PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
FACULTAD DE INGENIERIA
MAESTRÍA EN REDES DE COMUNICACIONES

ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LAS TECNOLOGÍAS DE INFORMACIÓN - CASO DE ESTUDIO "BANCO DEL ESTADO"

ANDRÉS FERNANDO HERNÁNDEZ ALVAREZ.

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
MAGISTER EN REDES DE COMUNICACIONES

QUITO, DICIEMBRE DEL 2014

RESUMEN

El presente proyecto plantea la **ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LAS TECNOLOGÍAS DE INFORMACIÓN - CASO DE ESTUDIO "BANCO DEL ESTADO"**, esta guía permitirá elaborar planes de contingencia para tecnologías de información, los mismos que permitirán asegurar la continuidad de la infraestructura tecnológica del negocio, en caso de que sea interrumpido por algún tipo de incidente.

Esta guía para la elaboración de Planes de Contingencia de TIs, se compone de varias etapas que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para la infraestructura tecnológica del negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción de las TIs.

Como resultado de esta investigación se obtendrá un documento guía el cual puede ser tomado para la creación de un plan de contingencia de TIs, en cualquier institución, en el caso de esta investigación y como caso de estudio en el cual se muestra la aplicabilidad de esta tesis se ha elegido al "Banco del Estado", para el desarrollo de un plan de contingencia y así demostrar paso a paso todo lo detallado en cada una de las etapas de esta tesis.

Con este documento aplicado a las tecnologías del Banco del Estado se permitirá reducir el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores, se establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos tecnológicos, así como acuerdos con entidades internas y externas.

La activación de este Plan de Contingencia debería producirse en situaciones de paralización de servicios tecnológicos y cuando las medidas de seguridad hayan fallado.

Esta investigación, se divide en cuatro capítulos, detallados de la siguiente manera:

En el Capítulo I, se definen los lineamientos para el desarrollo de esta investigación, se realiza una introducción a los planes de contingencia de TIs, se justifica la elaboración de este proyecto y se plantean los objetivos principales, además se resume el estado del arte en cuanto a Planes de Contingencia de TIs.

En el Capítulo II, se realiza la investigación basado en 4 etapas mismas que se pueden resumir en lo siguiente:

- Etapa 1: Se obtiene un conocimiento de los objetivos de negocio y de los procesos que se consideran críticos para el funcionamiento de la institución. Una vez identificados los procesos críticos, se analizarán cuáles son los riesgos asociados a dichos procesos para identificar cuáles son las causas potenciales que pueden llegar a interrumpir la infraestructura tecnológica del negocio.

- Etapa 2: Se basa en dos objetivos principales que son la valoración de las diferentes alternativas y las estrategias de respaldo en función de los resultados obtenidos el capítulo de análisis del negocio y evaluación de riesgos, con la elaboración de este capítulo se logra seleccionar la estrategia más adecuada a las necesidades institucionales y la corrección de las vulnerabilidades detectadas en los procesos tecnológicos críticos de negocio identificadas en el Análisis de Riesgos.
- Etapa 3: Se muestra como una vez que se ha seleccionado la estrategia de respaldo se la desarrollarla y se la implementa, en este capítulo se desarrollan los procedimientos y planes de acción para las distintas áreas y se conforman los distintos equipos que intervienen en cada etapa del Plan.
- Etapa 4: Se define la estrategia de pruebas y se realiza la prueba del Plan, para afinarlo según los resultados. Además, en este capítulo se definirán los procedimientos de mantenimiento del Plan.

En el Capítulo III, se realiza la aplicación de cada una de las etapas descritas en el capítulo II para el caso de estudio “Banco del Estado”, obteniendo como resultado un Plan de Contingencia para las tecnologías de Información de dicha institución.

Por último el capítulo IV presenta las conclusiones y recomendaciones, producto de la realización de este proyecto, así como también la respectiva bibliografía utilizada para el desarrollo de este trabajo de titulación.

TABLA DE CONTENIDOS

1. CAPITULO I: DESARROLLO CONCEPTUAL DE LA INVESTIGACIÓN

1.1. INTRODUCCIÓN

Se puede considerar como un desastre informático a la interrupción prolongada, no planificada, que afecta los servicios críticos de una organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio (centro de cómputo) o equipo alterno para su recuperación.

Dentro de la Gestión de redes y la Gestión de seguridad de la información en una institución ya sea esta pública o privada de pequeño o gran tamaño, es de vital importancia contar con un plan de contingencia de TIs, que asegure la inmediata recuperación en las operaciones tecnológicas de las instituciones ante desastres informáticos provocados por distintos tipos de incidentes ya sean estos internos o externos.

Un Plan de Contingencia, se compone de varias etapas que en principio comienzan con un análisis de los principales procesos que componen a la infraestructura tecnológica de la organización. Este análisis servirá para priorizar los procesos críticos de las TIs del negocio y establecer una política de recuperación de estas ante un eventual desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la operatividad de la infraestructura tecnológica en caso de una interrupción.

Los beneficios que trae consigo el contar con un plan de contingencia son innumerables, principalmente porque está orientado al mantenimiento de toda la infraestructura tecnológica de la organización, priorizando las operaciones críticas e identificando los procesos mínimos necesarios para continuar en funcionamiento después de un incidente.

Gracias a la elaboración de un correcto plan de contingencia se puede reducir significativamente el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores.

La activación de un Plan de Contingencia debería producirse en situaciones de paralización de servicios y cuando las medidas de seguridad hayan fallado.

En esta tesis se desglosan cada una de las actividades necesarias durante el desarrollo del Plan de Contingencia para las tecnologías de la información, las cuales podrán ser aplicadas de manera general en cualquier institución que cuente con infraestructura tecnológica misma que apalanque los procesos del negocio.

Para fines prácticos y como caso de estudio se utilizará este documento para realizar el desarrollo de un plan de contingencia para el Banco del Estado, demostrando así la aplicabilidad de esta investigación.

1.2. ANTECEDENTES Y JUSTIFICACION

La gran dependencia de tecnología que actualmente tienen las empresas principalmente las que apalancan el núcleo de su negocio sobre la tecnología, hace necesario contar con una plataforma tecnológica confiable que apoye incondicionalmente el desarrollo del negocio. En este tipo de instituciones un incidente en la infraestructura tecnológica de unas pocas horas de duración puede tener un impacto catastrófico en los resultados económicos y por ende en la continuidad de sus actividades.

Un desastre tecnológico no necesariamente debe estar relacionado con un incendio, terremoto, inundaciones o cualquier otro evento de gran magnitud producido por la naturaleza, para poner en peligro no sólo las operaciones del negocio sino su misma supervivencia; eventos tales como la irrupción de un virus, ataques informáticos o la instalación de un parche de seguridad pueden provocar la pérdida de información crítica de la institución, inoperatividad temporal y en el peor de los casos el daño definitivo de los sistemas e infraestructuras tecnológicas.

Como se había mencionado en el párrafo anterior, existen varios tipos de incidentes y no sólo las catástrofes naturales, pueden causar daños irreparables a la infraestructura tecnológica de una organización; existen otro tipo de incidentes, que pueden tener impactos gravísimos y en ocasiones irreversibles para una empresa, por ejemplo daños en la infraestructura donde están alojados los equipos informáticos, fallas en el suministro eléctrico, fallo en los enlaces de comunicación de los proveedores, incidentes de seguridad en los sistemas informáticos como hacking, phishing, pérdida o robo de

información sensible del negocio, errores de operación en la infraestructura tecnológica, inclusive incidentes ajenos a la operación del negocio como actos de terrorismo, vandalismo o sabotaje.

Las empresas que alojan servicios de interés común en su infraestructura tecnológica usualmente están siendo atacadas por hackers (piratas informáticos) que principalmente buscan realizar fraudes a la institución y a sus clientes. Un número creciente de ataques informáticos les deja poco tiempo para reaccionar a nuevas amenazas y remediar los sistemas para asegurarse de que no serán violentados en una nueva ocasión

Las consecuencias de estos accidentes sobre las organizaciones que no cuentan con un plan de contingencia de TIs pueden llegar a ocasionar el cese de las operaciones, más aún si se tratan de entidades financieras que sostienen la operación de su negocio sobre las tecnologías de la información, como es el caso de estudio en uno de los capítulos de esta tesis.

Por todas estas razones es de vital importancia contar con un plan de contingencia de TIs que permita obtener un mapa de acciones que reduzcan la toma de decisiones durante las operaciones de recuperación de la infraestructura tecnológica, restaure eficazmente los servicios críticos y permita un normal funcionamiento de los sistemas y procesos de inmediato, minimizando costos y niveles operativos. El plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, para la restauración efectiva de la infraestructura tecnológica.

Es fundamental conocer los beneficios que trae a una Institución la elaboración de un Plan de Contingencia de TIs, a partir de los siguientes elementos:

- Protección de la viabilidad de la gestión al enfrentar una interrupción mayor, mediante una estrategia de continuidad.
- Aprovechamiento de la infraestructura actual para ese objetivo.
- Aprovechamiento de la documentación actual (procesos y procedimientos).
- Equilibrio entre las variables: costo, beneficio y riesgo.
- Definición de una estructura organizacional para el Plan de Contingencia de la Gestión en TIC.
- Diseño de medidas para reducción de riesgos identificados.
- Definir una estrategia global de continuidad de negocio, basada en la recuperación de la operación y servicios sustantivos de cualquier organización.
- Selección de componentes para cumplir con la estrategia de contingencia.
- Tener la documentación necesaria y suficiente para alguna auditoria.
- Contar con análisis de riesgo e impacto de los componentes (activos) que soportan al proceso.
- Identificar los puntos más críticos y vulnerables de los procesos de TI en la organización.

Es importante resaltar la complejidad de la realización de un plan de contingencia, más aún en entidades tan dependientes del recurso tecnológico, ya que se requiere de un

profundo análisis de cada uno de los componentes tecnológicos que forman parte de los procesos del negocio.

Algunas de las dificultades que se podrían presentar al tratar de llevar a cabo esta investigación principalmente en el capítulo donde se realizará el caso de estudio son:

- Falta de involucramiento del personal de la organización.
- Falta de Compromiso de la Dirección.
- Complejidad en la recolección de información
- En el diseño del plan no se realiza una gestión correcta del riesgo.
- No se realizan simulacros o planes de prueba completos.
- Limitaciones de presupuesto.

1.3. OBJETIVOS

1.3.1. Objetivo General

- Crear un plan de contingencia para las Tecnologías de información con aplicación general, en el que se detallen los procedimientos mínimos necesarios, para la recuperación inmediata de la infraestructura tecnológica antes desastres Informáticos.

1.3.2. Objetivos específicos:

- Desarrollar un documento completo sobre la Contingencia de la infraestructura tecnológica, donde se muestren cada una de las etapas que componen el Plan.

- Realizar una guía para el análisis de la infraestructura tecnológica y evaluación de los principales riesgos de una institución, lo que se desea conseguir con este objetivo es poner de manifiesto potenciales amenazas y debilidades de la infraestructura tecnológica para atender los procesos y actividades del negocio que se consideran críticos y que pueden estar en riesgo.
- Seleccionar las mejores estrategias para la recuperación del negocio en caso de fallos de las TIs, con este objetivo se podrá valorar las diferentes alternativas y estrategias de respaldo en función de los resultados obtenidos con el objetivo anterior, para seleccionar la más adecuada a las necesidades institucionales y se podrán corregir las vulnerabilidades detectadas en los procesos críticos de TI del negocio identificadas en el Análisis de Riesgos
- Reunir los procedimientos y acciones que permitirán preparar la recuperación y restauración de las operaciones normales de tecnología de una institución después de un desastre, gracias a este objetivo, se desarrollarán los procedimientos y planes de acción para las distintas áreas y equipos, y se organizarán los equipos que intervienen en cada etapa del Plan.
- Crear los delineamientos para la elaboración de un plan de pruebas y mantenimiento.
- Aplicar el desarrollo de esta guía de elaboración de plan de contingencia para las tecnologías de información en un caso de estudio, particularmente y para propósitos de esta investigación se elegirán las tecnologías de información del

Banco del Estado, con este objetivo se podrá comprobar la aplicabilidad y funcionalidad de esta investigación.

- Establecer conclusiones y recomendaciones luego de la elaboración del Plan de Contingencia y de su aplicación en el caso de estudio “Banco del Estado”.

Es importante mencionar que para realizar el caso de estudio se cuenta como base con información de la Unidad de Sistemas de la Institución, documentación de procesos tecnológicos del negocio, documentación de la red, informes de vulnerabilidades, entre otros documentos.

1.4. DELIMITACIÓN DEL TEMA

Esta investigación cubrirá aspectos técnicos de orden general de contingencia de centro de datos, los mismos que se aplicarán en el desarrollo del presente trabajo. Por la facilidad que tiene el investigador en la observación y recolección de información del centro de datos del Banco del Estado, la propuesta estará orientada a brindar delineamientos de contingencia exclusivamente para esta locación en el capítulo que hará referencia al caso de estudio.

Para cumplir con cada uno de los objetivos específicos planteados, se redactan los diferentes capítulos de esta tesis, además de haberse realizado análisis previos de los diferentes tipos de riesgos que conlleva cada una de las etapas de la investigación.

1.5. MARCO TEÓRICO

1.5.1. ¿QUÉ ES UN PLAN DE CONTINGENCIA?

Un Plan de Contingencia de TIs se compone de varias etapas que comienzan con un análisis de los procesos tecnológicos 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 la organización, estableciendo un plan que permita continuar con la actividad empresarial apalancada en la tecnología en caso de una interrupción.

En el desarrollo de un Plan de Contingencia de TIs existen dos preguntas clave:

- ¿Cuáles son los **recursos de información** relacionados con los procesos tecnológicos críticos del negocio de la empresa?
- ¿Cuál es el período de **tiempo de recuperación crítico** para los recursos tecnológicos de información en el cual se debe establecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o aceptables?

Un Plan de Contingencia 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 Contingencia debería producirse solamente en situaciones de emergencia y cuando las medidas de seguridad hayan fallado.

1.5.1.1. Beneficios

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.
- Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.
- Fomenta e implica a los recursos humanos de la empresa en las actividades de contingencia.

1.5.2. ¿QUIEN 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 Contingencia. 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.

1.5.3. POR DÓNDE SE DEBE COMENZAR

Para desarrollar un Plan de Contingencia de TIs tenemos que empezar por obtener un conocimiento general de la empresa: sus productos/servicios, sus objetivos empresariales, procesos internos, etc.

No es lo mismo un Plan de Contingencia de TIs para una empresa de servicios de Internet que para una empresa fabricante de juguetes. Aunque en ambos casos el objetivo será el de seguir dando servicio a sus clientes, las actividades y procesos sobre las que se soporta la empresa tendrán diferentes prioridades de recuperación ante una contingencia grave.

El propósito general de un Plan de recuperación es **obtener un mapa de acciones** que reduzcan "la toma de decisiones" durante las operaciones de recuperación, restaure los servicios críticos rápidamente y permita un normal funcionamiento de los sistemas y procesos lo antes posible, minimizando costos y aumentando la efectividad.

Podemos dividir un Plan de Contingencia en cuatro Etapas:

ETAPA I – ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

Se trata de obtener un conocimiento de los objetivos de negocio y de los procesos tecnológicos que se consideran críticos para el funcionamiento de la empresa. Una vez identificados los procesos críticos, se analizarán cuáles son los riesgos asociados a dichos procesos para identificar cuáles son las causas potenciales que pueden llegar a interrumpir un negocio.

ETAPA II – SELECCIÓN DE ESTRATEGIAS

Esta etapa tiene dos objetivos:

- Por un lado, valorar las diferentes alternativas y estrategias de respaldo en función de los resultados obtenidos en la etapa anterior, para seleccionar la más adecuada a las necesidades de la empresa.
- Por otro lado, corregir las vulnerabilidades detectadas en los procesos tecnológicos críticos de negocio identificadas en el Análisis de Riesgos.

ETAPA III- DESARROLLO DEL PLAN

Una vez que se ha seleccionado la estrategia de respaldo hay que desarrollarla e implantarla dentro de la empresa. En esta etapa se desarrollan los procedimientos y planes de actuación para las distintas áreas y equipos, y se organizan los equipos que intervienen en cada etapa del Plan.

ETAPA IV – PRUEBAS Y MANTENIMIENTO

Una parte importante del Plan de Contingencia de TIs, es conocer que realmente funciona y es efectivo. Para ello se define la estrategia de pruebas y se realiza la prueba del Plan, para afinarlo según los resultados. Además, en esta última etapa se definirán los procedimientos de mantenimiento del Plan

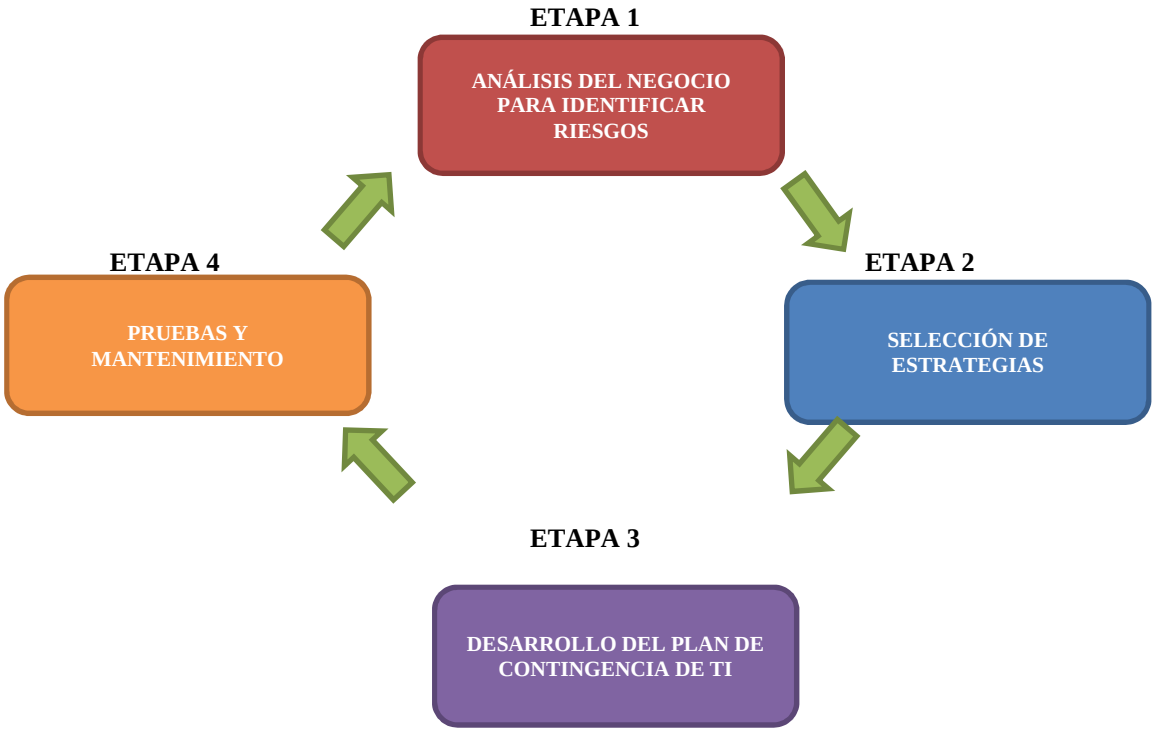


Figura 1. Diagrama de Etapas del Plan de Contingencia

2. CAPITULO II: ETAPAS PARA LA ELABORACIÓN DE UN PLAN DE CONTINGENCIA DE TIs.

2.1. ETAPA I: ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

Para desarrollar un Plan de Contingencia en este caso orientado a las tecnologías de la información, lo primero es conocer y entender cuáles son los procesos tecnológicos de negocio que son esenciales dentro de la empresa en la que se va a desarrollar el Plan, con el objetivo de asegurar la continuidad del negocio en caso de contingencia. Para esto debemos empezar por responder las siguientes preguntas:

- ¿Cuáles son las principales actividades de la empresa?
- ¿Cómo afectaría económicamente una interrupción de los servicios tecnológicos?
- ¿Cuál sería la capacidad operativa de la empresa a medida que pasa el tiempo?
- ¿Cuál es el plazo máximo para normalizar los servicios tecnológicos sin llegar a incurrir en graves pérdidas?

