ESCENARIO 8: FALLA DE CORREO

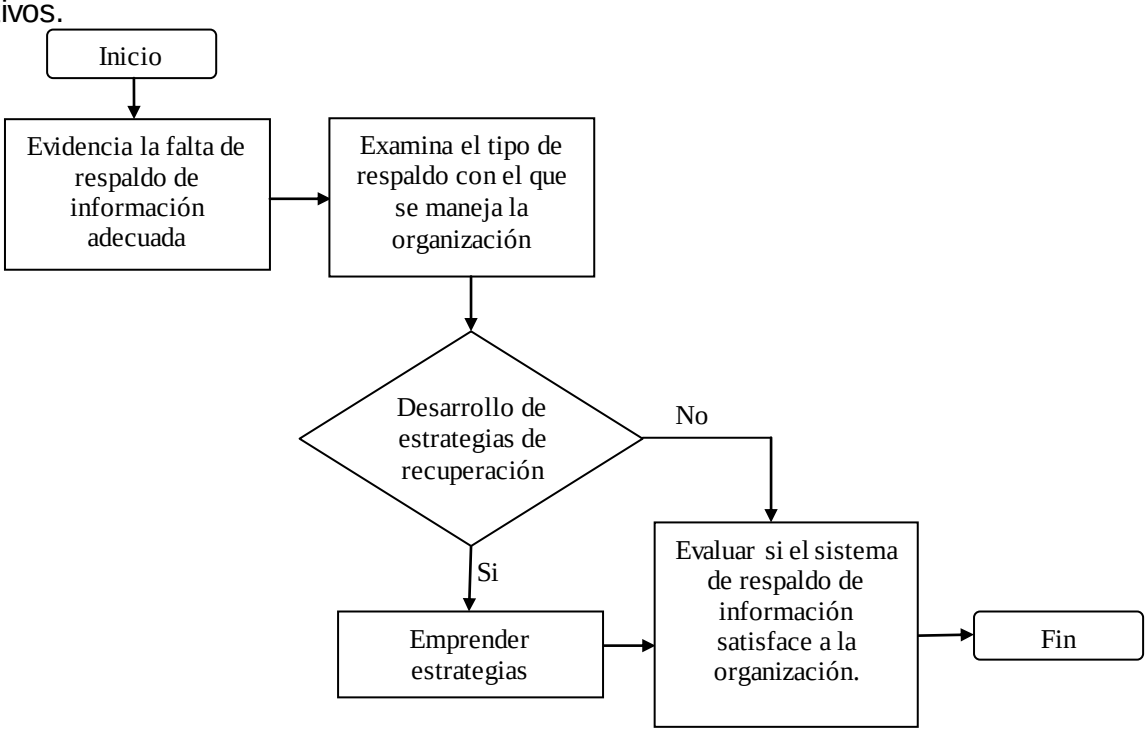
- Realizar una migración de correos plena y completamente documentada a través de un servidor Zimbra.
- Realizar copias de seguridad diarias automáticas del buzón de correo electrónico y se han guardado en el sistema de Backup.



4.13.2 Esquema 27. Estrategia para resolver falla de correo

ESCENARIO 9: FALTA DE RESPALDOS DE LA INFORMACIÓN.