Las actividades y procesos que se clasifican como esenciales dentro de una empresa suelen ser en su mayoría los Operacionales y que en la actualidad están apalancados en su gran mayoría sobre procesos tecnológicos. Estos procesos interactúan directamente con los clientes o con otras organizaciones externas a la empresa (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 las empresas en cuanto a estrategias de contingencia, se utilizarán dos mecanismos de análisis:

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.

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 debe tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado.

2.1.1. ANÁLISIS DE IMPACTO

El Análisis de Impacto es esencial para establecer una estrategia de recuperación para los procesos tecnológicos, que en principio darán continuidad a las actividades críticas y posteriormente al resto, si es posible.

El nivel de criticidad de una actividad dentro de la empresa se mide en función de lo que depende de ella, que es la organización y de lo que repercutiría su indisponibilidad. En términos económicos esta valoración sería responder a la pregunta de cuánto perdería la organización si la actividad/proceso no estuviera disponible, en este caso procesos tecnológicos.

Dentro del Análisis de Impacto podemos distinguir las siguientes actividades:

- **Obtención de la Relación de Procesos:** Establecer los procesos tecnológicos de negocio que se realizan en la empresa.
- **Obtención de la Relación de Aplicaciones**: Establecer la relación de aplicaciones que soportan los procesos de la empresa.
- **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 empresa de los procesos tecnológicos cuya ausencia tendría un impacto alto en la actividad de

la empresa (valoración cualitativa). La otra, se referiría a las pérdidas económicas por período debido a la ausencia de los procesos tecnológicos (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 se denomina Período Máximo de Interrupción, las pérdidas sufren un aumento significativo y las funciones no podrían ser reasumidas.

En caso de que la organización tenga varias sucursales u oficinas, será necesario establecer un alcance geográfico.

A continuación se incluye un ejemplo de la recolección de datos para cada una de las partes que componen el Análisis de Impacto. La recolección de esta información permitirá evaluar las necesidades de la organización en materia de continuidad, por lo que es importante que la información sea lo más completa posible.

CUADRO DE PROCESOS

En este cuadro se recogen los procesos y subprocesos que componen la organización donde se va a desarrollar el Plan de Contingencia de TIs.

Proceso	Subproceso	Breve descripción	Frecuencia (Diario/Semanal Mensual)	Persona responsable

SISTEMAS QUE SOPORTAN EL PROCESO

En este cuadro se recogen los sistemas que soportan el proceso analizado.

Nombre del Sistema	Descripción	Criticidad	Tipo de Sistema (PC/Servidor/ Mainframe)	Nº de Equipos con la aplicación	Responsable	Contacto Técnico

Rangos de Criticidad:

1. La organización/departamento no puede funcionar sin el sistema
2. La organización/departamento no puede funcionar parcialmente sin el sistema
3. La organización/departamento puede funcionar sin el sistema

RECURSOS HARDWARE DEL PROCESO

En este apartado se recogen los componentes hardware que soportan los procesos.

Tipo de hardware	Detalles del Modelo/Configuración	Distribuidor	Criticidad	Localización

Rangos de Criticidad:

1. La organización/departamento no puede funcionar sin el hardware
2. La organización/departamento no puede funcionar parcialmente sin el hardware
3. La organización/departamento puede funcionar sin el hardware

OTROS ACTIVOS

En este apartado se recogen todos aquellos activos (comunicaciones, datos, infraestructura, etc.), que forman parte del proceso y que son necesarios para dar continuidad al mismo en caso de interrupción.

Descripción	Tipo	Criticidad	Localización

Rangos de Criticidad:

1. La organización/departamento no puede funcionar sin el activo
2. La organización/departamento no puede funcionar parcialmente sin el activo
3. La organización/departamento puede funcionar sin el activo

TIEMPO MÁXIMO DE INTERRUPCIÓN

Para cada uno de los procesos, se determinará el tiempo máximo de interrupción, especificando cuántos días puede permanecer el proceso sin incurrir en pérdidas económicas graves.

Proceso	Necesidades de Recuperación	Criticidad

Necesidad de Recuperación:

Día 0: Recuperación inmediata

Día 1-7: El proceso debe ser recuperado entre el primer y el quinto día después de un incidente.

Día 7–30: El proceso debe ser recuperado después de la primera semana y antes de un mes.

Más 30 días: El proceso pude esperar más de 30 días a ser recuperado.

2.1.1.1. Relación de procesos

Para obtener la información sobre los procesos tecnológicos y las respectivas aplicaciones que gestionan, es esencial la participación de las personas responsables de los mismos dentro de la empresa, y de aquellos trabajadores que conocen en profundidad los mismos. Para ello pueden utilizarse entrevistas personales y cuestionarios que nos acercarán a los procesos tecnológicos críticos del negocio.

Podemos dividir los procesos tecnológicos en operativos y procesos de soporte. Los procesos operativos son aquellos que brindan funcionalidades directas para los clientes del negocio por ejemplo funcionalidades de tipo (comercial, facturación, almacenaje, atención al cliente, etc.). Los procesos de soporte en cambio serían aquellos que facilitan los "recursos" para poder realizar los procesos operativos (recursos humanos, gestión financiera, etc.)

2.1.1.2. Relación de aplicaciones

Este punto hace referencia a la recolección del inventario de los recursos tecnológicos que soportan los procesos de la empresa, a fin de identificar aquellos que den soporte directo a los servicios críticos.

Los tipos de recursos que se deben analizar son:

- **Hardware,** identificando cada uno de los elementos hardware que soportan los sistemas de información de la empresa.
- **Software Base,** recogiendo todos aquellos componentes de software, incluido todos los asociados al sistema operativo, indispensables para el funcionamiento y optimización del Sistema de Información de la empresa.
- **Software de Aplicaciones,** inventariando las aplicaciones de gestión que son utilizadas en la empresa.

- **Sistemas de Infraestructura,** considerando aquellos elementos o componentes que sin disponer de una tecnología enfocada propiamente al tratamiento de la información sí son requeridos para garantizan la operatividad del servicio.

2.1.1.3. Relación de departamentos y usuarios

Los procesos de la empresa están gestionados por departamentos/usuarios. Dentro del inventario de procesos tecnológicos es necesario conocer el personal involucrado en los mismos. Esta información puede obtenerse en las mismas entrevistas donde se recoge la información de los procesos existentes y de los elementos (hardware, software, etc.) que lo componen.

2.1.1.4. Determinar los procesos críticos

Esta tarea supone evaluar los impactos económicos y operacionales sobre el negocio en caso de no disponer de la función analizada. La valoración de pérdidas no es una cuestión sencilla, ya que pueden concurrir aspectos intangibles, tales como la imagen de la organización ante sus clientes.

Algunos criterios que pueden ayudar a valorar las eventuales pérdidas pueden ser:

- Costo de horas de trabajo perdidas, al no poder usar las aplicaciones que no tengan alternativa manual o cuyo tratamiento manual suponga una pérdida de eficiencia importante.
- Ingresos dejados de percibir.
- Penalizaciones por incumplimiento de contratos con clientes.
- Sanciones administrativas por incumplimiento de leyes debido a la falta de control en situación de desastre (exposición de datos personales, incumplimiento de normativas, etc.).
- Gastos financieros.

Para simplificar esta valoración de los procesos podemos establecer una clasificación numérica, asignando mayor prioridad (prioridad 1) a aquellos procesos que se consideren más críticos y menor prioridad (prioridad 3) a aquellos que se consideren menos críticos.

2.1.1.5. Periodo máximo de interrupción

Una vez que obtenemos la visión del negocio, de los procesos tecnológicos que lo componen y de la criticidad de cada uno de ellos, debemos establecer los tiempos de recuperación.

Teniendo en cuenta que el objetivo del Plan es dar continuidad a los procesos tecnológicos del negocio tras un incidente o contingencia grave con las menores

pérdidas económicas posibles para la empresa, deben estimarse para cada uno de los procesos que se han considerado críticos, el tiempo a partir del cual las pérdidas económicas afectarían de forma grave a la empresa *(Tiempo máximo de interrupción)*. Esta estimación es importante para seleccionar la estrategia de respaldo adecuada a las necesidades de recuperación.

Pueden existir procesos en los que el tiempo de recuperación sea muy pequeño (horas o minutos), por ejemplo el servicio de banca electrónica, y otros procesos como la facturación a clientes en una empresa de servicios, pueden tener un periodo de recuperación mayor (días o semanas).

En definitiva, el Análisis de Criticidad nos proporciona una visión de los procesos, actividades y recursos a proteger con la prioridad de recuperación de cada uno de ellos, junto con los tiempos objetivo de puesta en marcha tras producirse incidente

2.1.2. ANÁLISIS DE RIESGOS

El principal 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 Contingencia de TIs. El Análisis de Riesgo debe centrarse en los procesos tecnológicos 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 costo que supondría. Se debe tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado.

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

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

ESQUEMA DEL ANÁLISIS DE RIESGOS

A continuación se muestra un diagrama de flujo donde se muestran los pasos que se deben considerar al realizar un esquema del análisis de riesgos.

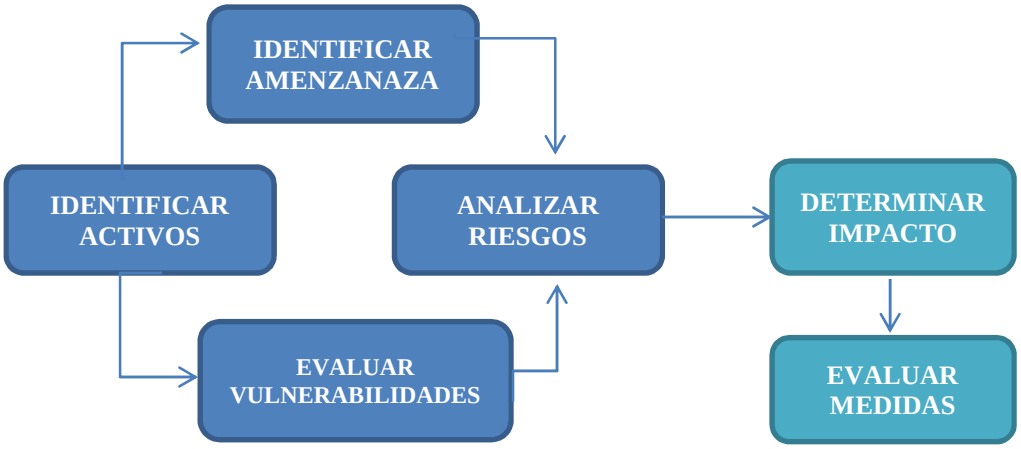


Figura 2. Esquema Análisis de Riesgos

Para el desarrollo de esta tesis no se ha seleccionado ninguna metodología concreta de análisis de riesgos, sino que se realiza una descripción general de los pasos que lo componen.

2.1.2.1. Identificar activos

Para cada uno de los procesos críticos de la empresa es necesario realizar un inventario de los activos involucrados en el proceso. Los activos se definen como los recursos de una empresa que son necesarios para la consecución de sus objetivos de negocio. Algunos ejemplos de activos de una empresa pueden ser:

- Información
- Infraestructura Tecnológica
- Conocimiento
- Sistemas de Información

Cada uno de los activos de la empresa tendrá algún costo asociado. En algunos casos este costo puede ser cuantificado con un valor económico (activos tangibles) como el software o el hardware, y en otros casos es más complicado cuantificar el activo con valores monetarios (activos intangibles) tales como el prestigio de la empresa o la confianza de los clientes.

El proceso para elaborar un inventario de activos es uno de los aspectos fundamentales de un correcto análisis de riesgos. En este inventario se identificarán claramente sus propietarios y su valor para la organización, así como su ubicación actual.

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

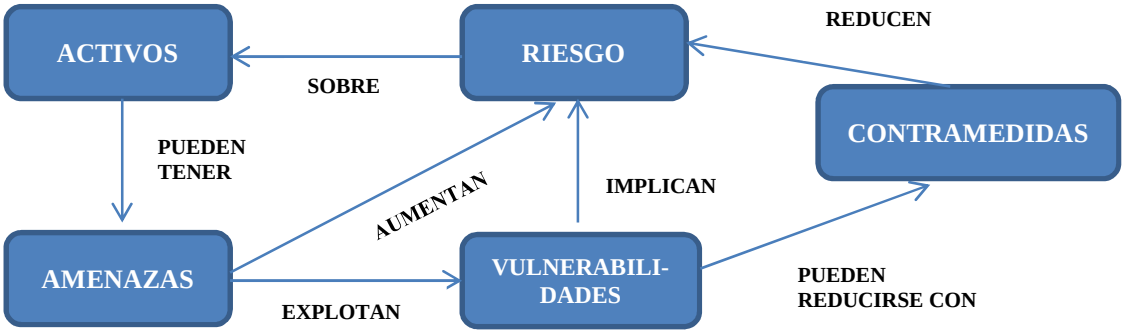


Figura 3. Relación entre los elementos que intervienen en el Análisis de Riesgos.

2.1.2.2. Identificar amenazas

Una amenaza se define como un evento que puede desencadenar un incidente en la empresa, produciendo daños materiales 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.

La siguiente figura clasifica a las distintas amenazas de los sistemas.

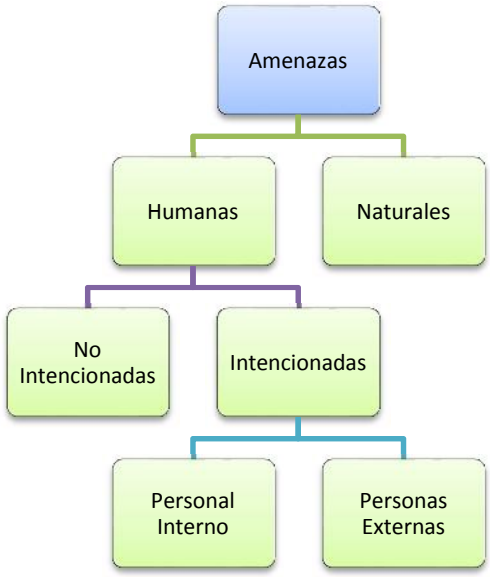


Figura 4. Clasificación General de Amenaza

Dependiendo de la institución y del proceso analizado, serán aplicables distintos tipos de amenazas. Las amenazas tendrán una ***probabilidad de ocurrencia*** que dependerá de la existencia de una vulnerabilidad que pueda ser explotada, para materializarse en un incidente.

A la hora de valorar la probabilidad de ocurrencia de una amenaza, resulta más complicado valorar las amenazas humanas (ataques maliciosos, robos de información, etc.), que las amenazas naturales. En el componente humano existen dos factores a tener en cuenta:

AMENAZA= CAPACIDAD X MOTIVACIÓN

La motivación es una característica humana que es difícil de valorar, pero que sin embargo es un factor a considerar, usualmente tiene que ver con empleados descontentos, ex-administradores de infraestructura tecnológica, etc.

A continuación, se han seleccionado algunos ejemplos de posibles amenazas.

AMENAZAS
DESASTRES NATURALES
Terremotos
Inundaciones
Incendios
DAÑOS ACCIDENTALES
Fuego fortuito
Inundaciones
Fallo del aire acondicionado
Exceso de humedad
Humo, gases tóxicos
Subida de tensión
Fallo de suministro eléctrico
Fallo de la UPS
Accidentes del personal
Capacidad inadecuada de las comunicaciones
Fallo/degradación del hardware
Fallo/degradación de las comunicaciones
Errores de operación
Fallos en las copias de seguridad
Fallos de los sistemas de autenticación/autorización
Pérdida de confidencialidad
Incumplimientos legales
ATAQUES INTENCIONADOS
Explosivos
Fuego intencionado
Accesos no autorizados al edificio
Actos de vandalismo

Robos intencionados
Manipulación de datos/software
Manipulación de hardware
Uso de software por personal no autorizado
Acceso no autorizados a datos de la empresa
Software malicioso
Robo de equipos
Robo de documentos
Robo de software
Descarga de software no controlada
Manipulación de las líneas de comunicación
Abuso de privilegios de acceso
Introducción de virus en los sistemas
Troyanos
Ataques por ingeniería social
Bombas lógicas
Ataques de denegación de servicio (DoS)
Errores intencionados
Copias incontroladas de documentos/software/datos
Errores en el mantenimiento
Corrupción de datos

2.1.2.3. 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 empresa. Las vulnerabilidades como tales no causan daño alguno, sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo o servicio.

A continuación se muestran algunos ejemplos de las vulnerabilidades más comunes, las cuales servirán como guía para el caso de estudio.

VULNERABILIDADES
Existencia de materiales inflamables como papel o cajas
Cableado inapropiado
Ancho de banda inapropiado
Suministro eléctrico inapropiado
Mantenimiento inapropiado del servicio técnico
Ausencia de mantenimiento
Políticas de firewall inadecuadas
Política de seguridad de la información inadecuada
Ausencia de política de seguridad
Derechos de acceso incorrectos
Ausencia de un sistema de extinción automática de fuegos/humos
Ausencia de backup
Ausencia de control de cambios de configuración eficiente y efectiva
Ausencia de mecanismos de identificación y autenticación
Ausencia de política de restricción de personal para uso licencias de software
Ubicación física en un área susceptible de desastres naturales
Falta de software antivirus
Descarga incontrolada y uso de software de Internet
Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales
Protección física de equipos inadecuada
Personal sin formación adecuada
Definición de privilegios de acceso inadecuada
Ausencia de un Plan de recuperación de incidentes

Para identificar las vulnerabilidades que pueden afectar a una empresa debemos responder a la pregunta: **¿Cómo puede ocurrir una amenaza?**

Para responder a esta pregunta ponemos como objetivo la amenaza y definimos las distintas situaciones por las que puede ocurrir la misma, evaluando si dentro de la empresa puede darse esa circunstancia; es decir, si el nivel de protección es suficiente

para evitar que se materialice la amenaza. Por ejemplo si la amenaza es que nos roben datos estratégicos de la empresa, podemos establecer, entre otros, los siguientes escenarios:

ESCENARIOS	NIVEL DE PROTECCIÓN
1. Entrada no autorizada a los datos a través del sistema informático.	¿Existe un control de acceso a los datos?
2. Robo de datos de los dispositivos de almacenamiento magnético.	¿Están los dispositivos de almacenamiento protegidos y controlados de forma adecuada?
3. Robo de datos mediante accesos no autorizados.	¿Existen perfiles adecuados de acceso a los datos?

Figura 5. Cuadro de Escenarios

Si no se responde afirmativamente a las preguntas de la columna derecha, es que existen vulnerabilidades que podrían utilizarse de forma que la amenaza se convierta en un incidente real, y causar daños importantes en la empresa.

2.1.2.4. Cuantificación económica

Para definir la cuantificación económica de las vulnerabilidades, se pueden trazar todos los elementos que conforman nuestro sistema (hardware y software) y observar cuáles involucran más o menos riesgo.

Para este propósito se puede utilizar la siguiente fórmula:

RIESGO TOTAL= RIESGO (componente 1) + RIESGO (componente 2)...

El riesgo de cada componente está dado en función directa a las pérdidas que ocasionaría el que éste deje de operar, así como en función de cuán vulnerable es dicho componente en este momento.

El riesgo no es fácil de cuantificar, siendo en general un estimador subjetivo. A modo de ejemplo se puede plantear la siguiente fórmula:

RIESGO (componente) = P * V

Donde P=pérdida, es la pérdida en dinero que implicaría la inoperatividad del componente hasta su reparación, aunque se pueden agregar otros estimadores como el desprestigio ante nuestros clientes y V=vulnerabilidad, es tanto o más subjetiva puesto que no hay una manera segura de establecer para todos los casos si los supuestos mecanismos de protección (del componente) son o no realmente confiables, para el caso de estudio se utilizarán las vulnerabilidades en base a la criticidad del proceso.

Para el caso de estudio se aplicarán estas fórmulas y se determinará la cuantificación económica en caso de existir vulnerabilidades en las tecnologías de información.

2.1.2.5. 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 empresa puede causar un impacto alto si ésta cae en personal malintencionadas.

También se puede estimar las pérdidas económicas de equipos tangibles valorando el costo de reposición y puesta en marcha.

2.1.2.6. Evaluación del riesgo

El riesgo es la posibilidad de que se produzca un impacto determinado en la empresa. El riesgo calculado es simplemente un indicador ligado a los valores calculados de vulnerabilidad y el impacto, ambos ligados a su vez a 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

El riesgo suele expresarse en términos cualitativos (Alto, Medio, Bajo), a continuación se muestra un ejemplo de una matriz de probabilidad/impacto:

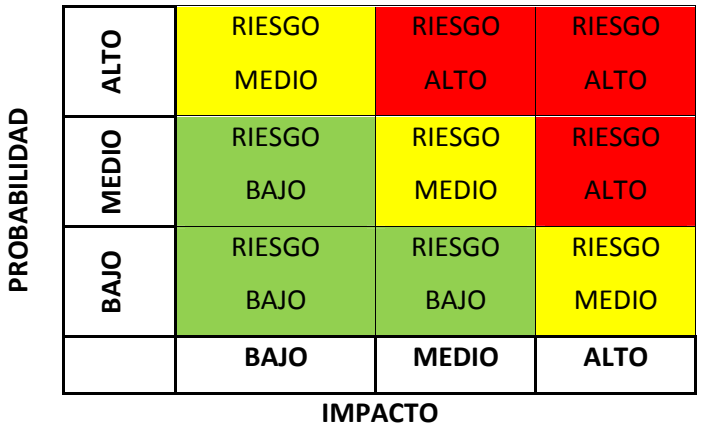


Figura 6. Matriz de Riesgos

Cuanto más baja sea la probabilidad de ocurrencia (no existan vulnerabilidades) y el impacto sobre la empresa sea también bajo, estaremos en un nivel bajo de riesgo.

Sin embargo, si existen vulnerabilidades que aumenten la probabilidad de ocurrencia o el impacto del incidente sea alto para la empresa, estaremos en un nivel de riesgo medio-alto.

A modo de ejemplo se muestra la siguiente tabla:

DESCRIPCIÓN	PROBABILIDAD	IMPACTO	RIESGO
Terremoto en ciudades situadas fuera de fallas sísmicas	**BAJA**	**MEDIO**	**BAJO**
Terremoto en ciudades situadas sobre fallas sísmicas	**ALTA**	**MEDIO**	**ALTO**
Robo de información confidencial empresa con control de acceso lógico	**BAJA**	**ALTO**	**MEDIO**
Robo de información confidencial empresa sin control de acceso lógico	**ALTA**	**ALTO**	**ALTO**

Una vez que se han evaluado los riesgos, queda decidir qué hacemos con ellos. Se pueden tomar diferentes caminos:

- Transferir el riesgo a través de seguros o subcontratando la gestión del riesgo a terceras empresas.
- Aceptar el riesgo (Esto de ser previamente aprobado por los niveles gerenciales de la empresa).
- Reducir el riesgo con controles que los mitiguen.
- Eliminar el riesgo (eliminando la causa o el foco del riesgo).

2.1.2.7. Evaluar contramedidas

Para reducir riesgos se utilizan los denominados controles o medidas de seguridad, mismos que se pueden clasificar en:

- **Controles preventivos**
    - Identifican potenciales problemas antes de que ocurran
    - 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:

  - Monitoreo de eventos.
  - Auditorías internas.
  - Revisiones periódicas de procesos.
  - Sensores de humo.
  - Antivirus.

- **Controles Correctivos**
  - Minimizan el impacto de una amenaza.
  - Solucionan errores detectados por controles detectivos.
  - Identifican la causa de los problemas con el objeto de corregir errores producidos.
  - Modifican los procedimientos para minimizar futuras ocurrencias del problema.

  Ejemplos:

  - Parches de seguridad.

- Corrección de daños por virus.
- Recuperación de pérdida de datos.

Las medidas seleccionadas para mitigar los diferentes tipos de riesgo deben mantener una proporción entre el esfuerzo y el costo necesarios para su implantación y el riesgo que mitigan (evaluación costo-beneficio).

Uno de los objetivos del Plan de Contingencia de TIs es evitar en la medida de lo posible que se produzcan incidentes que hagan necesaria su ejecución. Por ello, es importante que la empresa conozca sus riesgos tecnológicos 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. ETAPA II. ESTRATEGIA DE RESPALDO

En esta etapa se seleccionarán los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en los procesos tecnológicos de la empresa. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos determinados por el Análisis de Impacto.

2.2.1. SELECCIÓN DE ESTRATEGIAS

Existen diferentes estrategias para mitigar el impacto de una interrupción. Cada una de estas estrategias tiene ciertos parámetros de tiempo, disponibilidad y costos 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 empresa 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:** Posibilidad de trabajar desde ubicaciones exteriores a la empresa mediante conexión remota.
- **Acuerdos Recíprocos:** Acuerdos entre dos empresas (o dos unidades de negocio de la propia empresa diferentes) con características de equipamiento similar que permita a cada una de las partes recuperar funciones en la otra locación. En este caso es importante definir las condiciones de uso y la realización de pruebas periódicas para asegurar las condiciones pactadas.

- **Sitios alternos subcontratados a terceros:** Usualmente, contratación con empresas especializadas en el arrendamiento de espacios alternativos para la recuperación de la actividad del negocio, por ejemplo housing[1] o hosting[2] de infraestructura (IaaS[3], SaaS[4], etc). En este caso hay que asegurar que estas empresas pueden proporcionar unos tiempos de recuperación acordes con las necesidades de la organización, esto se define en los SLAs que se firmen con las diferentes empresas. Este tipo de empresas 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 empresas. 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.

[1] Servicio de alojamiento de infraestructura
[2] Servicio de arrendamiento de infraestructura
[3] **Infrastructure as a Service (Iaas)**, *Infraestructura como Servicio:* Modelo de distribución de infraestructura de computación como un servicio. En lugar de adquirir servidores, espacio en un centro de datos o equipamiento, los clientes rentan estos recursos a un proveedor de servicios externo
[4] **Software as a Service (SaaS)**, *Software como Servicio:* Modelo de distribución de software donde una empresa sirve el mantenimiento, soporte y operación que usará el cliente durante el tiempo que haya contratado el servicio

- **Localizaciones diversas:** Se traslada la operación pero no el personal.
- **Centro replicado (Centro de Datos Alterno):** Esta solución permite trasladar de forma inmediata la operación y continuar la actividad de forma inmediata. Esta solución es normalmente la más cara, pero también la mejor en el caso de que se necesite una recuperación muy rápida de la operación,

A continuación se muestra una tabla que recoge la relación entre el Tiempo Objetivo de recuperación y la solución de continuidad más adecuada a este Objetivo:

TIEMPO OBJETIVO DE RECUPERACIÓN	INTERNAS	CONTRATADO
MESES	Reconstrucción / Realojamiento	----
SEMANAS	Edificios prefabricados On-Site	Contratación de unidades móviles o prefabricados
DIAS		Subcontratación de procesos en oficinas móviles
HORAS	Localizaciones diversas con empleados formados	Re-localización de un grupo de personas
INMEDIATO	Localizaciones diversas para la misma función	Cambio de funcionamiento a un centro de respaldo subcontratado

Figura 7. Tabla de Estrategias de Recuperación

De todas las alternativas existentes hay que elegir la más adecuada en cada caso. Dependerá de las necesidades de cada empresa, en cuanto a tiempos de recuperación, costos económicos, recursos, etc.

Además deberá considerarse otros 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
  - Costo

Usualmente si el tiempo de recuperación objetivo es menor, mayor será el costo de la solución. Por ello es conveniente realizar un análisis con tiempos de recuperación adecuados y adaptados a la realidad de la empresa.

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 tecnológicos de negocio en un plazo razonable.

2.3. ETAPA III. DESARROLLO DEL PLAN DE CONTINGENCIA DE TIs.

Hasta el momento se ha obtenido conocimiento de los procesos tecnológicos de la empresa, valorando cuáles son críticos para el funcionamiento del negocio, valoración de los riesgos tecnológicos que pueden afectar al negocio y que pueden disparar el Plan de Contingencia de TIs. Y estrategias de Contingencia adecuadas para el negocio.

Con estos conceptos, se desarrollará el Plan de Contingencia de TIs. Para ello se debe definir lo siguiente:

- 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.

2.3.1. ORGANIZACIÓN DE LOS EQUIPOS

Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Contingencia de TIs. Cada equipo tiene funciones y procedimientos que tendrán que desarrollar en las distintas etapas 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 clientes y de ser el caso a los medios de comunicación.

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.

2.3.1.1. 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 claves durante los incidentes, además de ser el enlace con la dirección de la empresa, manteniéndolos informados de la situación.

Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación.
- Decisión de activar o no el Plan de Contingencia de TIs.
- 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.

2.3.1.2. Equipo de recuperación

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

2.3.1.3. 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..
- Contacto con los proveedores.
- Trámites administrativos, etc.

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

2.3.1.4. 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:

- Comunicación con los clientes.
- Elaboración de comunicados para la prensa (de ser el caso).

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

2.3.1.5. 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 su respectiva puesta en marcha.

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

2.3.2. 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 etapas de activación del Plan de Contingencia de TIs.

ETAPA DE ALERTA

- Procedimiento de notificación del desastre.
- Procedimiento de lanzamiento del Plan
- Procedimiento de notificación de la puesta en marcha del Plan a los equipos implicados.

ETAPA DE TRANSICIÓN

- Procedimiento de concentración de equipos.
- Procedimiento de traslado y puesta en marcha de la recuperación.

ETAPA DE RECUPERACIÓN

- Procedimientos de restauración.
- Procedimientos de soporte y gestión.

ETAPA DE VUELTA A LA NORMALIDAD

- Análisis del impacto.
- Procedimientos de vuelta a la normalidad.

En el siguiente esquema podemos ver las etapas que componen el Plan de Contingencia de TIs:

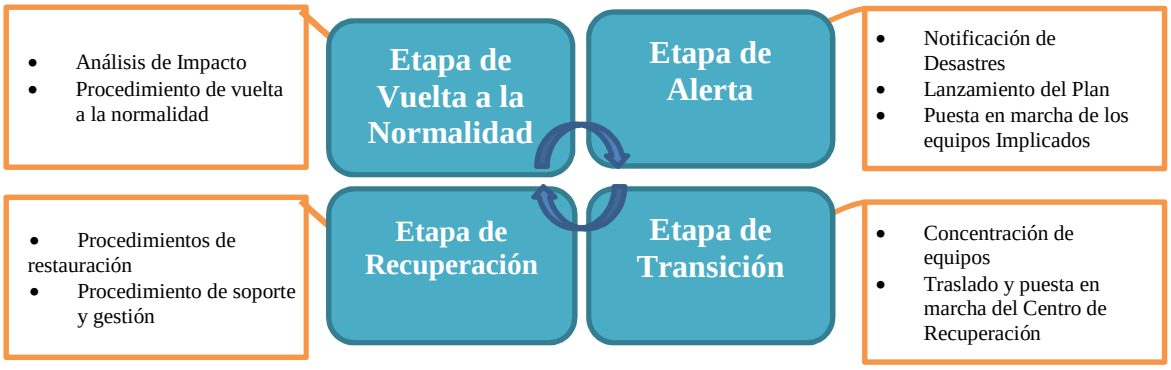


Figura 8. Etapas y Actividades del Plan de Contingencia de TIs

2.3.2.1. <u>Etapa de alerta</u>

La Etapa 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 etapa en tres partes:

1. **Notificación:** Define quién y como debe ser informado en primera instancia de lo ocurrido.

2. **Evaluación:** Análisis de la situación y valoración inicial de los daños, definición de estrategias.
3. **Ejecución del Plan:** Decisión del equipo director de ejecutar el Plan debido al alcance de los daños.

2.3.2.1.1. Notificación

Dado que no es posible elaborar un Plan de Alerta que dé cabida a todos los casos que resultan de suponer que cualquier persona pueda dar aviso de un incidente, vamos a suponer que la persona que descubre la contingencia deberá ser un empleado o cualquier otra persona próxima al lugar donde ocurre el incidente. Como parte del Plan de Contingencia de TIs se debe establecer un programa de concientización, en el que se informe debidamente al personal de cómo actuar ante estos casos y a quién comunicar lo ocurrido.

	EVENTO	ACCIÓN

1	Situación de contingencia/incidente detectado por algún empleado de la empresa. (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).

Figura 9. Cuadro Etapa de Notificación

2.3.2.1.2. Evaluación

Una vez que un miembro del Comité de Crisis es contactado e informado del incidente, procederá a evaluar la situación con la recopilación de la mayor información posible. El Comité informará a los responsables de los distintos equipos de lo ocurrido y de la situación en ese momento para que permanezcan en situación de espera, hasta que se tome la decisión de ejecutar el Plan o iniciar otro tipo de estrategia.

	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 Contingencia.
		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.

Figura 10. Cuadro Etapa de Evaluación

2.3.2.1.3. Ejecución del Plan

Una vez que el Comité de Crisis ha decidido poner en marcha el Plan de Contingencia, debe iniciarse el árbol de llamadas para comunicar a los Responsables y componentes de cada equipo, la situación de inicio de las actividades del Plan para comenzar los procedimientos de ejecución de cada uno de ellos. Deberá informarse también al Comité de Dirección. A continuación se muestra un ejemplo del árbol de llamadas.

	EVENTO	ACCION
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 Etapa de Transición.	

Figura 11. Cuadro Etapa de Lanzamiento del Plan

2.3.2.2. Etapa de transición

La Etapa de Transición es la etapa previa a la de recuperación de los sistemas e infraestructura tecnológica. Es importante que aquí exista una coordinación entre los diferentes equipos y los equipos de logística, ya que son éstos los encargados de que todo se encuentre disponible para comenzar la recuperación en el menor tiempo posible.

Podemos dividir la etapa de transición en dos partes principalmente:

- Procedimientos de concentración y traslado de personas y equipos.

- Procedimientos de puesta en marcha del centro de recuperación.

Ambos procedimientos son la base del proceso de recuperación de los sistemas. Si esta parte falla, no será posible comenzar la recuperación, y por tanto el Plan de Contingencia fallará.

A continuación pasamos a describir de manera detallada cada uno de los procedimientos y equipos que deben interactuar en esta etapa de transición.

2.3.2.2.1. 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. Se realizará una descripción general de los procedimientos, que podrán completarse una vez que se tome una solución definitiva.

Una vez que se ha dado aviso a los equipos y se ha puesto en marcha el Plan de Contingencia, deberán acudir al centro de reunión. En 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, etc.)

2.3.2.2.2. Procedimientos de puesta en marcha del centro de recuperación

Una vez se ha concentrado 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, hardware y de comunicaciones, etc.

2.3.2.3. Etapa de recuperación

Una vez que se han 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 suelen precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados.

Podemos dividir esta etapa en dos:

- Procedimientos de Restauración
- Procedimientos de Gestión y Soporte

2.3.2.3.1. Procedimientos de Restauración

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

2.3.2.3.2. Procedimientos de soporte y gestión

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.

2.3.2.4. Etapa de vuelta a la normalidad / fin de la emergencia

Una vez que han sido ejecutados los procesos críticos y se haya solventada la contingencia, debemos plantearnos las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Para ello vamos a dividir esta etapa en diferentes procedimientos:

- Análisis del impacto.
- Procedimientos de vuelta a la normalidad

2.3.2.4.1. 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.

2.3.2.4.2. 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.

2.3.2.5. Generación de informes y evaluación

Una vez solventado el incidente y de vuelta a la normalidad, cada equipo deberá realizar un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Contingencia de TIs, los tiempos empleados, dificultades con las que se encontraron, etc.

Toda esta información servirá para valorar si el Plan de Contingencia funcionó según lo planificado, así como para conocer los posibles fallos que existieron para tomarlos en cuenta en la adecuación del mismo.

2.4. ETAPA IV: PRUEBAS Y MANTENIMIENTO

2.4.1. PRUEBAS

2.4.1.1. Objetivos del plan de pruebas

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

El Plan de Pruebas diseñado tiene como objetivos:

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

2.4.1.2. Tipos de pruebas

Las pruebas de un Plan de Contingencia 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 para el negocio, usualmente estas pruebas se realizan fines de semana o fuera de horarios laborables.

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

2.4.1.3. Ejercicios técnicos

Este tipo de ejercicio requerirán la ejecución de procedimientos de notificación y de procedimientos operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado. Algunos ejemplos de elementos verificados durante un ejercicio de pruebas son:

- Procedimientos de emergencia.
- Métodos alternativos.

- Enlaces de comunicaciones de backup.
- Procedimientos de notificación Vendedores / Clientes.
- Capacidad y rendimiento del hardware.
- Portabilidad del software.
- Accesibilidad al centro de datos de respaldo.
- Movilización de los equipos de trabajo.
- Recuperación de ficheros y documentación almacenados en lugar externo.
- Recuperación de datos.

2.4.1.4. Test completo

Los ejercicios de test son ejercicios planificados que implican la restauración real de la capacidad de proceso en un centro de datos alterno. Generalmente, los procesos en producción no son interrumpidos, pero puede planificarse su restauración y validación en el centro de datos alterno. Normalmente, este tipo de prueba requiere la participación de toda la organización de contingencia de TIs, incluyendo usuarios, personal técnico y de operaciones.

2.4.2. MANTENIMIENTO DEL PLAN DE CONTINGENCIA DE TIs

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 Contingencia evitará que en poco tiempo quede obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.

2.4.2.1. Cambios al plan

Los cambios dentro del plan estarán enfocados a cumplir los siguientes puntos:

- La periodicidad con la que realizará una revisión.
- Una descripción con los principales aspectos a revisar.
- Identificación de cambios en las disposiciones relativas al negocio aún no reflejadas en los planes de continuidad.
- Establecer mecanismos de distribución de la actualización del plan y procedimientos de control

2.4.2.2. Avisos de cambios al plan.

Para la comunicación de las modificaciones al plan se debe utilizar este formulario. Adicionalmente, es conveniente que se entregue el documento en forma electrónica para facilitar su incorporación al Plan.

REV	FECHA	ALTERACION	OBSERVACIONES

3. CAPITULO III: APLICACIÓN DEL PLAN DE CONTINGENCIA DE TI PARA EL CASO DE ESTUDIO "BANCO DEL ESTADO"

A continuación se aplicará cada una de las Etapas del Capítulo II, para el caso de estudio de esta tesis, se ha elegido al Banco del Estado y con esto se corroborará que la guía para elaboración de Planes de Contingencia de TIs, es aplicable en cualquier institución.