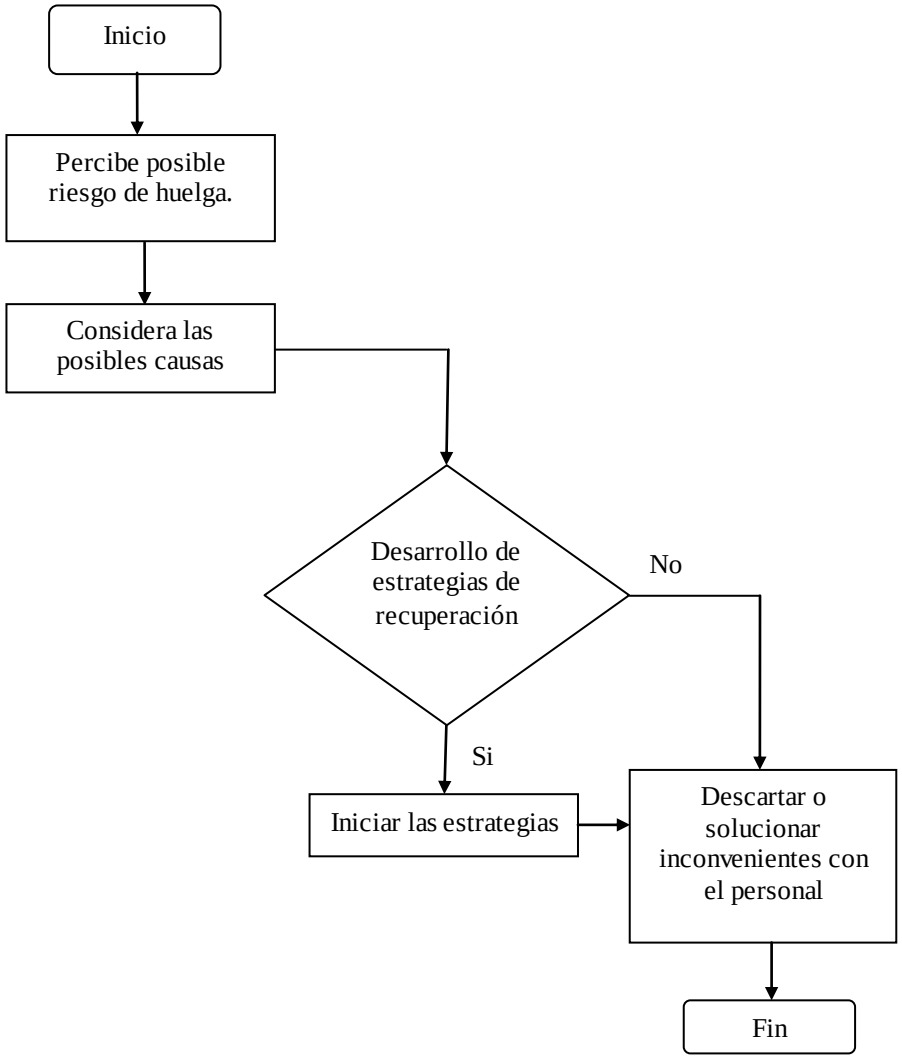
- Respaldar toda la información importante en medio magnético, ya sea en CD-ROM, Memory flash, Disco Duro portable, dependiendo de los recursos que cuente cada área. Acordamos que debe respaldarse es información y no aplicaciones.
- Generar disco de arranque para las maquinas dependiendo de su sistema operativo, libre de virus y protegidos contra escritura.
- Mantener una copia de antivirus más reciente en disco para emergencias.
- Guardar una copia impresa de la documentación de los sistemas e interface, al igual de los planes de continencia por el resto de las áreas.
- Instalar todo los Service packs que el equipo necesite y llevar un registro de los mismos, en caso de formatear el equipo o desinstalar.
- Los medios magnéticos que contienen los respaldos de información deberán ser debidamente protegidos contra amenazas de tipo físico, accidental o intencional.
- Se debe tener una copia de los respaldos fuera de la organización, procedimiento que será realizado según alguna periodicidad y con una empresa que posea acuerdos de confidencialidad con sus empleados y sea de reconocido prestigio por la seguridad con que maneja este tipo de activos.



4.13.2 Esquema 28 Estrategia para prevenir la falta de respaldos de información

ESCENARIO 10: HUELGA.

- Mantener sano el clima laboral mediante la comunicación directa y honesta con el personal.
- Informar siempre la realidad financiera de la empresa.
- Hacer pláticas mensuales con el personal para explicar acciones de prevención, preparación, antes, durante y después de una emergencia.



4.13.2 Esquema 29. Estrategia para prevenir la huelga de trabajo en el GPLR

4.13.3 FASE 3: DESARROLLO DEL PLAN

A partir de esta fase empezaremos a desarrollar nuestro Plan de Continuidad para ello definiremos lo siguiente:

- Organización de equipos necesarios para el desarrollo del Plan
- Las responsabilidades y funciones de cada equipo.
- Las dependencias orgánicas entre los diferentes equipos.
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.
- Los procedimientos de actuación ante eventualidades.
- La estrategia de vuelta a la normalidad.

4.13.3.1 ORGANIZACIÓN DE LOS EQUIPOS

Los equipos de emergencia estarán conformados por el personal clave considerado indispensable en la activación y proceso del Plan de Continuidad. Cada equipo deberá cumplir funciones y procedimientos que se ejecutarán en las distintas fases del Plan.

Los equipos que formarán parte de nuestro Plan son:

- Comité de Crisis
- Equipo de Recuperación
- Equipo Logístico
- Equipo de las Unidades de Negocio
- Equipo de Relaciones Públicas

El personal asignado a cada uno de los equipos podrá variar dependiendo de la estrategia de recuperación seleccionada y de la decisión tomada por los superiores encargados de la ejecución del Plan en el GPLR. Un miembro de la organización puede pertenecer a más de un equipo, siempre y cuando no existan dificultades al momento de realizar sus actividades en las diferentes áreas a las que corresponde el equipo.

4.13.3.1.1 EQUIPO DIRECTOR O COMITÉ DE CRISIS

Este equipo conformado por Ing. Harry Saltos e Ing. Bolívar Bravo, es el encargado de dirigir las acciones durante la contingencia y recuperación.