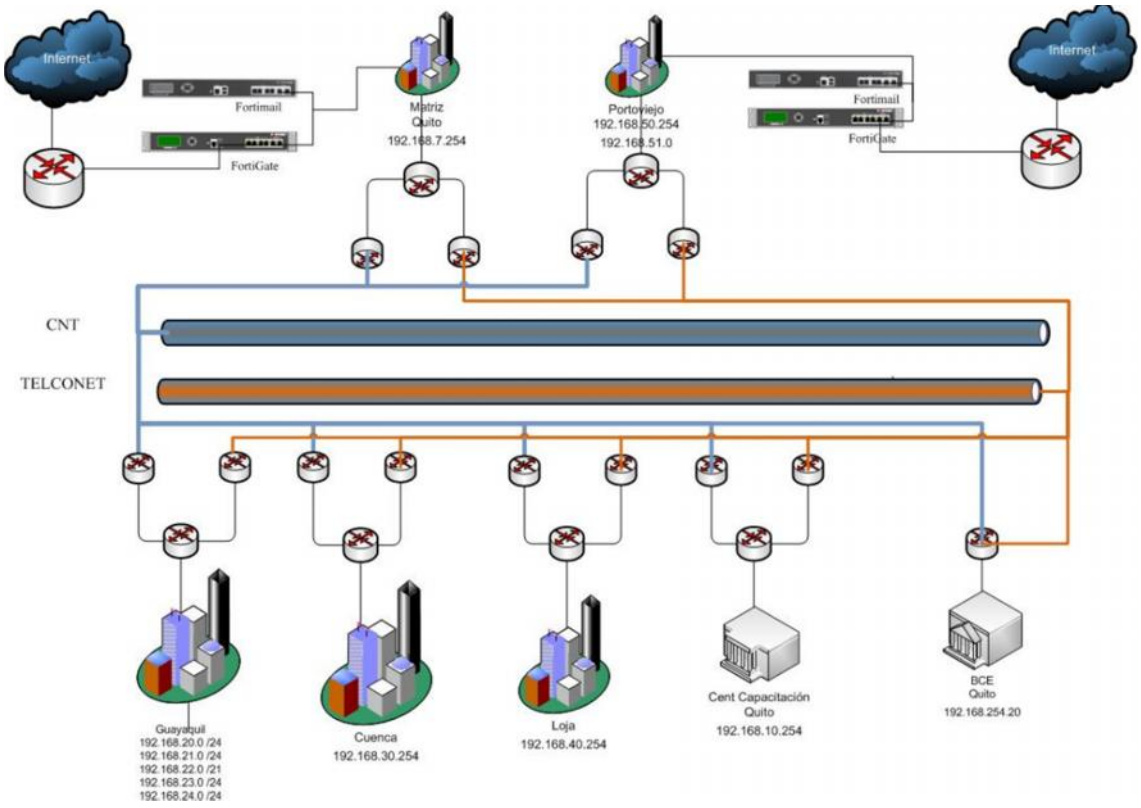
3.1. ETAPA I: ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

3.1.1. ANÁLISIS DE RIESGOS

El principal objetivo de un Análisis de Riesgos es poner de manifiesto potenciales amenazas y debilidades de la infraestructura tecnológica del Banco del Estado para atender los procesos y actividades del negocio que se consideran críticos y que pueden estar en riesgo.

3.1.1.1. Identificar activos y servicios de tecnología de la información y comunicación

A continuación se detalla el esquema de infraestructura de la red WAN del Banco:



Los activos del Banco del Estado en el área de tecnología de la Matriz en Quito y las Sucursales Regionales, son los siguientes:

3.1.1.1.1. Listado de activos y servicios de la plataforma tecnología del Banco del Estado matriz y sucursales regionales

Servidor (Función)	Localidad	Marca	Modelo	Tecnología	Número de Procesadores	Memoria RAM (MB)	Almacena-miento	Sistema Operativo	Contrato de mantenimiento (S/N)	SLA Línea Base 98 %
CUE01SERV	**Cuenca**	HP	DL380 G3	Intel(R) Xeon(TM) CPU 3.06GHz	**1 (4 Núcleos)**	2 Gb	**180 GB**	**Windows 2003 Standart**	N	98
GYE01SERV	**Guayaquil**	HP	DL380 G5	Intel(R) Xeon(R) CPU 2.00GHz	**1 (8 Núcleos)**	4 Gb	**292 GB**	**Windows 2003 Standart**	N	98
LOJ01SERV	**Loja**	HP	DL380 G3	Intel(R) Xeon(TM) CPU 3.06GHz	**1 (4 Núcleos)**	2 Gb	**126 GB**	**Windows 2003 Standart**	N	98
MAN01SERV	**Manabi**	HP	DL380 G3	Intel(R) Xeon(TM) CPU 3.06GHz	**1 (4 Núcleos)**	2 Gb	**180 GB**	**Windows 2003 Standart**	N	98
MAN02SERV	**Manabi**	HP	DL380 G5	Intel(R) Xeon(R) CPU 2.00GHz	**1 (8 Núcleos)**	4 Gb	**180 GB**	**Windows 2008 R2 Standart**	N	98
UIO03DC	**Quito**	HP	DL380 G3	Intel(R) Xeon(TM) CPU 3.06GHz	**1 (4 Núcleos)**	2 Gb	**219,6 GB**	**Windows 2003 Standart**	S	98
UIO2008DC	**Quito**	HP	DL380 G5	Intel(R) Xeon(R) CPU 2.00GHz	**1 (8 Núcleos)**	4 Gb	292 GB	**Windows 2008 R2 Standart**	S	98
UIOCORREO	**Quito**	HP	DL380 G5	Intel(R) Xeon(R) CPU 2.00GHz	**1 (8 Núcleos)**	10 Gb	584 GB	**Windows 2008 R2 Enterprise**	S	98

UIOBACKUP	**Quito**	HP	rx2600	ia64 Family 31 Model 1 Stepping 5 GenuineIntel 1300 Mhz	**1 (2 Núcleos)**	4 Gb	67,7 GB	**Windows 2003 Standart**	S	98
UIODESARRO	**Quito**	HP	rx2600	ia64 Family 31 Model 1 Stepping 5 GenuineIntel 1300 Mhz	**1 (2 Núcleos)**	4 Gb	**219,6 GB**	**Windows 2003 Enterprise**	S	98
UIOISASERVER	**Quito**	HP	DL370 G3	Intel(R) Xeon(TM) CPU 2.80GHz	**1 (4 Núcleos)**	2 Gb	72 GB	**Windows 2003 Standart**	S	98
UIO01SERV	**Quito**	IBM	SYSTEMX 3550 M3	Intel(R) Xeon(R) CPU E5405 @ 2.4GHz	**1 (8 Núcleos)**	16 Gb	1 TB	**Windows 2008 R2 Standart**	S	98
UIOSERVICIOS	**Quito**	HP	DL380 G5	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz	**1 (8 Núcleos)**	4 Gb	**292 GB**	**Windows 2003 Standart**	S	98
UIOVIDEO	**Quito**	IBM	SYSTEMX 3550 M3	Intel(R) Xeon(R) CPU E5405 @ 2.27GHz	**1 (24 Núcleos)**	32 Gb	929 GB	**Windows 2008 R2 Standart**	S	98
UIO01APP	**Quito**		HSS22	Intel(R) Xeon(TM) CPU 2.88GHz 4 core	**4 (8 Núcleos)**	32 Gb	1024 GB	**Windows 2008 R2 Standart**	S	98
UIO02APP	**Quito**		X 5650	Intel(R) Xeon(TM) CPU 2.88GHz 4 core	**4 (8 Núcleos)**	10 Gb	500 GB	**Windows 2008 R2 Standart**	S	98
UIORESPALDOS	**Quito**		X 5560	Intel(R) Xeon(TM) CPU 2.80GHz	**1**	2 Gb	2800 GB	**Windows 2008 R2 Standart**	S	98

UIOV01ADM	**Quito**	Virtual	Virtual	Intel(R) Xeon(TM) CPU E5405 2.00 Ghz	1	640 MB	16 GB	Windows Server 2003 **Standart** SP2	S	98
UIOV03ADM	**Quito**	Virtual	Virtual	Intel(R) Xeon(TM) CPU E5405 2.00 Ghz		640 MB	16 GB	Windows Server 2003 **Standart** SP2	S	98

3.1.1.1.2. Listado de equipos de redes lan de la plataforma tecnología del Banco del Estado

Cantidad	**Descripción (hub, switch, router, tarjetas de red, otros)**	**Marca**	**Modelo**	**Protocolo (TCP/IP, IPX/SPX, Netbeui, Appletalk, otros)**	**Adquisición o alquiler**	**Contrato de mantenimiento (S/N)**	**Número de Puertos/Velocidad**					
							10baseT	**100baseTX, T4**	**100baseFX**	**GB Ethernet**	**ATM**	**Otros**
2	Switch de Core	Cisco	3560G	TCP/IP	Adquisición	N			X	X		
36	Switch	Cisco	2960G	TCP/IP	Adquisición	N			X	X		
26	Access Points	Cisco	1262G	TCP/IP	Adquisición	N			X	X		
5	Routers	Cisco	1941	TCP/IP	Adquisición	N			X	X		

3.1.1.1.3. Listado de enlaces wan de la plataforma tecnología del Banco del Estado

Analógico / Digital	Proveedor			Última Milla			Ancho de Banda	Protocolo: (TCP/IP, SNA, HDLC, SLIP, ATM, Frame Relay, PPP, X25, ISDN, Otros)	SLA (línea Base 99.6 %)
	Propio	Empresa	Medio Físico: (satelital, terrestre, radio, Microonda)	Propio	Empresa	Medio Físico			
Digital–UIO-GYE	CNT – TERRESTRE			CNT-FIBRA OPTICA			3MB	MPLS	99.6
Digital–UIO-GYE	TELCONET – TERRESTRE			TELCONET-FIBRA OPTICA			3MB	MPLS	99.6
Digital–UIO-CUE	CNT – TERRESTRE			CNT-FIBRA OPTICA			3MB	MPLS	99.6
Digital–UIO-CUE	TELCONET – TERRESTRE			TELCONET-FIBRA OPTICA			3MB	MPLS	99.6
Digital–UIO-LOJ	CNT – TERRESTRE			CNT-FIBRA OPTICA			3MB	MPLS	99.6
Digital–UIO-LOJ	TELCONET – TERRESTRE			TELCONET-FIBRA OPTICA			3MB	MPLS	99.6
Digital–UIO-POR	CNT – TERRESTRE			CNT-FIBRA OPTICA			3MB	MPLS	99.6
Digital–UIO-POR	TELCONET – TERRESTRE			TELCONET-FIBRA OPTICA			3MB	MPLS	99.6
Digital–INTERNET	CNT – TERRESTRE			CNT-FIBRA OPTICA			8MB	TCP/IP	99.6
Digital–INTERNET	TELCONET – TERRESTRE			TELCONET-FIBRA OPTICA			3MB	TCP/IP	99.6

3.1.1.1.4. Listado resumen de equipos computadores pc´s de los usuarios del Banco del Estado

Por número de Pc´s disponibles (Totalizado)	Por localidad (Matriz/ Agencias)	Por tipo de procesador / velocidad	Contrato de Mantenimiento (S/N)?
5	Matriz	Pentium 4	S
8	Matriz	Dual Core	S
182	Matriz	Core 2 Duo	S
42	Matriz	Core I3	S
15	Matriz	Core I5	S
31	Matriz	Core I7	S
38	Guayaquil	Core 2 Duo	S
16	Guayaquil	Core I3	S
2	Cuenca	Dual Core	S
20	Cuenca	Core 2 Duo	S
1	Cuenca	Core 2 Quad	S
9	Cuenca	Core I3	S
1	Cuenca	Core I5	S
6	Manabí	Dual Core	S
3	Manabí	Core 2 Duo	S
19	Manabí	Core I3	S
2	Loja	Dual Core	S
15	Loja	Core 2 Duo	S
9	Loja	Core I3	S
1	Loja	Core I7	S

3.1.1.1.5. Listado de base de datos de la plataforma tecnología del Banco del Estado

Nombre	Proveedor	Versión	Número de licencias	RAM Gb	Servidor en que está instalada	Producción / Desarrollo	Localidad
SQL SERVER	Microsoft	2008 R2	1		UIO02APP	PRODUCCIÓN	MATRIZ
SQL SERVER	Microsoft	2008 R2	1		UIOWDESARRO	DESARROLLO	MATRIZ
SQL SERVER	Microsoft	2000	1		UIO01APP	PRODUCCIÓN	MATRIZ
SQL SERVER	Microsoft	2000	1		UIODESARRO	DESARROLLO	MATRIZ
SQL SERVER	Microsoft	2008 R2	1		MAN02SERV	PRODUCCIÓN	PORTOVIEJO
SQL SERVER	Microsoft	2008	1		UIOWSQLBPM	DESARROLLO	MATRIZ
SQL SERVER	Microsoft	2008	1		UIOWSQLBPMP	PRODUCCIÓN	MATRIZ

3.1.1.1.6. Listado de equipos para garantizar la continuidad de los servicios

Ups/modems/generadores electricos/clusters/servidores redundantes

Software/Hardware	Componente (Descripción)	Marca	Modelo o versión	Localidad	Contrato de mantenimiento (S/N)	SLA (línea Base 98 %)
UPS	30 KVA	General Electric	Digital Energy LP Series	Quito	S	98
UPS	40 KVA	APC	SYPN10KF	Quito	S	98
UPS	6 KVA	Power Ware	Prestige 6000	Quito	S	98
UPS	6 KVA	Power Ware	Prestige 6000	Centro de Capacitación (Quito)	S	98
GENERADOR ELECTRICO		FORD	666T BSD	Quito	S	98
GENERADOR ELECTRICO		DEUTZ	B464B	Quito	S	98
AIRE ACONDICIONADO	60000BTU	EMERSSON	Aire Presición	Quito	S	98

AIRE ACONDICIONADO	60000BTU	MILLER	Aire Presición	Quito	S	98
Switch de Core Redundante		CISCO	Catalyst 3560	Quito	S	98
Servidores Redundantes	Chasis Blade	IBM	Blade	Quito	S	98
Equipo de Comunicaciones Alterno	Arrendamiento	Telconet	Cisco	Matrizy Sucursales	S	98

3.1.1.1.7. Cuadro de infraestructura que soporta cada servicio de TI's

SERVICIO	ALCANCE DEL SERVICIO		SLA	URL CONSOLA DE ADM.	URL CONSOLA INDICADOR DEL SERVICIO	CRITICIDAD	TÉCNICO RESPONSABLE	CONTACTO DE SOPORTE PROVEEDOR	METODO DE REVISIÓN DE ACTIVIDAD	PERIODICIDAD DE REVISIÓN	URL REGISTRO DE INCIDENTES
	LOCAL	NACIONAL	%								
LAN		X	98	Switch Core 1: telnet Switch Core 1: telnet Fortinet Analyzer: https://192.168.7.53/login Fortinet Gate: https://192.168.7.52:44310/index	Fortinet Analyzer: https://192.168.7.53/login Fortinet Gate: https://192.168.7.52:44310/index	1	RUBEN CONRADO - DIEGO SOTOMAYOR	TOTALTEK S.A.	MONITOREO	PERMANENTE	Fortinet Analyzer: https://192.168.7.53/login Fortinet Gate: https://192.168.7.52:44310/index
WAN		X	98	Router Bde (5): Telnet Router CNT (5): Telnet Router Telconet (5): Telnet Fortinet Analyzer: https://192.168.7.53/login Fortinet Gate: https://192.168.7.52:44310/index	Fortinet Analyzer: https://192.168.7.53/login Fortinet Gate: https://192.168.7.52:44310/index	1	RUBEN CONRADO - DIEGO SOTOMAYOR	Corporación Nacional de Telecomunicaciones (CNT) / TELCONET	MONITOREO	PERMANENTE	Fortinet Analyzer: https://192.168.7.53/login Fortinet Gate: https://192.168.7.52:44310/index

INALAMBRICA		X	98	ACS/Red Guest : https://172.16.1.5 Cisco ACS: https://192.168.7.221/acsadmin/login.jsp	ACS/Red Guest : https://172.16.1.5 Cisco ACS: https://192.168.7.221/acsadmin/login.jsp	1	RUBEN CONRADO - DIEGO SOTOMAYOR	TOTALTEK S.A.	MONITOREO	PERMANENTE	ACS/Red Guest : https://172.16.1.5 Cisco ACS: https://192.168.7.221/acsadmin/login.jsp
INTERNET		X	98	PRTG	192.168.8.2/login	1	RUBEN CONRADO - DIEGO SOTOMAYOR	BE	MONITOREO	PERMANENTE	www.bancoestado.com
INTRANET		X	98	\\BEDEWEB	\\BEDEWEB	1	PABLO SOSA	BE	MONITOREO	PERMANENTE	\\BEDEWEB
ACDMINISTRADOR DE ANCHO DE BANDA		X	98	https:\\NetExplorer	https:\\NetExplorer	1	RUBEN CONRADO - DIEGO SOTOMAYOR	TOTALTEK S.A.	MONITOREO	PERMANENTE	https:\\NetExplorer
ACTIVE DIRECTORY		X	98	\\UIO03DC	\\UIO03DC	1	RAUL ENDARA - RUBEN CONRADO	BE	MONITOREO	PERMANENTE	\\UIO03DC
CORREO ELECTRÓNICO		X	98	\\UIOCORREO FortiMail: https://192.168.7.50/admin/	\\UIOCORREO FortiMail: https://192.168.7.50/admin/	1	RAUL ENDARA	BE	MONITOREO	PERMANENTE	\\UIOCORREO FortiMail: https://192.168.7.50/admin/
TELEFÓNIA IP		X	98	\\TARIFADOR1	\\TARIFADOR1	1	RUBEN CONRADO	TELALCA	MONITOREO / MANTENIMIENTO PREVENTIVO / CORRECTIVO DE HW	PERMANENTE	\\TARIFADOR1
VIDEOCONFERENCIA		X	98	HTTP://VIDEO.BANCOESTADO.COM	HTTP://VIDEO.BANCOESTADO.COM	1	JORGE ESPINOSA / RUBEN CONRADO / CATALINA BURGOS	BE	MANTENIMIENTO PREVENTIVO / CORRECTIVO DE HW	PERMANENTE	HTTP://VIDEO.BANCOESTADO.COM
ANTIVIRUS		X	98	\\uioservicios\antivirus	\\uioservicios\antivirus	1	RAUL ENDARA	BE	MANTENIMIENTO PREVENTIVO / CORRECTIVO DE HW	PERMANENTE	\\uioservicios\antivirus

HELP DESK		X	98	http://uiow01lin/HelpDesk	http://uiow01lin/HelpDesk	1	JOSE LUIS MUÑOZ - GARY CASTILLO	SOFTWARE LIBRE	MANTENIMIENTO PREVENTIVO / CORRECTIVO DE HW	PERMANENTE	http://uiow01lin/HelpDesk
IMPRESIÓN Y FOTOCOPIADO		X	98	CONSOLA DE INPRESIÓN EN \\UIOSERVICIOS	CONSOLA DE INPRESIÓN EN \\UIOSERVICIOS	1	MAURICIO MOLINEROS	MAURICIO MOLINEROS SONDA S.A.	MONITOREO DEL SISTEMA	PERMANENTE	CONSOLA DE INPRESIÓN EN \\UIOSERVICIOS
BPM		X	98	BMP STUDIO / PROCESS ADMINTRATOR / ULTIMUS CLIENT	BMP STUDIO / PROCESS ADMINTRATOR / ULTIMUS CLIENT	1	PABLO SOSA	PROPARTNER	MONITOREO Y MANTENIMIENTO	PERMANENTE	BMP STUDIO / PROCESS ADMINTRATOR / ULTIMUS CLIENT
BASES DE DATOS		X	98	\\UIO02APP	\\UIO02APP	1	FABIAN ANALUISA	BE	MONITOREO Y MANTENIMIENTO	PERMANENTE	\\UIO02APP

3.1.1.2. Identificar amenazas

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

Para poder analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir de las más diversas fuentes, a continuación se detallan las principales amenazas levantas:

TIPO DE DESASTRE	POSIBLES QUITO/MATRIZ	POSIBLES GUAYAQUIL	POSIBLES MANABI	POSIBLES LOJA	POSIBLES CUENCA
DESATRES NATURALES					
Huracanes					
Inundaciones		X			X
Incendios	X	X	X	X	X
Deslizamientos					
Terremotos	X	X	X	X	X
Erupciones volcánicas	X	X		X	X
DAÑOS ACCIDENTALES O FORTUITOS					
Caídas totales de los servicios	X	X	X	X	X
Caídas parciales de los servicios	X	X	X	X	X
Fuego fortuito	X	X	X	X	X
Inundaciones	X	X	X	X	X
Fallo del aire acondicionado	X	X	X	X	X
Exceso de humedad		X	X		
Humo, gases tóxicos	X	X	X	X	X
Variación de voltaje	X	X	X	X	X
Fallo de suministro eléctrico	X	X	X	X	X
Fallo de la UPS	X	X	X	X	X
Accidentes del personal	X	X	X	X	X
Capacidad inadecuada de las comunicaciones	X	X	X	X	X
Fallo/degradación del hardware	X	X	X	X	X
Fallo/degradación de las comunicaciones	X	X	X	X	X