El objetivo de este comité es disminuir el riesgo y la incertidumbre en la dirección del suceso. Este Comité debe tomar las decisiones "claves" durante los incidentes, además de hacer de enlace con la dirección de la organización, manteniéndole habitualmente informada de la situación.

Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación o incidente.
- Decisión de activar o no el Plan de Continuidad.
- Emprender el proceso de notificación a los empleados a través del personal responsable.
- Supervisión del proceso de recuperación, de acuerdo a los tiempos estimados de recuperación.

4.13.3.1.2 EQUIPO DE RECUPERACIÓN

La función de Ing. Harry Saltos, Ing. Bolívar Bravo e Ing. Jacinto Aguirre como miembros del equipo de recuperación es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.).

El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye todos los servidores, PC's, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio.

4.13.3.1.3 EQUIPO LOGÍSTICO

Como miembros del equipo logístico el Lcdo. Fernando Medina e Ing. Manuel Moreno son los responsable de toda la logística necesaria en el esfuerzo de recuperación. Este equipo se encarga de todo lo concerniente a las necesidades logísticas en el marco de la recuperación, tales como:

- Transporte de material y personas (si es necesario) al lugar de recuperación.
- Suministros de oficina.

- Alimentación.
- Reservas de hotel, si son necesarias.
- Contacto con los proveedores.

El personal de este equipo debe trabajar conjuntamente con los demás equipos, para asegurar que todas las necesidades logísticas sean cubiertas.

4.13.3.1.4 EQUIPO DE LAS UNIDADES DE NEGOCIO

El equipo de Unidades de negocio está encargado de la ejecución de pruebas para verificar la efectiva recuperación de los sistemas críticos.

Este equipo estará formado por Ing. Harry Saltos e Ing. José Velasteguí que se encargan de laborar con las aplicaciones críticas, y serán los encargados de efectuar las pruebas de funcionamiento para confirmar la operatividad de los sistemas y comenzar a funcionar.

Cada equipo establecerá las diferentes pruebas que se deben realizar para los sistemas.

4.13.3.1.5 EQUIPO DE RELACIONES PÚBLICAS

La función del Ing. Jacinto Aguirre y Lcda. Marcia Bustamante como equipo de relaciones públicas es encargarse de las comunicaciones a los medios de comunicación y personal que requiere de los servicios del GPLR.

Consiste en canalizar la información que se realiza al exterior en un solo punto para que los informes sean descritos o narrados desde una sola fuente. Sus funciones principales son:

- Elaboración de comunicados para la prensa.
- Comunicación con los usuarios.

Un valor o factor muy importante de la organización son sus usuarios, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación.

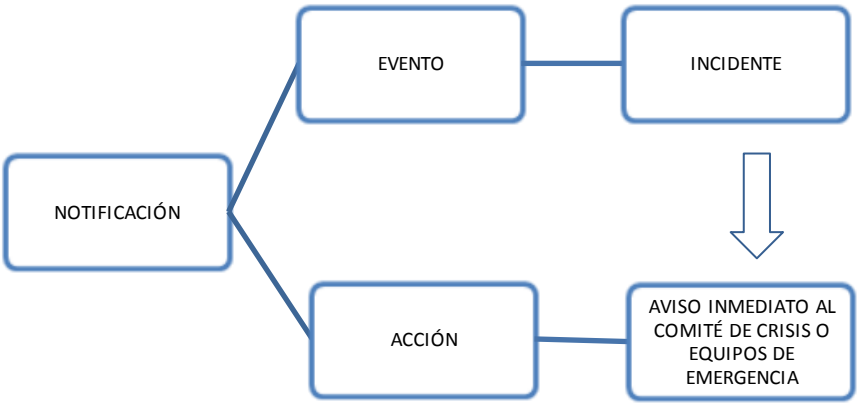
4.13.3.2 EL DESARROLLO DE LOS PROCEDIMIENTOS DE ALERTA Y ACTUACIÓN ANTE EVENTOS QUE PUEDAN ACTIVAR EL PLAN.

Habiendo establecido los equipos designadas las funciones que debe desempeñar cada equipo, procedemos a desarrollar los procedimientos que van a seguir, y su participación en cada una de las fases de activación del Plan de Continuidad.

4.13.3.2.1 FASE DE ALERTA

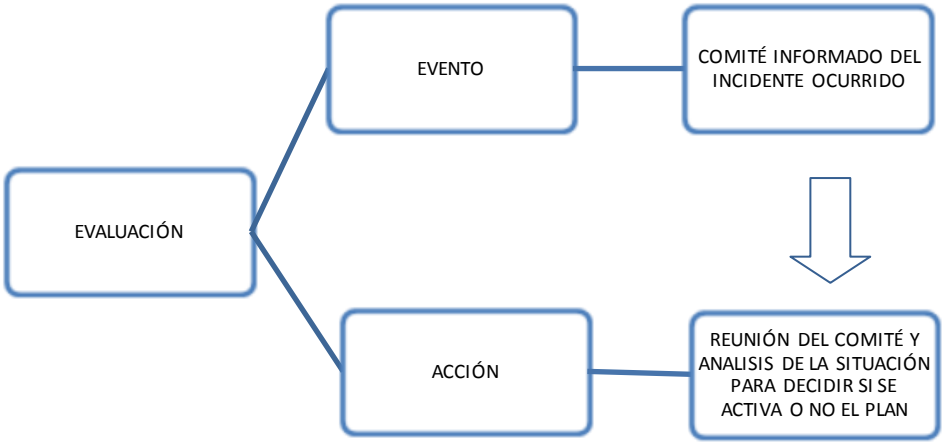
En la Fase de Alerta se define los procedimientos de actuación ante las etapas primarias de los acontecimientos que impliquen la pérdida parcial o total de uno o varios servicios críticos. Esta fase se divide en tres partes:

- NOTIFICACIÓN**:** Define cómo y quién debe ser informado en primera instancia de lo ocurrido.



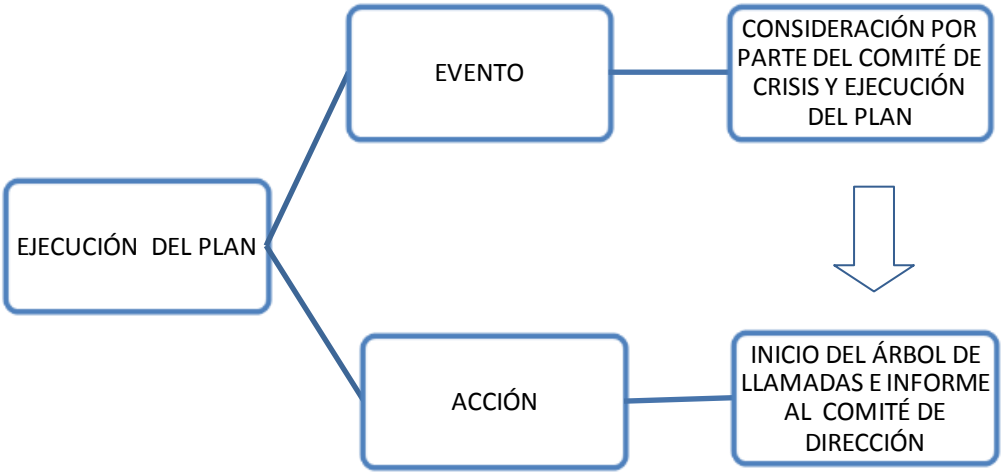
4.13.3.2.1 Esquema 30. Notificación en los procesos de fase de alerta

- EVALUACIÓN: Análisis de la situación y valoración inicial de los daños. Definición de estrategias.



4.13.3.2.1 Esquema 31. Evaluación en el proceso de fase de alerta

- EJECUCIÓN DEL PLAN: Consiste en la decisión del equipo director de proyectar el Plan debido al alcance de los daños.



4.13.3.2.1 Esquema 32. Ejecución en el proceso de fase de alerta

4.13.3.2.2 FASE DE TRANSICIÓN

La Fase de Transición es el período previo a la de recuperación de los sistemas. Resulta indispensable que en el transcurso de esta fase exista una coherencia entre los diferentes dispositivos y equipos de logística, ya que son ellos los que se encargan de que todo esté disponible para promover la recuperación en el menor tiempo posible.

La fase de transición la dividimos en dos partes principalmente:

- PROCEDIMIENTOS DE CONCENTRACIÓN Y TRASLADO DE PERSONAS Y EQUIPOS.

El procedimiento de concentración y traslado de personas y equipos podría variar dependiendo de la solución final que se solvente como estrategia de respaldo. Efectuaremos una representación general de los procedimientos, que podrá completarse una vez que se tome una solución definitiva.

Habiendo informado a los equipos de emergencia y puesto en marcha el Plan, deberán acudir al centro de reunión previamente establecido. Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como centro de respaldo, o cualquier otro designado por el Comité de Dirección de Crisis.

Además del traslado de personas al centro de recuperación en caso de ser necesario, se debe llevar a cabo una importante tarea de acoplamiento y coordinación para el traslado de todo el material necesario para poner en marcha el centro de recuperación (cintas de Backup, material de oficina, documentación...)

- PROCEDIMIENTOS DE PUESTA EN MARCHA DEL CENTRO DE RECUPERACIÓN.

Una vez concentrados los distintos equipos que van a intervenir en la recuperación, y con todos los elementos necesarios disponibles para emprender la misma, se pondrá en marcha este centro, implantando la infraestructura necesaria, tanto de software como de comunicaciones, etc.