Errores de operación	X	X	X	X	X
Fallos en las copias de seguridad	X	X	X	X	X
Fallos de los sistemas de autenticación/autorización	X	X	X	X	X
Pérdida de confidencialidad	X	X	X	X	X
Replicación base de datos	X	X	X	X	X
Incumplimientos legales					
ATAQUES INTENCIONADOS					
Actos de terrorismo	X	X	X	X	X
Fuego intencionado	X	X	X	X	X
Accesos físicos no autorizados al centro de cómputo	X	X	X	X	X
Actos de vandalismo	X	X	X	X	X
Radiaciones electromagnéticas					
Robos intencionados	X	X	X	X	X
Manipulación malintencionada de datos/software	X	X	X	X	X
Manipulación malintencionada de hardware	X	X	X	X	X
Uso de software por personal no autorizado	X	X	X	X	X
Acceso no autorizados a datos	X	X	X	X	X
Software malicioso	X	X	X	X	X
Robo de equipos	X	X	X	X	X
Robo de documentos	X	X	X	X	X
Robo de software	X	X	X	X	X
Descarga de software no controlada	X	X	X	X	X
Interceptación de las líneas de comunicación	X	X	X	X	X
Manipulación de las líneas de comunicación	X	X	X	X	X
Abuso de privilegios de acceso a los sistemas	X	X	X	X	X
Introducción de virus en los sistemas	X	X	X	X	X
Troyanos	X	X	X	X	X

Ataques por ingeniería social	X	X	X	X	X
Bombas lógicas	X	X	X	X	X
Ataques de denegación de servicio	X	X	X	X	X
Errores intencionados	X	X	X	X	X
Copias incontroladas de documentos/software/datos	X	X	X	X	X
Errores en el mantenimiento	X	X	X	X	X
Plan anual de HW actualizada	X	X	X	X	X
Corrupción de datos	X	X	X	X	X
Incumplimientos legales intencionados					

3.1.1.3. 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 institución. Por cada amenaza se detallan los posibles escenarios a presentarse y el nivel de protección de los mismos; a continuación se detallan las siguientes vulnerabilidades:

LISTADO DE AMENAZAS	ESCENARIOS	NIVEL DE PROTECCIÓN (PREGUNTA)	RESPUESTA (SI/NO)
DESASTRES NATURALES			
Inundaciones	Ubicación física del centro de cómputo en un área susceptible de desastres naturales fluviales	¿El centro de cómputo está alejado de área cerca de ríos o en las plantas medias o superiores del edificio?	SI
Incendios	Ausencia de un sistema de extinción automática de fuegos/humos	¿Existe sistema contra incendios?	SI
	Existencia de materiales inflamables como papel o cajas	¿Existe sistema contra incendios?	SI

	Ausencia de mantenimiento	¿Se le da mantenimiento al sistema?	SI
	Mantenimiento inapropiado del servicio técnico	¿Se le da mantenimiento al sistema por técnicos calificados?	SI
Deslizamientos	Ubicación física del centro de cómputo en un área susceptible de desastres ocasionados por desprendimiento de tierras	¿El centro de cómputo está alejado de área cercana a montañas o peñas en los que existan posibles desprendimientos de tierra?	SI
Terremotos	Ubicación física del centro de cómputo en un área susceptible de desastres naturales	¿El centro de cómputo está construido con estructura antisísmica?	SI
Erupciones volcánicas	Ubicación física en un área susceptible de desastres naturales	¿El centro de cómputo está alejado de área cerca de volcanes en riesgo de erupción o en las plantas medias o superiores del edificio?	SI
DAÑOS ACCIDENTALES O FORTUITOS			
Caídas totales de los servicios	Ausencia o suspensión total de los servicios de la plataforma tecnológica (red, internet, correo electrónico, impresoras, telefonía, sistemas internos)	¿Existe monitoreo permanente de los servicios y aplicaciones?	SI
	Personal suficiente para resolver todos los problemas que se presenten en los servicios y aplicaciones	¿Existe el personal suficiente para atender las caídas de servicios y aplicaciones?	NO
	Proveedores alternos de servicios	¿Existen proveedores alternos de servicios?	SI
	Planes o procedimientos de resolución de incidentes	¿Existen planes o procedimientos de resolución de incidentes?	SI
Caídas parciales de los servicios	Ausencia o suspensión parcial de los servicios de la plataforma tecnológica	¿Existe monitoreo permanente de los servicios y	SI

	(red, internet, correo electrónico, impresoras, telefonía, sistemas internos)	aplicaciones?	
	Proveedores alternos de servicios	¿Existen proveedores alternos de servicios?	SI
	Planes o procedimientos de resolución de incidentes	¿Existen planes o procedimientos de resolución de incidentes?	SI
	Personal suficiente para resolver todos los problemas que se presenten en los servicios y aplicaciones	¿Existe el personal suficiente para atender las caídas de servicios y aplicaciones?	NO
Fuego fortuito	Ausencia de un sistema de extinción automática de fuegos/humos	¿Existe sistema contra incendios?	SI
	Existencia de materiales inflamables como papel o cajas	¿Existe sistema contra incendios?	SI
	Ausencia de mantenimiento	¿Se le da mantenimiento al sistema?	SI
Inundaciones	Ubicación física en un área susceptible de accidentes hidráulicos.	¿El centro está ubicado en un área segura, protegida de sistemas hidráulicos?	SI
Fallo del aire acondicionado	Ausencia de mantenimiento del sistema de aire acondicionado	¿Se realiza mantenimiento periódico al sistema de aire acondicionado?	SI
	Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento?	SI
Exceso de humedad	Mala construcción del edifico o centro de cómputo	¿La construcción donde se ubica el centro de cómputo cumple con los estándares de construcción?	SI
Humo, gases tóxicos	Centro de cómputo no es suficientemente hermético	¿La construcción es hermético?	SI

Variaciones de voltaje	Las instalaciones eléctricas son inadecuadas generando variaciones de voltaje	¿El sistema eléctrico es regulado y protegido por un sistema de UPS?	SI
Fallo de suministro eléctrico	Ausencia de mantenimiento	¿Se brinda mantenimiento periódico al sistema eléctrico?	SI
	Cableado inapropiado	¿Se instaló un sistema eléctrico confiable?	SI
	Suministro eléctrico inapropiado	¿Se instaló un suministro eléctrico confiable?	SI
	Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento?	SI
Fallo de la UPS	Ausencia de mantenimiento	¿Se brinda mantenimiento periódico al UPS?	SI
	Cableado inapropiado	¿Se instaló un sistema equipo confiable?	SI
	Espacio físico no es óptimo para el funcionamiento de los equipos	¿El área de UPS cumple con los estándares de funcionamiento?	NO
	Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal técnico calificado para mantenimiento?	SI
Accidentes del personal	Centro de cómputo propenso a accidentes de personal	¿Existe en el centro de cómputo seguridades para evitar accidentes del personal?	SI
Capacidad inadecuada de las comunicaciones	Ausencia de mantenimiento	¿Se brinda mantenimiento periódico al sistema de comunicaciones?	SI
	Ancho de banda inapropiado	¿Se dispone de un adecuado ancho de banda para uso de las comunicaciones?	SI
Fallo/degradación del hardware	Ausencia de mantenimiento	¿Se brinda mantenimiento periódico al hardware?	SI
	Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento de	SI

		hardware?	
Fallo/degradación de las comunicaciones	Ausencia de mantenimiento	¿Se brinda mantenimiento periódico al sistema de comunicaciones?	SI
	Cableado inapropiado	¿Se instaló cableado estructurado certificado?	SI
	Proveedor del sistema de comunicaciones no confiable	¿El proveedor de comunicaciones cumple con los niveles de servicio establecidos?	SI
	Caída enlaces principales de comunicaciones con sucursales	¿Existe líneas de backup instaladas con diferente proveedor?	SI
	Ancho de banda inapropiado	¿Se provisionó un adecuado ancho de banda para uso de las comunicaciones?	SI
	Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento de comunicaciones?	SI
Errores de operación	Personal técnico inexperto y con falta de conocimiento	¿Cuenta con personal calificado para los procesos operativos?	SI
	Falta de documentación de los procesos de operación y configuración?	¿Cuenta con los manuales técnicos de operación y configuración actualizados?	SI
Fallos en las copias de seguridad	Ancho de banda inapropiado	¿Se provisionó un adecuado ancho de banda para uso de las comunicaciones?	SI
	Personal técnico inexperto y con falta de conocimiento en el proceso de copias de seguridad	¿Cuenta con personal calificado para los procesos de respaldo?	SI

	Falta de documentación de los procesos de administración de respaldos de información y copias de seguridad?	¿Cuenta con los manuales técnicos de administración de respaldos y manuales copias de seguridad actualizados?	SI
Fallos de los sistemas de autenticación/autorización	Personal no calificado para la operación del sistema de autentificación y autorización	¿Cuenta con personal calificado para la operación del sistema de autentificación y autorización?	SI
Pérdida de confidencialidad	Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales	¿Existen mecanismos de transmisión de cifrado de datos?(cifrado parcial)	SI
Incumplimientos legales	Falta de auditorías por parte de los entes de control?	¿Se realizan auditorías periódicas para evaluar el cumplimiento de normas y procedimientos?	SI
	El software no se encuentra legalizado	¿El software instalado cuenta con las licencias de uso respectivas?	SI
ATAQUES INTENCIONADOS			
Terrorismo	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso al centro de cómputo?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso al centro de cómputo?	SI
Fuego intencionado	Ausencia de un sistema de extinción automática de fuegos/humos	¿Existe sistema contra incendios?	SI
	Existencia de materiales inflamables como papel o cajas	¿Existe sistema contra incendios?	SI
	Ausencia de mantenimiento	¿Se le da mantenimiento al	SI

		sistema?	
	Mantenimiento inapropiado del servicio técnico	¿Se le da mantenimiento adecuado y periódico al sistema?	SI
	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso al centro de cómputo?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso al centro de cómputo?	SI
Accesos físico no autorizados al centro de cómputo	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso físicos al centro de cómputo?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso físicos al centro de cómputo?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso al centro de cómputo?	SI
Actos de vandalismo	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI

	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso al centro de cómputo?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso al centro de cómputo?	SI
Robos intencionados	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso al centro de cómputo?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso al centro de cómputo?	SI
	Protección física de equipos inadecuada	¿Existe protección en el edificio y centro de cómputo que impida el robo de equipos?	SI
Manipulación malintencionada de datos/software	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas	SI

		informáticos?	
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
	Ausencia de política de restricción de personal para uso licencias de software	¿Existen políticas de restricción de personal para uso licencias de software?	SI
	Política de seguridad de la información inadecuada	¿Existen políticas de seguridad de la información inadecuada?	SI
Manipulación de hardware	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los equipos informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los equipos informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los equipos informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los equipos informáticos?	SI
	Protección física de equipos inadecuada	¿Existe protección en el edificio y centro de cómputo que impida el robo de equipos?	SI
Uso de software por personal no autorizado	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas	SI

		informáticos?	
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
	Ausencia de política de restricción de personal para uso licencias de software	¿Existen políticas de restricción de personal para uso licencias de software?	SI
Acceso no autorizados a datos	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los datos de los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los datos de los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los datos de los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los datos de los sistemas informáticos?	SI
	Políticas de firewall inadecuadas	¿Existen en el área políticas de firewall que protejan la seguridad de la red de datos?	SI
Software malicioso	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas	SI

		informáticos?	
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
Robo de equipos	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los equipos informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los equipos informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los equipos informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los equipos informáticos?	SI
	Protección física de equipos inadecuada	¿Existe protección en el edificio y centro de cómputo que impida el robo de equipos?	SI
Robo de documentos	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso al centro de cómputo?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso al centro de	SI

		cómputo?	
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso al centro de cómputo?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso al centro de cómputo?	SI
Robo de software	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
Descarga de software no controlada	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de descarga de sw en los sistemas informáticos ?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de descarga de sw en los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de descarga de sw en los sistemas informáticos?	SI

	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para descarga de sw en los sistemas informáticos?	SI
	Descarga incontrolada y uso de software de Internet	¿Existen políticas de restricción de personal para descargas de software e internet?	SI
Interceptación de las líneas de comunicación	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los equipos de comunicaciones?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los equipos de comunicaciones?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los equipos de comunicaciones?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los equipos de comunicaciones?	SI
	Políticas de firewall inadecuadas	¿Existen en el área políticas de firewall que protejan la seguridad de la red de datos?	SI
Manipulación de las líneas de comunicación	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los equipos de comunicaciones?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los equipos de comunicaciones?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los equipos de comunicaciones?	SI

	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los equipos de comunicaciones?	SI
	Políticas de firewall inadecuadas	¿Existen en el área políticas de firewall que protejan la seguridad de la red de datos?	SI
Abuso de privilegios de acceso a los sistemas	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
Introducción de virus en los sistemas y troyanos	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI

	Educación inadecuada del personal en virus y malware	¿Cuenta con personal calificado en conocimiento de antivirus?	SI
	Carencia de software antivirus	¿Se cuenta con software antivirus?	SI
	Políticas de firewall inadecuadas	¿Existen en el área políticas de firewall que protejan la seguridad de la red de datos?	SI
Ataques por ingeniería social	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
	Falta de concientización e información al usuario sobre mecanismos de ataques por ingeniería social	¿Se realizan campañas para concientización e información al usuario sobre mecanismos de ataques por ingeniería social?	SI
	Políticas de firewall inadecuadas	¿Existen en el área políticas de firewall que protejan la seguridad de la red de datos?	SI
Bombas lógicas	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI

	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
Ataques de denegación de servicio	Ausencia de backup	¿Existen políticas de backup para proteger los datos, los sistemas y las comunicaciones?	SI
	Ausencia de un Plan de recuperación de incidentes	¿Existe Plan de Recuperación de incidentes?	SI
Errores intencionados	Ausencia de backup	¿Existen políticas de backup para proteger los datos?	SI
Copias incontroladas de documentos/software/datos	Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Derechos de acceso incorrectos	¿Existen políticas para otorgar derechos de acceso a los sistemas informáticos?	SI
	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas informáticos?	SI
	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autentificación para el acceso a los sistemas informáticos?	SI
	Política de seguridad de la información inadecuada	¿Existen políticas de seguridad de la información inadecuada?	SI

Errores en el mantenimiento	Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento del centro de cómputo en general?	SI
Plan anual de HW actualizado	Política de actualización de HW periódica	¿Se cumple con cronograma de adquisiciones?	SI
Corrupción de datos	Ausencia de backup	¿Existen políticas de backup para evitar la corrupción de los datos?	SI
	Ausencia de un Plan de recuperación de incidentes	¿Existe Plan de Recuperación de incidentes?	SI

3.1.1.4. Evaluación de impactos

Por cada incidente que se suscite en la infraestrcutura tecnológica del Banco del Estado se produce un impacto; a continaución se detallan los principales impactos:

3.1.1.4.1. Cuadro de Procesos

Proceso	Breve descripción	Subproceso	Frecuencia (Diario/Semanal/ Mensual)	Responsable
INGRESAR Y ANALIZAR SOLICITUD DE CRÉDITO	Registrar en los sistemas institucionales el requerimiento del financiamiento del crédito; así como, revisar y analizar si la solicitud presentada está dentro de los sectores que financia el Banco; y, si cumple con los requisitos necesarios para la entrega del financiamiento	Registrar y analizar solicitud	Semanal	• Grupo de Evaluación • Coordinación de Asistencia Técnica
EFECTUAR EVALUACIÓN DEL CRÉDITO	Analizar y evaluar los diferentes aspectos que permiten verificar la viabilidad del proyecto a ser financiado por el BDE, de manera que cumpla con los requerimientos de ley y políticas de Financiamiento del BDE	Analizar requisitos para evaluación	Semanal	• Grupo de Evaluación de cada Sucursal Regional • Comité de Crédito de cada Sucursal
		Efectuar evaluación técnica		
		Efectuar evaluación ambiental		
		Efectuar evaluación de participación comunitaria		
		Efectuar evaluación económica		
		Analizar gestión de servicio		
		Efectuar evaluación financiera		
		Analizar legalmente al crédito		
		Consolidar informe de evaluación		

APROBAR OPERACIÓN DE FINANCIAMIENTO	Tomar conocimiento del proyecto y examinar el Informe de Evaluación de Crédito por parte de la autoridad competente para la aceptación y aprobación del crédito solicitado	Calificar operación de financiamiento	Semanal	• Gerente de Sucursal • Gerente General • Presidente del Directorio • Comité de Crédito de Matrizo Sucursales • Grupo de Evaluación • Secretaría General
		Aprobar operación de financiamiento		
LEGALIZAR CRÉDITO	Inscribir la condición de deuda pública del crédito otorgado por el Banco del Estado, para legalizar el Contrato de Crédito y Fideicomiso	Elaborar y formar contrato de crédito y fideicomiso	Semanal	• Comité y Secretaría de Crédito de Sucursal o Matriz • Grupo de Evaluación
EFECTUAR SEGUIMIENTO DEL CRÉDITO	Coordinar con las prestatarias el cumplimiento de las condicionantes de crédito y de los términos contractuales, en lo que tiene que ver con los aspectos técnicos y financieros del financiamiento entregado por el Banco del Estado; y, verificar que los recursos se destinen para el objeto para el que fueron previstos	Realizar seguimiento del crédito	Diario	• Grupo de seguimiento • Áreas del Banco
		Efectuar trámites de operación de crédito	Semanal	
EFECTUAR DESEMBOLSO DEL CRÉDITO	Realizar la operación del crédito de acuerdo con las políticas institucionales y condicionantes particulares de cada financiamiento, entregar los recursos que el Banco dispone para colocación de créditos	Elaborar informe de desembolso	Diario	• Grupo de seguimiento • Desembolso
		Aprobar desembolsos	Diario	• Gerente de Sucursal
		Entregar recursos	Semanal	• Coordinación Administrativa Financiera de Sucursales (Cartera, contabilidad, pagaduría)

3.1.1.4.2. Cuadro de sistemas que soporta cada proceso

Proceso	Subproceso	Nombre del Sistema	Criticidad	Tipo de Sistema (PC/Servidor/ Mainframe)	Nº de Equipos con la aplicación	Responsable	Contacto Técnicos
INGRESAR Y ANALIZAR SOLICITUD DE CREDITO	Registrar y analizar solicitud	SIC/REGYCONT/CORREO ELECTRONICO/ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
EFECTUAR EVALUACION DEL CREDITO	Analizar requisitos para evaluación	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC/ ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
	Efectuar evaluación técnica	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC/ UTIMUS BPM	2	Servidor/PC	10	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800
	Efectuar evaluación ambiental	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC/ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800
	Efectuar evaluación de participación comunitaria	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC/ ULTIMUS BPM	2	Servidor/PC	50	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800

	Efectuar evaluación económica	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC/ ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800
	Analizar gestión de servicio	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC/ ULTIMUS BPM	2	PC	10	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800
	Efectuar evaluación financiera	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC / ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800
	Analizar legalmente al crédito	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC / ULTIMUS BPM	2	PC	10	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800
	Consolidar informe de evaluación	SIC/REGYCONT/SIMWEB/SICEND/CORREO ELECTRONICO/INTERNET/ MS OFFICE/PROPLAN/VOC / ULTIMUS BPM	2	PC	10	César García/ Rodolfo Escobar/Santiago Flores/ Raúl Endara / Pablo Sosa	1800
APROBAR OPERACIÓN DE FINANCIAMIENTO	Calificar operación de financiamiento	SIC/REGYCONT/CORREO ELECTRONICO/INTERNET/ MS OFFICE / ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800