4.13.3.2.3 FASE DE RECUPERACIÓN.

Teniendo establecidas las bases para iniciar con la recuperación, se deberá proceder con la carga de datos y reposición de los servicios críticos. El proceso de esta fase y la anterior comúnmente precisan los mayores esfuerzos e intervenciones para cumplir con los plazos fijados.

Podemos dividir la fase de recuperación en dos:

- Procedimientos de Restauración

Estos procedimientos describen las acciones que se llevan a cabo para restaurar los sistemas críticos.

- Procedimientos de Gestión y Soporte.

Ya restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se repongan las actividades y labores de la organización con las máximas garantías de éxito. Los miembros del equipo de unidades de negocio serán los encargados de analizar, comprobar y verificar el correcto funcionamiento de los procesos.

4.13.3.2.4 FASE DE VUELTA A LA NORMALIDAD

Con los procesos críticos en marcha y solucionada la contingencia, debemos plantearnos las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento.

Tomando en consideración estas acciones vamos a dividir esta fase en diferentes procedimientos:

- Análisis del impacto.

El análisis de impacto pretende realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad.

- Procedimientos de vuelta a la normalidad.

Una vez determinado el impacto deben establecerse los mecanismos que en lo posible lleven a recuperar la normalidad total de funcionamiento de la organización.

Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

4.13.4 FASE 4: PRUEBAS Y MANTENIMIENTO

Las pruebas del Plan de Continuidad tendrán dos características principales:

- Realismo**:** La utilidad de las pruebas se reduce con la selección de escenarios irreales. Por ello es importante reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.
- Exposición Mínima**:** Las pruebas se diseñan de forma que impacten lo menos posible en el negocio, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, se realizará una ventana de tiempo que impacte lo menos posible en el negocio.

Puede resultar complicado realizar una prueba completa del Plan de Continuidad de Negocios. Por ello, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal se han ensayado durante un período de tiempo.

Por la propia dinámica de la organización, 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 quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.

4.14 CONCLUSIONES Y RECOMENDACIONES

4.14.1 CONCLUSIONES

1. Todas las empresas en la actualidad deben tener métodos en lo que sus operaciones no se vean afectadas, debido a los constantes cambios en las condiciones climáticas, políticas, culturales, etc. Por lo que el GADPLR consideró la importancia de diseñar un Plan de Continuidad del Negocio para sus procesos más críticos.
2. El objetivo general de la investigación se ha cumplido con el desarrollo del Plan de Continuidad del Negocio.
3. Los objetivos específicos de este proyecto fueron cumplidos, debido a que se realizaron entrevistas en donde se identificaron los eventos de posibles riesgos, se categorizaron de acuerdo a las fuentes genéricas de riesgo, se identificaron los riesgos de mayor probabilidad e impacto y de los cuales se diseñó estrategias de recuperación.
4. La hipótesis del proyecto fue demostrada debido a que con la identificación y el análisis de riesgos de acuerdo a dos parámetros importantes que son la probabilidad y el impacto, se pudo priorizar los riesgos y establecer estrategias a aplicar en caso de un desastre para prevenir impactos económicos.
5. Los beneficios de establecer el Plan de Continuidad del Negocio en el GADPLR, se resumen en que la empresa no parará las operaciones por causa de una interrupción debido a que ya están diseñadas estrategias de recuperación.
6. Para generar un Plan de Continuidad del Negocio, es necesario el total apoyo de la alta dirección de la empresa quien proporciona los recursos necesarios para la elaboración y ejecución del plan.
7. Juega un papel fundamental para la aplicación del Plan de Continuidad del Negocio el grado de compromiso de los funcionarios y ejecutores del proceso del GADPLR, los cuales dieron total apertura a las entrevistas y talleres realizados, contando con una información confiable para la realización de nuestro proyecto.

4.14.2 RECOMENDACIONES

1. Todas las empresas sean grandes, medianas o pequeñas deben considerar entre sus principales herramientas gerenciales un Plan de Continuidad del Negocio para sus procesos más críticos, con esto conseguirán tener una ventaja competitiva ante las demás empresas.
2. Para la organización en que se realizó el diseño, se recomienda que el área encargada de la administración del Plan de Continuidad del Negocio debería establecer responsabilidades de las áreas que las integran y una política de actualización y de realización de pruebas.
3. Se recomienda realizar pruebas del Plan de Continuidad del Negocio por lo menos dos veces al año, para que las personas involucradas sepan con exactitud qué se debe hacer en caso de un desastre y las personas que administran el Plan de Continuidad del Negocio puedan identificar posibles mejoras del mismo.
4. Es necesario que en una segunda fase de aplicación del Plan de Continuidad de Negocios se consideren las amenazas no incluidas en este análisis, debido a que la inestabilidad del ambiente externo podría ocasionar que las amenazas consideradas con probabilidad e impacto bajo llegaran a cambiar y a afectar considerablemente la continuidad de las operaciones normales de la organización.
5. Se considera necesario indicar que para tener éxito en el plan de continuidad, se debe tener al personal involucrado en el proceso de bien capacitado y comprometido para la ejecución del plan en caso de un desastre.
6. Es necesario crear conciencia en el personal de la importancia del Plan de Continuidad del Negocio, del beneficio económico obtenido al no parar las operaciones ante algún desastre.
7. Para las organizaciones que deseen desarrollar un Plan de Continuidad del Negocio, se recomienda que al desarrollarlo este sea flexible, sencillo y manejable para que se pueda actualizar y ejecutar fácilmente.