	Aprobar operación de financiamiento	SIC/REGYCONT/CORREO ELECTRONICO/INTERNET/ MS OFFICE / ULTIMUS BPM	1	Servidor/PC	100	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
LEGALIZAR CRÉDITO	Elaborar y formar contrato de crédito y fideicomiso	SIC/REGYCONT/CORREO ELECTRONICO/INTERNET/ MS OFFICE / ULTIMUS BPM	1	PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
EFECTUAR SEGUIMIENTO DEL CRÉDITO	Realizar seguimiento del crédito	SIC/REGYCONT/CORREO ELECTRONICO/INTERNET/ MS OFFICE / ULTIMUS BPM	1	PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
	Efectuar trámites de operación de crédito	SIC/REGYCONT/CORREO ELECTRONICO/INTERNET/ MS OFFICE / ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
EFECTUAR DESEMBOLSO DEL CRÉDITO	Elaborar informe de desembolso	SIC/REGYCONT/CGWEB/CORREO ELECTRONICO/INTERNET / ULTIMUS BPM	1	PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
	Aprobar desembolsos	SIC/REGYCONT/CGWEB/CORREO ELECTRONICO/INTERNET/ ULTIMUS BPM	1	Servidor/PC	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800
	Entregar recursos	SIC/REGYCONT/CGWEB/CORREO ELECTRONICO/INTERNET / ULTIMUS BPM	1	Servidor	50	César García/ Rodolfo Escobar/ Raúl Endara / Pablo Sosa	1800

Rangos de Criticidad:

1 – El proceso no puede ejecutarse sin el sistema

2 – El proceso puede ejecutarse parcialmente sin el sistema

3 - El proceso puede ejecutarse sin el sistema

3.1.1.4.3. Cuadro de Procesos del Negocio y servicios de tecnología

PROCESO	SUBPROCESO	SERVICIOS DE RED																	CRITICIDAD
		LAN	WAN		WIRELLES				INTERNET		DIRECTORIO ACTIVO	CORREO ELECTRÓNICO	TELEFONÍA IP	VIDEO CONFERENCIA	AUTENTICACIÓN FORTIGATE	ANTISPAM FORTIGATE	MESA DE AYUDA	SPI / SPL	
			PRINCIPAL	ALTERNO	CHASQUI	SMART PHONES	GUESS	CHULPI	PRINCIPAL	ALTERNO									
INGRESAR Y ANALIZAR SOLICITUD DE CREDITO	Registrar y analizar solicitud	X	X	X	X				X	X	X	X	X		X	X	X		1
EFECTUAR EVALUACION DEL CREDITO	Analizar requisitos para evaluación	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
	Efectuar evaluación técnica	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3

	Efectuar evaluación ambiental	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
	Efectuar evaluación de participación comunitaria	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
	Efectuar evaluación económica	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
	Analizar gestión de servicio	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
	Efectuar evaluación financiera	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
	Analizar legalmente al crédito	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
	Consolidar informe de evaluación	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
APROBAR OPERACIÓN DE FINANCIAMIENTO	Calificar operación de financiamiento	X	X	X	X				X	X	X	X	X	X	X	X	X		1
	Aprobar operación de financiamiento	X	X	X	X				X	X	X	X	X		X	X	X		1

LEGALIZAR CRÉDITO	Elaborar y formar contrato de crédito y fideicomiso	X	X	X	X		X	X	X	X	X	X	X		X	X	X		3
EFECTUAR SEGUIMIENTO DEL CRÉDITO	Realizar seguimiento del crédito	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X		2
	Efectuar trámites de operación de crédito	X	X	X	X		X	X	X	X	X	X	X		X	X	X		1
EFECTUAR DESEMBOLSO DEL CRÉDITO	Elaborar informe de desembolso	X	X	X	X				X	X	X	X	X		X	X	X		1
	Aprobar desembolsos	X	X	X	X				X	X	X	X	X		X	X	X	X	1
	Entregar recursos	X	X	X	X				X	X	X	X	X		X	X	X	X	1

Rangos de Criticidad:

1 – El proceso no puede ejecutarse sin el hardware

2 – El proceso puede ejecutarse parcialmente sin el hardware

3 – El proceso puede ejecutarse sin el hardware

3.1.1.4.4. Cuadro de Registro de Hardware de cada proceso

Proceso	Subproceso	Tipo de hardware	Detalles del Modelo/Configuración	Proveedor	Criticidad	Localización
INGRESAR Y ANALIZAR SOLICITUD DE CREDITO	Registrar y analizar solicitud	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE INTEL CORE I7	DBSG / DSI	1	Todas Sucursales BDE
EFECTUAR EVALUACION DEL CREDITO	Analizar requisitos para evaluación	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Efectuar evaluación técnica	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Efectuar evaluación ambiental	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Efectuar evaluación de participación comunitaria	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Efectuar evaluación económica	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Analizar gestión de servicio	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Efectuar evaluación financiera	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Analizar legalmente al crédito	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Consolidar informe de evaluación	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
APROBAR OPERACIÓN DE FINANCIAMIENTO	Calificar operación de financiamiento	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Aprobar operación de financiamiento	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
LEGALIZAR CRÉDITO	Elaborar y formar contrato de crédito y fideicomiso	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
EFECTUAR SEGUIMIENTO DEL CRÉDITO	Realizar seguimiento del crédito	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Efectuar trámites de operación de crédito	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE

EFECTUAR DESEMBOLSO DEL CRÉDITO	Elaborar informe de desembolso	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Aprobar desembolsos	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE
	Entregar recursos	PC ESCRITORIO / PORTABLE	PC ESCRITORIO/PORTABLE	DBSG / DSI	1	Todas Sucursales BDE

Rangos de Criticidad:

1 – El proceso no puede ejecutarse sin el hardware

2 – El proceso puede ejecutarse parcialmente sin el hardware

3 **–**El proceso puede ejecutarse sin el hardware

3.1.1.4.5. Cuadro de Tiempo máximo de interrupción de los procesos

Proceso	Subproceso	Necesidades de Recuperación	Criticidad
INGRESAR Y ANALIZAR SOLICITUD DE CREDITO	Registrar y analizar solicitud	DIA 1-7	2
EFECTUAR EVALUACION DEL CREDITO	Analizar requisitos para evaluación	DIA 1-7	2
	Efectuar evaluación técnica	DIA 1-7	2
	Efectuar evaluación ambiental	DIA 1-7	2
	Efectuar evaluación de participación comunitaria	DIA 1-7	2
	Efectuar evaluación económica	DIA 1-7	2
	Analizar gestión de servicio	DIA 1-7	2
	Efectuar evaluación financiera	DIA 1-7	2
	Analizar legalmente al crédito	DIA 1-7	2
	Consolidar informe de evaluación	DIA 1-7	2
APROBAR OPERACIÓN DE FINANCIAMIENTO	Calificar operación de financiamiento	DIA 1-7	1
	Aprobar operación de financiamiento	DIA 1-7	1
LEGALIZAR CRÉDITO	Elaborar y formar contrato de crédito y fideicomiso	DIA 1-7	1
EFECTUAR SEGUIMIENTO DEL CRÉDITO	Realizar seguimiento del crédito	DIA 1-7	2
	Efectuar trámites de operación de crédito	DIA 1-7	2
EFECTUAR DESEMBOLSO DEL CRÉDITO	Elaborar informe de desembolso	DIA 1-7	1
	Aprobar desembolsos	DIA 1-7	1
	Entregar recursos	DIA 1-7	1

Necesidad de Recuperación:

Día 0 : Recuperación inmediata

Día 1-7: El proceso debe ser recuperado entre el primer y el quinto día después de un incidente.

Día 7–30: El proceso debe ser recuperado después de la primera semana y antes de un mes.

Más 30 días: El proceso pude esperar más de 30 días a ser recuperado.

Rangos de Criticidad:

1. La organización/departamento no puede funcionar sin el sistema
2. La organización/departamento no puede funcionar parcialmente sin el sistema
3. La organización/departamento puede funcionar sin el sistema

Para este caso de estudio se ha definido realizar la cuantificación económica del proceso de **"EVALUACION DEL CREDITO"** para analizar el impacto económico que implica el no contar con este proceso en caso de un fallo en las tecnologías de información que apalancan este proceso. Para este propósito se utilizará la fórmula planteada en el capítulo 2, en el numeral 2.1.2.4. y se tomará como ejemplo el no contar un día completo con el sistema de evaluación de crédito.

RIESGO (componente) = P * V

Riesgo (**INGRESAR Y ANALIZAR SOLICITUD DE CREDITO) = 20000 *1 = $20000**

Riesgo **(EFECTUAR EVALUACION DEL CREDITO) = 30000*1 = $30000**

Riesgo **(APROBAR OPERACIÓN DE FINANCIAMIENTO) = 20000*2 = $40000**

Riesgo **(LEGALIZAR CRÉDITO) = 20000 * 1 = $20000**

Riesgo **(EFECTUAR SEGUIMIENTO DEL CRÉDITO) = 15000* 1 = $15000**

Riesgo **(EFECTUAR DESEMBOLSO DEL CRÉDITO) = 30000* 2 = $60000**

RIESGO TOTAL= RIESGO (componente 1) + RIESGO (componente 2)...

RIESGO TOTAL= 20000 + 30000 + 40000 + 20000 + 15000 + 60000

RIESGO TOTAL= $185000

Como se puede apreciar el costo operativo de no contar con el proceso crediticio del Banco es de aproximadamente 185000 diarios, sin embargo este valor puede aumentar dependiendo el tipo de crédito que se desea financiar estos datos fueron proporcionados por el departamento de crédito de la entidad y se basó en un promedio de transacciones del mes de mayo del 2014.

3.1.1.5. Evaluación de Riesgo

Basados en la matriz probabilidad / impacto del capítulo 2, se detalla a continuación los riesgos de los que pueden estar sujetos los sistemas de información del Banco del Estado, con su valor de acuerdo a la probabilidad de ocurrencia y su respectivo impacto:

DESCRIPCIÓN	PROBABILIDAD	IMPACTO	RIESGO
Fallo total de los servicios	M	A	RA
Fallo parcial de los servicios	M	A	RA
Incendios / Fuego Fortuito	M	A	RA
Terremotos	B	A	RM
Erupciones volcánicas	M	B	RB
Fallo del aire acondicionado	B	M	RB
Exceso de humedad	B	B	RB
Humo, gases tóxicos	B	B	RB
Variaciones de tensión	B	B	RB
Fallo de suministro eléctrico	M	B	RB
Fallo de la UPS	A	A	RA
Accidentes del personal	B	B	RB
Capacidad inadecuada de las comunicaciones	B	M	RB
Fallo/degradación del hardware	B	M	RB
Fallo/degradación de las comunicaciones	M	A	RA
Errores de operación	B	A	RM
Fallos en las copias de seguridad	B	A	RM
Fallos de los sistemas de autenticación/autorización	B	A	RM
Pérdida de confidencialidad	B	B	RB
Vencimientos de contratos no controlados	M	A	RA
Actos de terrorismo	B	A	RM
Accesos no autorizados a la institución	A	M	RA
Accesos no autorizados al centro de cómputo	B	A	RM
Fuego intencionado	B	A	RM
Actos de vandalismo	B	M	RB
Robos intencionados	B	M	RB
Manipulación malintencionada de datos/software	B	A	RM

Manipulación malintencionada de hardware	B	A	RM
Uso de software por personal no autorizado	B	M	RB
Acceso no autorizados a datos de la empresa	B	B	RB
Software malicioso	B	M	RB
Robo de equipos	B	M	RB
Robo de documentos	B	M	RB
Robo de software	B	B	RB
Descarga de software no controlada	B	A	RM
Interceptación de las líneas de comunicación	B	B	RB
Manipulación de las líneas de comunicación	B	A	RM
Abuso de privilegios de acceso	B	M	RB
Introducción de virus en los sistemas y troyanos	B	A	RM
Ataques por ingeniería social	A	A	RA
Bombas lógicas	M	A	RA
Ataques de denegación de servicio	A	M	RA
Errores intencionados	B	M	RB
Copias incontroladas de documentos/datos	A	M	RA
Copias incontroladas de software	B	M	RB
Errores en el mantenimiento	B	A	RM
Corrupción de datos	B	A	RM
HW Desactualizado	B	M	RB

3.1.1.6. Evaluar Contramedidas

Basados en los tres tipos de controles preventivos, detectivos y correctivos que fueron explicados en el capítulo 2, se detalla a continuación los controles utilizados para mitigar riesgos que previamente fueron levantados en el punto 3.1.1.3 en las TIs del Banco del Estado.

RIESGOS	RIESGOS	CONTROLES PREVENTIVOS / CORRECTIVOS	CONTROLES DETECTIVOS	ACCIONES CORRECTIVAS
Incendios	RA	Instalar un sistema de extinción automática de fuegos/humos	Sensores de humo	Recuperación de activos y datos perdidos
		Desalojar el centro de cómputo de papel o cajas	Monitoreo de eventos	
		Dar mantenimiento al sistema de incendios	Revisar los contratos de mantenimiento y el tiempo medio de servicio acordados con el proveedor con objeto de obtener una cifra de control constante	
		Contratar con una empresa especializada en mantenimiento del sistema de incendios		
		Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo		
		Establecer procedimientos / políticas de seguridad y prevención de incendios		
Terremotos	RM	Disponer de un centro de cómputo alterno	Monitoreo de eventos/fallas	Habilitar centro de cómputo afectado
Erupciones volcánicas	RB	Disponer de un centro de cómputo alterno	Monitoreo de eventos/fallas	Habilitar centro de cómputo afectado
Fallo Total de los Servicios	RA	Realizar controles diarios de servicios	Monitoreo de eventos/fallas	Mantener un registro documental de las acciones de monitore realizadas, incluyendo la descripción del problema y la solución dada al mismo
		Revisar configuraciones en consolas de servicios no se hayan cambiado	Procesos que no se ejecutaron	Mantener bitácora de errores o fallas

		Realizar pruebas periódicas de conectividad, uso de red, consumo de ancho de banda, enlaces WAN y proveedores de servicios		Mantener bitácora de errores o fallas
Fallo Parcial de los Servicios	RA	Realizar controles diarios de servicios	Monitoreo de eventos/fallas	Mantener un registro documental de las acciones de monitoreo realizadas, incluyendo la descripción del problema y la solución dada al mismo
		Revisar configuraciones en consolas de servicios no se hayan cambiado	Procesos que no se ejecutaron	Mantener bitácora de errores o fallas
		Realizar pruebas periódicas de conectividad, uso de red, consumo de ancho de banda, enlaces WAN y proveedores de servicios		Mantener bitácora de errores o fallas
Fallo del aire acondicionado	RB	Instalar un sistema de aire acondicionado	Monitoreo de eventos	Recuperación de datos perdidos
		Dar mantenimiento al sistema de aire acondicionado	Revisar los contratos de mantenimiento y el tiempo medio de servicio acordados con el proveedor con objeto de obtener una cifra de control constante	Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo
		Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo		
		Establecer procedimientos / políticas de manejo, seguridad y mantenimiento en sistema de aire acondicionado		
Exceso de humedad	RB	Realizar copias de seguridad de los archivos	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de manejo de humedad		

Humo, gases tóxicos	RB	Construir centro de cómputo hermético	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de manejo de humo y gases tóxicos		
Variaciones de voltaje	RB	Instalar instalaciones eléctricas adecuadas para no generar variaciones de voltaje	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de manejo, seguridad y mantenimiento en variaciones de voltaje		
Fallo de suministro eléctrico	RB	Dar mantenimiento periódico al sistema eléctrico	Monitoreo de eventos/fallas	Reemplazar sistema eléctrico afectado
		Instalar cableado apropiado	Revisar los contratos de mantenimiento y el tiempo medio de servicio acordados con el proveedor con objeto de obtener una cifra de control constante	
		Establecer procedimientos / políticas de manejo, seguridad y mantenimiento en suministro eléctrico		
		Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo		
Fallo de la UPS	RA	Dar mantenimiento periódico al sistema eléctrico	Monitoreo de eventos/fallas	Reemplazar equipo afectado
		Instalar cableado apropiado	Revisar los contratos de mantenimiento y el tiempo medio de servicio acordados con el proveedor con objeto de obtener una cifra de control constante	
		Contratar seguros para los activos		
		Establecer procedimientos / políticas de manejo, seguridad y mantenimiento en UPS		

		Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo		
Accidentes del personal	RB	Crear centro de cómputo libre de accidentes de personal		
Capacidad inadecuada de las comunicaciones	RB	Establecer procedimientos / políticas de manejo y seguridad en comunicaciones	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer ancho de banda apropiado		
		Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación		
Fallo/degradación del hardware	RB	Mantenimiento preventivo de todos los equipos y componentes de la red	Monitoreo de eventos	Recuperación de datos perdidos
		Contratar seguros para los activos		
		Establecer procedimientos / políticas de manejo en HW		
Fallo/degradación de las comunicaciones	RA	Mantenimiento preventivo de todos los equipos y componentes de la red	Monitoreo de eventos/fallas/SLA	Levantar enlace principal
		Establecer procedimientos / políticas de manejo y seguridad en comunicaciones		
		Monitorización para medir la eficiencia de la red		
		Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación		
		Disponer de enlaces alternos		
Errores de operación	RM	Establecer procedimientos / políticas de operación del centro de cómputo	Monitoreo de eventos	Parches de seguridad
		Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación	Revisiones periódicas de procesos	Recuperación de datos perdidos
Fallos en las copias de seguridad	RM	Establecer procedimientos / políticas de copias de seguridad de datos	Monitoreo de eventos	Parches de seguridad

			Revisiones periódicas de procesos	Recuperación de datos perdidos
			Monitoreo de eventos	
			Detectar la correcta o mala recepción de mensajes	
Fallos de los sistemas de autenticación/autorización	RM	Revisión periódica de políticas de seguridad informática	Monitoreo de eventos	Instalar parches de seguridad
		Control de acceso a la red, establecimiento de perfiles de usuario.	Revisiones periódicas de procesos	
		Implementación de equipos de autenticación		
Pérdida de confidencialidad	RB	Establecer procedimientos / políticas de seguridad generales	Monitoreo de eventos	Recuperación de datos perdidos
Vencimientos de contratos no controlados	RA	Mantener registro de información de contratos	Establecer procedimientos de control	Renovar / iniciar procesos de contratación
Terrorismo	RM	Establecer procedimientos / políticas de seguridad generales	Monitoreo de eventos	Recuperación de datos perdidos
Accesos físicos no autorizados a la institución	RA	Establecer procedimientos / políticas de seguridad de ingreso al centro de cómputo	Revisiones periódicas de procesos	Corrección de daños por virus
Actos de vandalismo	RB	Establecer procedimientos / políticas de seguridad generales	Monitoreo de eventos	Recuperación de datos perdidos
Robos intencionados	RB	Existencia de inventario de todos los activos	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de seguridad generales		
Accesos físicos no autorizados al centro de cómputo	RM			
Manipulación malintencionada de datos/software	RM	Procedimientos de control del software contratado bajo licencia	Monitoreo de eventos	Parches de seguridad
		Controles de acceso a datos mediante clave		Recuperación de datos perdidos
		Control de acceso a la red, establecimiento de perfiles de usuario.		
		Existencia de inventario de todo el software		

		Establecer procedimientos / políticas de seguridad en datos y SW		
Manipulación malintencionada de hardware	RM	Existencia de inventario de todos los activos	Monitoreo de eventos	Parches de seguridad
		Establecer procedimientos / políticas de seguridad en HW		Recuperación de datos perdidos
Uso de software por personal no autorizado	RB	Normativas y procedimientos de desarrollo y adquisición de software de aplicaciones	Monitoreo de eventos	Parches de seguridad
		Establecer procedimientos / políticas de seguridad de uso de SW y licencias		Recuperación de datos perdidos
Acceso no autorizados a datos	RB	Controles de acceso a datos mediante clave	Monitoreo de eventos	Parches de seguridad
		Establecer mecanismos de identificación y autenticación	Revisiones periódicas de procesos	Recuperación de datos perdidos
		Control de acceso a la red, establecimiento de perfiles de usuario.		
		Establecer procedimientos / políticas de seguridad en acceso a datos		
Software malicioso	RB	Procedimientos de control del software contratado bajo licencia	Monitoreo de eventos	Parches de seguridad
		Controles de acceso a datos mediante clave		Corrección de daños por virus
		Normativas y procedimientos de desarrollo y adquisición de software de aplicaciones		Recuperación de datos perdidos
		Control de acceso a la red, establecimiento de perfiles de usuario.		
Robo de equipos	RB	Existencia de inventario de todos los activos	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de acceso y seguridad a los activos		
		Contratar seguros para los activos		