REFERENCIAS BIBLIOGRÁFICAS

BIBLIOGRAFÍA

- Auditoría en Informática, Ms. Lorena Carmina Jiménez, 2003
- Guía de Desarrollo de un Plan de Continuidad de Negocio, Ing. Laura del Pino

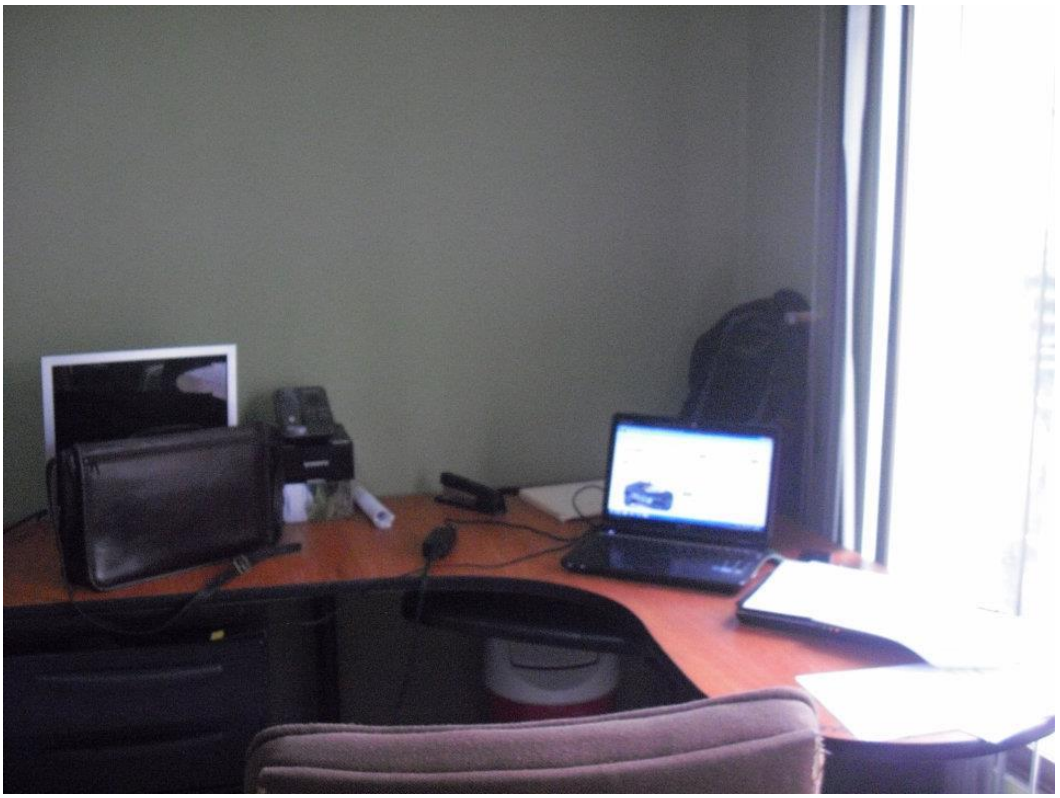
LINKOGRAFÍA

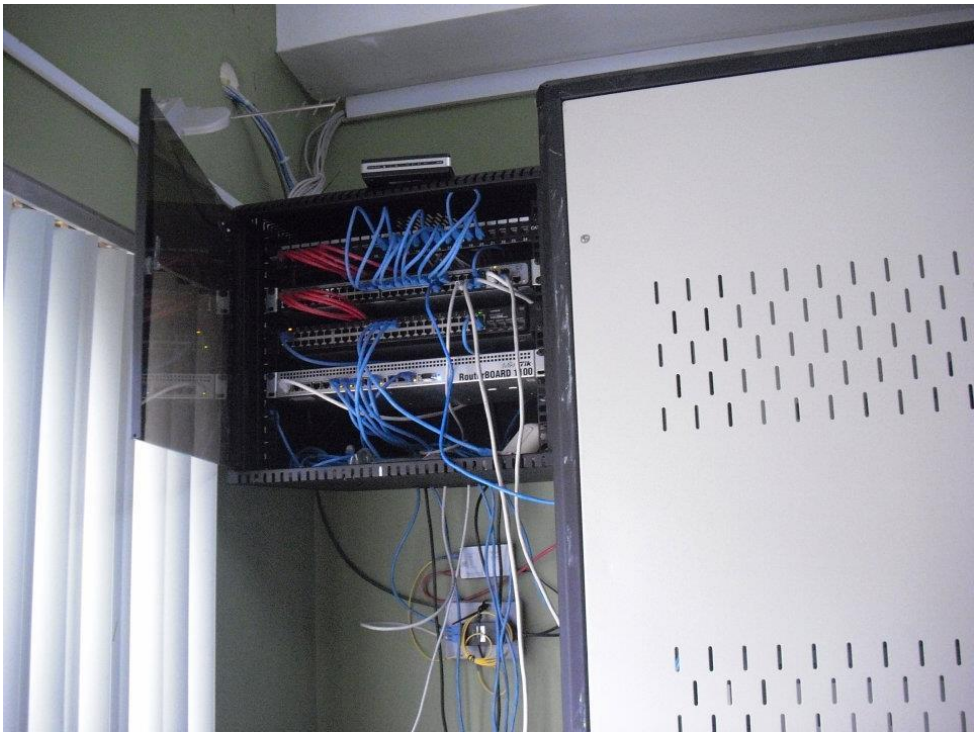
- http://www.gerencie.com/auditoria-interna.html; Autor: Mauricio León Consultor en Administración de Operaciones
- http://www.mitecnologico.com/Main/ClasificacionObjetivosDeTiposDeAuditoria; Universidad Dr. Andrés Bello El Salvador C.A
- http://www.mitecnologico.com/iem/Main/AuditoriaAdministrativa; Prof. Lauro Soto, BC, México.
- http://es.scribd.com/doc/53381984/10/Planificacion-de-la-auditoria-Informatica; Ing. Sandra Patricia Balseca Alcocer e Ing. Miguel Eduardo Cachimuel Querembás
- http://www.univo.edu.sv:8081/tesis/018134/018134_Cap5.pdf
- http://jrvargas.files.wordpress.com/2009/03/conceptos-basicos-deauditoria-informatica.pdf; .Ms. Julio Rito Vargas Avilés
- http://www.concope.gob.ec/sites/default/files/OFERTATECNICA.pdf
- http://www.los-rios.gov.ec
- http://www.los-rios.gov.ec/documentos/organico.pdf; Administración de Recursos Humanos

ANEXOS

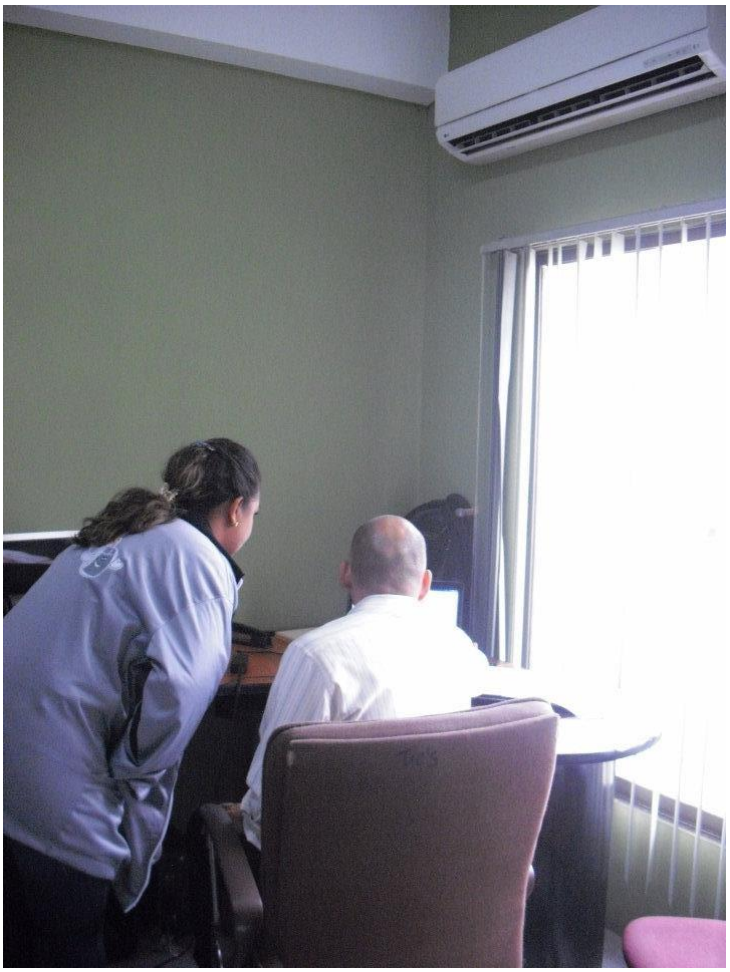
ANEXO Nº 1

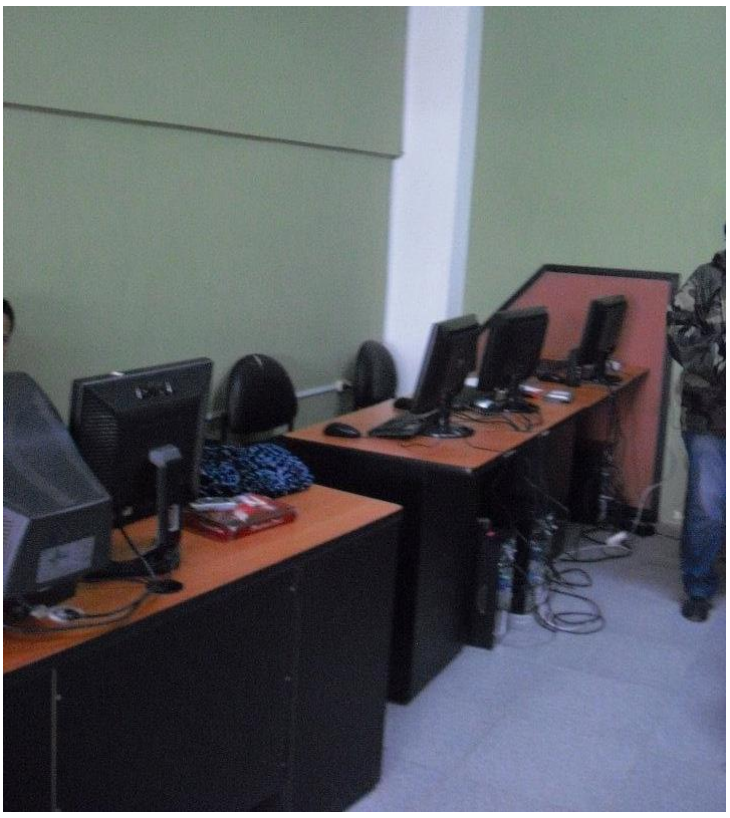
INSTALACIONES DEL GADPLR






forza





ANEXO Nº 2

Resoluciones sobre encuesta realizada a los funcionarios del GADPLR Seguridad de Información

¿Cree usted que existe una correcta ubicación y un control adecuado de acceso físico a la Unidad De Tecnología De Información Y Comunicaciones del Gobierno Provincial de Los Ríos?

En la unidad tecnología de información y comunicaciones cuenta con un espacio muy reducido para la función tan importante que desempeñan, de igual forma el control de acceso físico no es el apropiado.
Por lo tanto: Debería existir una ubicación adecuada y control restringido de acceso físico a la unidad de tecnología de información y comunicaciones en especial a las áreas de servidores.

¿Se cuenta con un procedimiento de obtención de respaldo en función a un cronograma definido y aprobado?

De acuerdo a la información acreditada, conocemos que la unidad de la TIC´S cuenta con un procedimiento de obtención periódica de respaldo en función a un cronograma.

¿En caso de actualización de tecnologías a donde se deberá emigrar la información pudiendo garantizar la permanencia de los datos?

La empresa maneja respaldo de información a través de discos duros portables.