Robo de documentos	RB	Establecer procedimientos / políticas de acceso y seguridad a documentos	Monitoreo de eventos	Recuperación de datos perdidos
Robo de software	RB	Controles de acceso a datos mediante clave	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de acceso y seguridad al SW legalizado		
Descarga de software no controlada	RM	Controles de acceso a datos mediante clave	Revisiones periódicas de procesos	Parches de seguridad
		Control de acceso a la red, establecimiento de perfiles de usuario.	Monitoreo de eventos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de seguridad de descarga de SW		
Interceptación de las líneas de comunicación	RB	Control de acceso a la red, establecimiento de perfiles de usuario.	Monitoreo de eventos	Parches de seguridad
		Establecer procedimientos / políticas de seguridad en la red de datos y líneas de comunicación	Revisiones periódicas de procesos	Recuperación de datos perdidos
		Monitorización para medir la eficiencia de la red		
		Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación local		
Manipulación de las líneas de comunicación	RM	Control de acceso a la red, establecimiento de perfiles de usuario.	Monitoreo de eventos	Parches de seguridad
		Establecer procedimientos / políticas de seguridad en la red de datos y líneas de comunicación	Revisiones periódicas de procesos	Recuperación de datos perdidos
		Monitorización para medir la eficiencia de la red		

		Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación local		
Abuso de privilegios de acceso a los sistemas	RB	Controles de acceso a datos mediante clave	Monitoreo de eventos	Parches de seguridad
		Control de acceso a la red, establecimiento de perfiles de usuario.	Revisiones periódicas de procesos	Recuperación de datos perdidos
		Establecer procedimientos / políticas de seguridad en ingreso y claves de acceso a los sistemas		
Introducción de virus en los sistemas y troyanos	RM	Procedimientos de control del software contratado bajo licencia	Detección de virus (Antivirus)	Corrección de daños por virus
		Control de acceso a la red, establecimiento de perfiles de usuario.	Monitoreo de eventos	Parches de seguridad
		Establecer procedimientos / políticas de seguridad en datos		Recuperación de datos perdidos
Ataques por ingeniería social	RA	Procedimientos de control del software contratado bajo licencia	Monitoreo de eventos	Corrección de daños por virus
		Control de acceso a la red, establecimiento de perfiles de usuario.	Detección de virus (Antivirus)	Parches de seguridad
		Establecer procedimientos / políticas de seguridad.		Recuperación de datos perdidos
Bombas lógicas	RA	Procedimientos de control del software contratado bajo licencia	Monitoreo de eventos	Corrección de daños por virus
		Control de acceso a la red, establecimiento de perfiles de usuario.	Detección de virus (Antivirus)	Parches de seguridad

		Establecer procedimientos / políticas de seguridad.		Recuperación de datos perdidos
Ataques de denegación de servicio	RA	Diseño el sistema de prevención de instrusos	Implementar el sistema de prevención de instrusos	
Copias incontroladas de documentos/software/datos	RA	Establecer procedimientos / políticas de copias	Revisiones periódicas de procesos	Recuperación de datos perdidos
Errores en el mantenimiento	RM	Establecer procedimientos / políticas de mantenimiento.	Monitoreo de eventos	Recuperación de datos perdidos
		Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo		
		Contratar seguros para los activos		
HW Desactualizado	RB	Establecer procedimientos / políticas de actualización de HW.		
Corrupción de datos	RM	Establecer procedimientos / políticas de seguridad en datos.	Monitoreo de eventos	Recuperación de datos perdidos

3.2. ETAPA 2: SELECCIÓN DE ESTRATEGIAS

El Banco del Estado, dentro de su implementación del Plan de Contingencias para las tecnologías de la Información, ha definido al centro de cómputo de la Sucursal Regional Manabí como el centro de cómputo alterno para la operación de los servicios informáticos en caso de emergencia.

Esta definición se realizó en base a los siguientes criterios:

- Fallas totales o parciales en la red o servicios de la plataforma.
- Instalaciones propias.
- Centro de cómputo e instalaciones de energía con libre acceso, no es compartido con otras institucionales.
- Riesgo de sismo
- Riesgo de tsunami
- Riesgo de inundación por desbordamiento de río.
- Terminales aéreos locales y próximos (hasta 45 minutos)
- Frecuencia de vuelos desde Quito hasta terminal local o próximo
- Posibilidad de saturación de vuelos por alta demanda debido a concentración de empresas privadas y públicas
- Tiempo de traslado terrestre desde Quito.
- Posibilidad de saturación de canales por alta concentración de empresas privadas y públicas
- Tipo de enlace de última milla con varios proveedores de comunicación
- Disponibilidad de anillos de fibra óptica para comunicaciones

3.2.1. SELECCIÓN DE ESTRATEGIAS

Se han seleccionado las siguientes estrategias que permitirán mitigar el impacto de una posible interrupción de los recursos y servicios de la institución, considerando cuatro escenarios diferentes:

Definición de Términos:

- Centro de Cómputo Alterno – Oficinas de la Sucursal Regional Manabí

  Portoviejo - Manabí
- Centro Alterno de Operaciones Técnicas – Centro de Capacitación

  Calle de los Cipreses 6425 y Los Helechos, Sector Collaloma

  Quito – Pichincha
- Matriz del Banco del Estado

  Av. Atahualpa OE1-119 entre Calle Juan Bayas y AV. 10 de Agosto

  Quito – Pichincha

3.2.1.1. **Escenario 1:**

En este escenario se presentan condiciones de incidentes menores dentro del Centro de Cómputo de la Matriz:

1. Incidente menor en el Centro de Cómputo Principal que impida la operación de alguno de los servicios que este brinda:
    - Daño o desconfiguración parcial de la parte física o lógica en alguno de los servidores (correo, impresión, sistema financiero, BPM, archivo electrónico, telefonía y de los servidores de servicios).
    - Daño o desconfiguración parcial de la parte físico o lógico en alguno de los equipos de virtualización
    - Daño o desconfiguración parcial de la parte físico o lógico en alguno de los componentes de la red

- Daño o desconfiguración parcial de la parte físico o lógico en alguno de los equipos de comunicaciones alternas
- Daño o desconfiguración parcial de la parte físico o lógico en alguno de los UPS, generadores eléctricos, sistema de incendios o aire acondicionado
- Caída del proveedor de servicios principal.

2. Exista acceso al edificio Matriz.

Estrategia de recuperación:

1. En el caso de daño menor de alguno de los equipos servidores, dispositivos de comunicación, componentes de red y demás, se procede a su reemplazo inmediato del equipo con inconvenientes. Si el incidente tomara más tiempo, el Centro de Cómputo de la Sucursal Regional Manabí apoyará en lo que fuere del caso. Las actividades del Equipo de Recuperación, están detalladas en la Etapa III Desarrollo del Plan. (El técnico de la Regional Manabí se encuentra capacitado para afrontar la contingencia).
2. El personal informático de la matriz monitoreará e informará al Equipo de Recuperación, el desarrollo del proceso de recuperación.
3. En el caso de daño menor de alguno de los equipos servidores, dispositivos de comunicación, componentes de red y demás, se procederá a su remplazo inmediato del equipo o dispositivo con inconvenientes.
4. En caso de ser un fallo de comunicación con el proveedor principal de comunicaciones, el proveedor alterno tomará el control automáticamente. Se contactará urgentemente con los proveedores para el arreglo y monitoreo del enlace

principal. (el listado de proveedores se encuentra detallado en la Etapa III Desarrollo del Plan, 3.2 Equipo Logístico).

5. En el caso de que sea un fallo de hardware de alguno de los equipos, se contactará inmediatamente a los proveedores para ejecución de garantías de ser al caso, o para ejecutar algún contrato de soporte y mantenimiento.
6. Se levantarán respaldos de información de ser el caso y se montará en un servidor alterno para restaurar la aplicación.
7. En el caso de que el fallo sea en algún dispositivo de red alámbrica se trabajará en las redes inalámbricas configuradas disponibles, o viceversa.

El tiempo de restablecimiento de los servicios para este escenario en la Matriz dependiendo de su incidencia puede ser INMEDIATO o tardar HORAS, conforme los Acuerdos de Niveles de Servicios establecidos.

En el Centro de Cómputo de la Matriz del Banco del Estado, se consideran factores como:

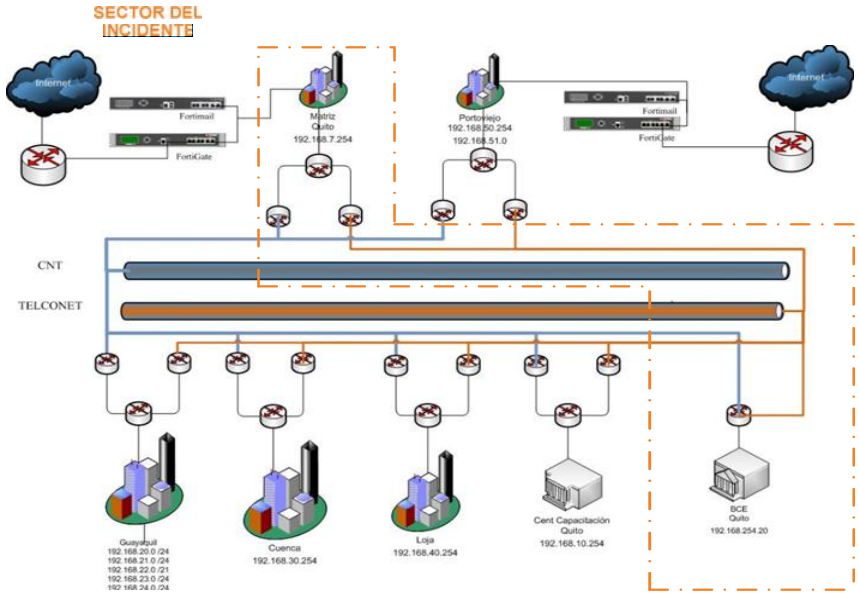
Recursos Técnicos:

- Centro de Cómputo de la Matriz.

Recursos Humanos:

- Personal Técnico Informático de la Matriz.
- Administrador de la red del Banco y apoyos.
- Personal de los proveedores de servicios y de contratos de mantenimiento.

Gráfico del Escenario 1:



3.2.1.2. Escenario 2:

En este escenario se presentan condiciones de incidencias mayores en los servicios informáticos o Centro de Cómputo de la matriz:

1. Incidente mayor en el Centro de Cómputo principal que impida la operación de los servicios que este brinda:
    - Daño físico o lógico en alguno de los servidores (correo, BPM, archivo electrónico, telefonía y de los servidores de servicios).
    - Daño físico o lógico en alguno de los equipos de virtualización
    - Daño físico o lógico en alguno de los componentes de la red
    - Daño físico o lógico en alguno de los equipos de comunicaciones alternas
    - Daño físico o lógico en alguno de los UPS, generadores eléctricos, sistema de incendios o aire acondicionado

- Caída de los proveedores de servicios principal

2. Exista acceso al edificio matriz

Estrategia de recuperación:

1. En el caso de daño definitivo de los equipos servidores, dispositivos de comunicación, componentes de red y demás, el Centro de Cómputo de la Sucursal Regional Manabí tomará el control de la red y recursos del Banco en ambiente de contingencia. Las actividades del Equipo de Recuperación, están detalladas en la Etapa III Desarrollo del Plan. (El técnico de la Regional Manabí se encuentra capacitado para afrontar la contingencia).
2. En caso de ser un fallo de comunicación con el proveedor principal de comunicaciones, el proveedor alterno tomará el control automáticamente.
3. En el caso de que sea un fallo de comunicación, se contactará urgentemente con los proveedores para el arreglo y monitoreo de los enlaces. (El listado de proveedores se encuentra detallado en la Etapa III Desarrollo del Plan, Equipo Logístico).
4. En el caso de que sea un fallo de hardware de alguno de los equipos, se contactará inmediatamente a los proveedores para ejecución de garantías de ser al caso, o para ejecutar algún contrato de soporte y mantenimiento.
5. El personal informático de la Matriz monitoreará e informará al Equipo de Recuperación, el desarrollo del proceso de recuperación.

El tiempo de restablecimiento de los servicios para este escenario en la Matriz dependiendo de su incidencia puede ser INMEDIATO o tardar HORAS.

En el Centro de Cómputo de la Matriz del Banco del Estado, se consideran factores como:

Recursos Técnicos:

- Centro de Cómputo de la Matriz.
- Centro de Cómputo de la SRM, adecuado como Centro de Cómputo Alterno.

Recursos Humanos:

- Personal Técnico Informático de la Matriz.
- Personal Técnico de la Sucursal Regional Manabí.
- Administrador de la red del Banco.
- Personal de los proveedores de servicios y de contratos de mantenimiento.

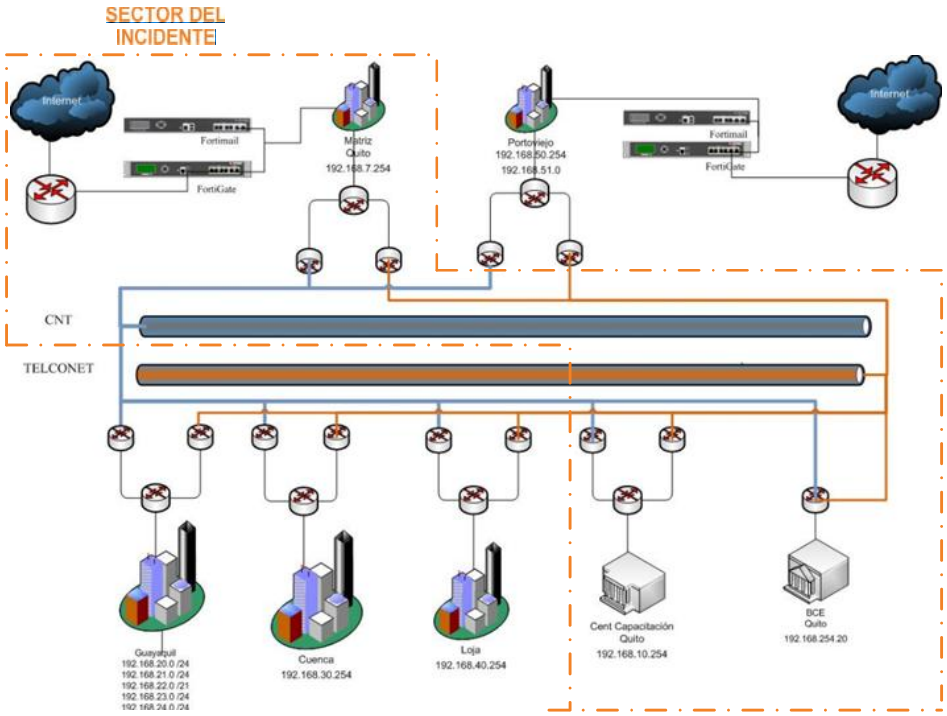
En la Sucursal Regional Manabí del Banco del Estado, se consideran los siguientes servicios de manera individual o mixta:

1. El servicio de Base de Datos debe ser íntegro para las aplicaciones en ambiente de Contingencia.
2. Se proveerá servicio de Correo Electrónico exclusivo para personal registrado en la lista de Continuidad de Servicio.
3. Servicio Alterno de Comunicaciones haciendo de nodo principal la Sucursal Regional Manabí.

En el Centro de Operaciones Técnicas Alterno, Centro de Capacitaciones, se consideran los siguientes servicios:

1. Servicio de enlace al Centro de Cómputo de la Matriz
2. Servicio de enlace al Centro Alterno en la Sucursal Regional Manabí, en caso de que se el Centro de Cómputo de la Matriz esta dado de baja y se haya notificado oficialmente el paso a ambiente de contingencia.

Gráfico del Escenario 2:



3.2.1.3. Escenario 3:

En este escenario se presenta lo siguiente:

1. No se presentan condiciones de incidentes dentro del Centro de Cómputo de la Matriz.
2. Se presenta incidente externo que impide la entrada al edificio Matriz del Banco del Estado.

Estrategia de recuperación:

1. En el caso de daño o incidente impida el ingreso al edificio Matriz del Banco, se operará desde el Centro de Capacitaciones adecuado para ejecutar el Plan de Contingencia de TIs. Si el incidente tomara más tiempo, o si hicieran más falta recursos, el Centro de Cómputo de la Sucursal Regional Manabí apoyará en lo que fuere del caso. Las actividades del Equipo de Recuperación, están detalladas en la Etapa III Desarrollo del Plan. (El técnico de la Regional Manabí se encuentra capacitado para afrontar la contingencia).
2. En caso de ser un fallo de comunicación con el proveedor principal de comunicaciones, el proveedor alterno tomará el control automáticamente.
3. En el caso de que sea un fallo de comunicación, se contactará urgentemente con los proveedores para el arreglo y monitoreo de los enlaces. (El listado de proveedores se encuentra detallado en la Etapa III Desarrollo del Plan, Equipo Logístico).
4. En el caso de que sea un fallo de hardware de alguno de los equipos, se contactará inmediatamente a los proveedores para ejecución de garantías de ser al caso, o para ejecutar algún contrato de soporte y mantenimiento.
5. Se levantarán respaldos de información de ser el caso y se montará en un servidor alterno para restaurar la aplicación.
6. El personal informático de la Matriz monitoreará e informará al Equipo de Recuperación, el desarrollo del proceso de recuperación.

En el caso que el fallo sea en algún dispositivo de red alámbrica se trabajará en las redes inalámbricas configuradas disponibles, o viceversa.

El tiempo de restablecimiento de los servicios para este escenario en la Matriz dependiendo de su incidencia puede ser INMEDIATO o tardar HORAS.

En el Centro de Cómputo de la Matriz del Banco del Estado, se consideran factores como:

Recursos Técnicos:

- Centro Alterno de Operaciones Técnicas o Centro de Capacitaciones, conectado al Centro de Cómputo Alterno.

Recursos Humanos:

- Personal Técnico Operativo identificado en el Plan de Contingencia de TIs.
- Personal Técnico Informático de la Matriz.
- Personal Técnico de la Sucursal Regional Manabí.
- Administrador de la red del Banco y apoyos.
- Personal de los proveedores de servicios y de contratos de mantenimiento.