Dándose el caso de actualización de tecnologías de soporte la información se deberá emigrar a los medios físicos adecuados con los estándares abiertos para garantizar de esa manera la permanencia y recuperación de los datos.

¿Se realiza almacenamiento de respaldo de información fuera de la empresa?

Es indispensable realizar almacenamiento de respaldo con información crítica y sensible en lugares externos a la organización.

¿Se implementa y administra seguridades a nivel de hardware y software?

Dentro de la organización se realiza implementación y administración de seguridades a nivel de estructura informática.
Esta implementación y administración es recomendable realizarla con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad que se pudiesen identificar.

¿Existe en la empresa instalaciones físicas adecuadas incluyendo mecanismo dispositivos y equipos especializados con respecto al ambiente de trabajo?

Se conoce de la unidad de tecnología de información y comunicaciones cuenta con instalaciones básicas en cuanto a mecanismo y a equipo se refiere, como energía acondicionada
Sin embargo resulta indispensable adecuar estas instalaciones para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, entre otros

ANEXO Nº 3

FORMATO DE ANÁLISIS DE RIESGOS

CÓDIGO	AMENAZAS Categorías	Probabilidad	Impacto	PxI	Exposición al riesgo

ANEXO Nº 4

FORMATO DE IDENTIFICACIÓN DE CONTROLES

AMENAZAS Categorías	PxI	Exposición al riesgo	Controles existentes	Controles recomendados (Próximos Pasos)
Compras				