En la Sucursal Regional Manabí del Banco del Estado, se consideran los siguientes servicios de manera individual o mixta:

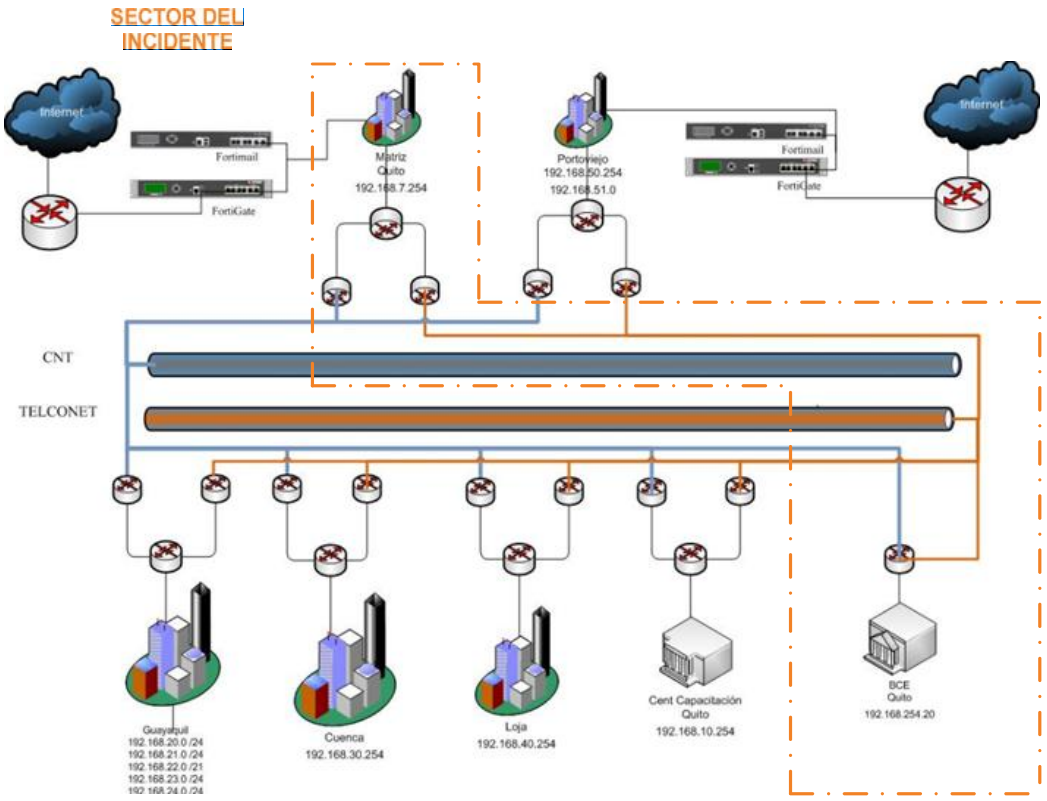
1. El servicio de Base de Datos debe ser íntegro para las aplicaciones en ambiente de Contingencia.
2. Se proveerá servicio de Correo Electrónico exclusivo para personal registrado en la lista de Continuidad de Servicio.

3. Servicio Alterno de Comunicaciones haciendo de nodo principal la Sucursal Regional Manabí.

En el Centro de Operaciones Técnicas Alterno, Centro de Capacitaciones, se consideran los siguientes servicios:

1. Servicio de enlace al Centro de Cómputo de la Matriz
2. Servicio de enlace al Centro Alterno en la Sucursal Regional Manabí, en caso de que se el Centro de Cómputo de la Matriz esta dado de baja y se haya notificado oficialmente el paso a ambiente de contingencia.

Gráfico del Escenario 3:



3.2.1.4. Escenario 4:

En el escenario en que se presenten las siguientes condiciones:

1. Incidente en el Centro de Cómputo principal que impida su operación
2. No exista acceso al edificio matriz
3. No exista acceso al Centro Alterno de Operaciones Técnicas o Centro de Capacitación.

Estrategia de recuperación:

1. La Sucursal Regional Manabí tomará el control de la red y recursos del Banco. (el técnico de la Regional Manabí se encuentra capacitado para afrontar la contingencia).
2. Levantar los servicios considerados como críticos en la gestión del Banco. Las actividades del Equipo de Recuperación, están detalladas en la Etapa III Desarrollo del Plan. (Manual de procedimientos para levantar procesos críticos en el centro de cómputo de la regional Manabí).
3. El personal informático de la SRM monitoreará e informará al Equipo de Recuperación, el desarrollo del proceso de recuperación.
4. De ser el caso, a la SRM acudirán miembros del Equipo de Recuperación de la Dirección de Sistemas de Información de la matriz.
5. De ser al caso, a la SRM acudirá el personal operativo y recursos que hayan sido designados en el Plan de Contingencia de TIs del Banco de Estado.
6. Mantener el control de la red y servicios del Banco desde la SRM, hasta que el centro de cómputo principal en la Matriz esté habilitado nuevamente.

El tiempo de restablecimiento de los servicios para este escenario en la SRM es INMEDIATO.

En la Sucursal Regional Manabí del Banco del Estado, se consideran factores como:

Recursos técnicos:

- Centro de Cómputo de la SRM, adecuado como Centro de Cómputo Alterno.

Recursos humanos:

- Personal Informático de la SRM
- Miembros del Equipo de Recuperación
- Técnicos especialistas de las diferentes aplicaciones (de ser requerido)
- Personal Técnico Operativo identificado en el Plan de Contingencia de TIs (de ser requerido)

En la Sucursal Regional Manabí del Banco del Estado, se consideran los siguientes servicios de manera individual o mixta:

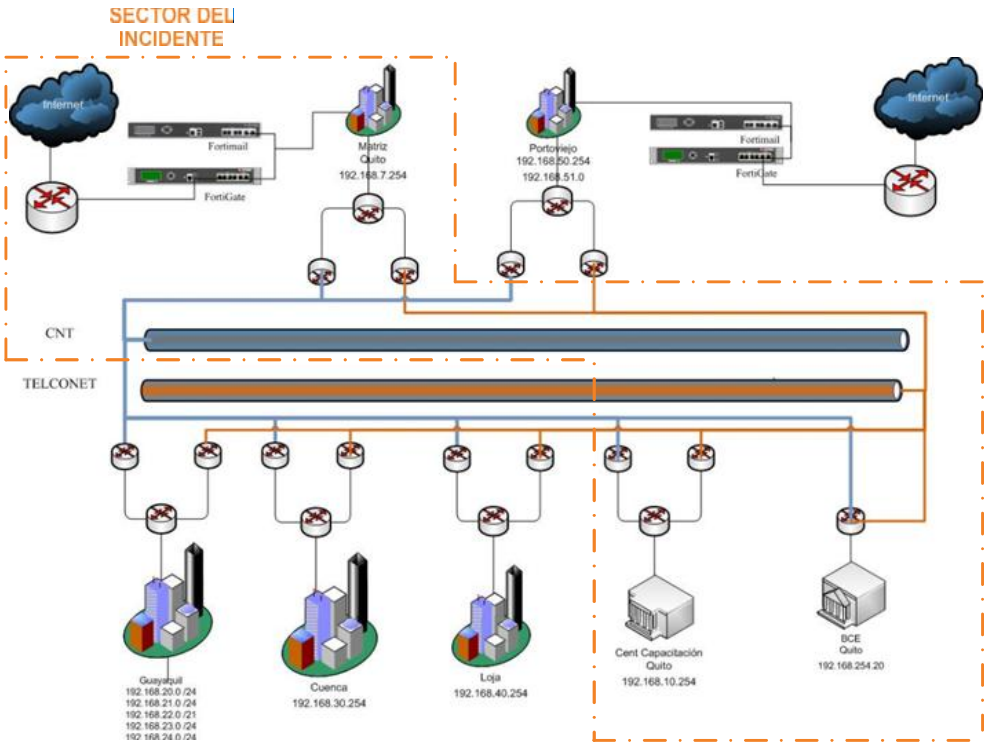
1. El servicio de Base de Datos debe ser íntegro para las aplicaciones en ambiente de Contingencia.
2. El servicio de Correo Electrónico exclusivo para personal registrado en la lista de Continuidad de Servicio.

3. Servicio Alterno de Comunicaciones haciendo de nodo principal la Sucursal Regional Manabí.

En el Centro Alterno de Operaciones Técnicas, Centro de Capacitaciones, se consideran los siguientes servicios:

1. Servicio de enlace al Centro de Cómputo de la Matriz.
2. Almacenamiento de Aplicaciones Cliente Servidor.
3. Servicio de enlace al Centro Alterno en la Sucursal Regional Manabí, en caso de que se el Centro de Cómputo de la Matriz esta dado de baja y se haya notificado oficialmente el paso a ambiente de contingencia.

Gráfico del Escenario 4:



A continuación se muestra una tabla que recoge la relación entre el Tiempo Objetivo de recuperación y la solución de contingencia más adecuada a cada escenario:

ESCENARIOS	TIEMPO OBJETIVO DE RECUPERACIÓN DE SERVICIOS EN CONTINGENCIA	TIEMPO OBJETIVO DE RESTAURACIÓN DE SERVICIOS A LA NORMALIDAD
ESCENARIO 1,2,3	INMEDIATO	SEMANAS
ESCENARIO 1,2,3	HORAS	DIAS
ESCENARIO 4	HORAS	SEMANAS

Se detallan los procesos que se ejecutaron y que permitirán llevar a cabo el Plan de Contingencia:

- Adquisición DATA CENTER para centro de cómputo alterno.
- Adquisición de equipos servidores para replicación de servicios.
- Contratación del servicio alterno de comunicaciones.
- Adquisición de equipos para comunicaciones alternas.
- Adquisición de un generador eléctrico para Centro de Capacitación.
- Habilitación cuarto de UPS en el edificio Matriz.

3.3. Etapa III: DESARROLLO DEL PLAN

Una vez que se ha seleccionado la estrategia de respaldo hay que desarrollarla e implantarla dentro de la institución. En esta etapa se desarrollan los procedimientos y planes de actuación para las distintas áreas y equipos, y se organizan los equipos que intervienen en cada etapa del Plan.

3.3.1. ORGANIZACIÓN DE LOS EQUIPOS DE RECUPERACIÓN

El equipo de recuperación es el encargado de poner en marcha todo el proceso de recuperación, para restaurar los servicios dentro de los cuatro escenarios descritos. Los integrantes primarios del Equipo de Recuperación Tecnológica son:

INTEGRANTES DEL EQUIPO DE RECUPERACIÓN TECNOLÓGICA	
RESPONSABLE DEL EQUIPO	
NOMBRE:	Bryan Jiménez Franco
CARGO:	Director de Sistemas de Información
FUNCIÓN:	Líder del Equipo de Recuperación Tecnológica
TELÉFONO CASA:	02-255-4348
TELÉFONO CELULAR:	098-7707-296
DIRECCIÓN CASA:	Yaguachi 186, El Dorado
MIEMBROS DEL EQUIPO	
NOMBRE:	Ruben Conrado
FUNCIÓN:	Responsable de Infraestructura y Redes
TELÉFONO CELULAR	099-833-2525
TELÉFONO CASA:	02-2542-502
DIRECCIÓN CASA:	Juan Manuel Lazo 237 y Mariana de Jesús
NOMBRE:	Fabián Analuisa
FUNCIÓN:	Responsable aplicaciones y soporte
TELÉFONO CASA:	02-237-6573
TELÉFONO CELULAR:	09-9823-6674
DIRECCIÓN CASA:	Urbanización Eucalipto Casa # 2, Gonzalo Meneses y Latacunga. Tumbaco
NOMBRE:	Irma Mera
FUNCIÓN:	Responsable de Seguridad y Base de Datos
TELÉFONO CASA:	02-249-5764
TELÉFONO CELULAR:	08-490-9411
DIRECCIÓN CASA:	Prados del Condado. Calle Pichincha y Calle 2. OE5-475
NOMBRE:	Raúl Endara

CARGO:	Responsable de Servidores, Correo, Telefonía y Directorio Activo.
TELÉFONO CASA:	02-222-6965
TELÉFONO CELULAR:	09-9981-9350
DIRECCIÓN CASA:	Tamayo N23-41 y Veintimilla
NOMBRE:	Catalina Burgos
CARGO:	Soporte General en la Coordinación del Plan de Contingencia
TELÉFONO CASA:	098-425-0924
TELÉFONO CELULAR:	02-332-4908
DIRECCIÓN CASA:	Calle El Batán y Eloy Alfaro. Edificio Alessandría. Piso 5

Los backups de los integrantes del Equipo de Recuperación Tecnológica son los siguientes:

INTEGRANTES DEL EQUIPO DE RECUPERACIÓN TECNOLÓGICA	
RESPONSABLE DEL EQUIPO	
NOMBRE:	Catalina Burgos
CARGO:	Líder Suplente del Equipo de Recuperación Tecnológica
TELÉFONO CASA:	098-425-0924
TELÉFONO CELULAR:	02-332-4908
DIRECCIÓN CASA:	Calle El Batán y Eloy Alfaro. Edificio Alessandría. Piso 5
MIEMBROS DEL EQUIPO	
NOMBRE:	Carlos Estrada
FUNCIÓN:	Responsable Suplente de la Administración de Infraestructura y Redes, Servidores, Correo y Telefonía.
REEMPLAZA A:	Rubén Conrado
TELÉFONO CELULAR	02-259-5856
TELÉFONO CASA:	09-833-55255
DIRECCIÓN CASA:	Pedro de Alvarado N56-324 y Fernández Salvador
NOMBRE:	César García
FUNCIÓN:	Responsable Suplente de Aplicaciones y Soporte
REEMPLAZA A:	Fabian Analuisa
TELÉFONO CASA:	02-256-6543
TELÉFONO CELULAR:	09-898-45893

DIRECCIÓN CASA:	Charles Darwin y Graciela Ayerve. Conocoto
NOMBRE:	Diego Campos
FUNCIÓN:	Responsable de Seguridad y Base de Datos
REEMPLAZA A:	Irma Mera
TELÉFONO CASA:	02-395-6951
TELÉFONO CELULAR:	098-469-9037
DIRECCIÓN CASA:	San Miguel de Conocoto, Isidro Ayora y Miguel de Ascazubi, conjunto prados del dean, Casa 8

Los integrantes del Equipo de Recuperación Tecnológica en caso del escenario cuarto del Plan de Contingencia para las tecnologías de Información, son los siguientes:

INTEGRANTES DEL EQUIPO DE RECUPERACIÓN TECNOLÓGICA	
RESPONSABLE DEL EQUIPO	
NOMBRE:	Jorge Correa
CARGO:	Líder del Equipo de Recuperación Tecnológica
TELÉFONO CASA:	09-9474-7019
TELÉFONO CELULAR:	05-265-0433
DIRECCIÓN CASA:	Av. Universitaria y América
MIEMBROS DEL EQUIPO	
NOMBRE:	Marcos Quiroga
FUNCIÓN:	Coordinador Regional del Equipo de Recuperación Tecnológica
TELÉFONO CELULAR	098-436-6900
TELÉFONO CASA:	04-249-4095
DIRECCIÓN CASA:	Cdl. Floresta 1 mz.21 villa 18
NOMBRE:	María Soledad Muñoz
FUNCIÓN:	Coordinador Regional del Equipo de Recuperación Tecnológica
TELÉFONO CASA:	07-282-4878
TELÉFONO CELULAR:	098-499-9460
DIRECCIÓN CASA:	Charles Darwin y Graciela Ayerve. Conocoto
NOMBRE:	Manuel Ochoa
FUNCIÓN:	Coordinador Regional del Equipo de

	Recuperación Tecnológica
TELÉFONO CASA:	072581752
TELÉFONO CELULAR:	0992261111
DIRECCIÓN CASA:	Augusto Salazar y José Vaconcellos intersección. El Rosal.

Para poner en marcha el Plan de Contingencia de TIs se consideran dos posibilidades:

1. **Que exista un incidente de carácter técnico:**

Si se determina un estado de emergencia o incidente de carácter técnico, el responsable del Equipo de Recuperación, Director de Sistemas de Información, se reunirá con resto del equipo para tomar decisiones y afrontar la situación; y, determinará si es necesario iniciar el Plan de Contingencia. El equipo debe estar continuamente informado de lo que acontece.

2. **Que exista un incidente declarado por el Comité de Riesgos**

Si se determina un estado de emergencia o incidente declarado por el Comité de Riesgos, se comunicará inmediatamente al responsable del Equipo de Recuperación Tecnológica, Director de Sistemas de Información, el que se reunirá con el resto del equipo para tomar decisiones y afrontar la situación; y, determinará si es necesario iniciar el Plan de Contingencia. El equipo debe estar continuamente informado de lo que acontece.

3.3.1.1. <u>Escenario 1:</u>

Lugar de Reunión del Equipo de Recuperación:

Sala de reuniones de la Dirección de Sistemas de Información en el Edificio Matriz del Banco del Estado, ubicado en la Av. Atahualpa OE1-119 entre Calle Juan Bayas y AV. 10 de Agosto, en Quito – Pichincha.

Actividades del Equipo de Recuperación:

- El equipo técnico de la Dirección de Sistemas de Información procederá de inmediato a realizar el análisis del equipo o servicio con inconvenientes. Si el incidente tomara más de 1 día, el Centro de Cómputo de la Sucursal Regional Manabí apoyará en lo que fuere del caso.
- El encargado de la Dirección de Sistemas de Información, será quien monitoree e informe al Equipo de Recuperación la ejecución de las operaciones del centro de cómputo.
- El administrador de red y su equipo, harán el principal papel en esta recuperación, ya que será quien ejecute el plan de contingencia de TIs, realice acciones inmediatas y monitoree los sucesos.
- El administrador de red y su equipo, se contactarán con los proveedores de servicios de comunicaciones y de contratos de mantenimiento para reportar el daño o fallo en los equipos de hardware o software donde se presente el incidente.
- El administrador de red y su equipo, deben solventar o reemplazar de manera urgente los equipos o aplicaciones en las que se haya presentado el incidente, con algún equipo de backup si lo hubiere.
- El administrador de red y su equipo, estarán a cargo de ver su recuperación y de dar el apoyo necesario para restablecer los servicios en el menor tiempo posible.
- De ser necesario, se contactará con los proveedores de los equipos necesarios para restablecer durante el desarrollo del plan de Contingencia de TIs.

- Una vez que se vayan restaurando los servicios en el Centro de Cómputo de la Matriz, se comprobará su operatividad y se trabajará con normalidad.
- Se emitirá un informe, identificando causas, acciones, tiempos y nivel del servicio restaurado, registrándose en la Matriz de contingencia de servicio para actualizar los porcentajes de continuidad.
- En el caso que el fallo sea en algún dispositivo de red alámbrica se trabajará en las redes inalámbricas configuradas disponibles, o viceversa.

3.3.1.2. Escenario 2:

Lugar de Reunión del Equipo de Recuperación:

Sala de reuniones de la Dirección de Sistemas de Información en el Edificio Matriz del Banco del Estado, ubicado en la Av. Atahualpa OE1-119 entre Calle Juan Bayas y AV. 10 de Agosto, en Quito – Pichincha.

Actividades del Equipo de Recuperación:

- El responsable del Equipo de Recuperación será quien tome a cargo la responsabilidad de ejecutar el Plan de Contingencia de TIs en el centro de cómputo de la matriz, y se reunirá con los demás miembros del equipo para ejecutar los procedimientos y resolver la contingencia.
- El equipo técnico de la Dirección de Sistemas de Información procede al inmediato del equipo con inconvenientes. Como el incidente es mayor y puede tomar más de un día la interrupción del servicio, el Centro de Cómputo de la Sucursal Regional Manabí apoyará en lo que fuere del caso.

- El encargado de la Dirección de Sistemas de Información, será quien monitoree e informe al Equipo de Recuperación la ejecución de las operaciones del centro de cómputo y equipo técnico de la SRM.
- El administrador de red y su equipo, harán el papel principal en esta recuperación, ya que será quien ejecute el plan de contingencia, realice acciones inmediatas y monitoree los sucesos.
- El administrador de red y su equipo, se contactarán con los proveedores de servicios de comunicaciones y de contratos de mantenimiento para reportar el daño o fallo en los equipos de hardware o software donde se presente el incidente.
- El responsable del equipo de recuperación comunicará al personal técnico de la SRM para que se revise la disponibilidad de servicios del Centro Alterno.

    1. Servicio de Comunicaciones
    2. Servicio de BDD
    3. Servicio de Aplicaciones WEB
    4. Servicio de Correo Electrónico

- El administrador de red y su equipo, deben solventar o reemplazar de manera urgente los equipos o aplicaciones en las que se haya presentado el incidente, con algún equipo de backup si lo hubiere.
- El administrador de red y su equipo, estarán a cargo de ver su recuperación y de dar el apoyo necesario para restablecer los servicios en el menor tiempo posible.

- El administrador de red y el equipo de recuperación tomarán la decisión de tomar los servicios alternos de la SRM como principales.
- De ser necesario, se contactará con los proveedores de los equipos necesarios para restablecer durante el desarrollo del plan de Contingencia.
- Una vez que se vayan restaurando los servicios en el Centro de Cómputo de la Matriz, se comprobará su operatividad y se trabajará con normalidad.
- En el caso que el fallo sea en algún dispositivo de red alámbrica se trabajará en las redes inalámbricas configuradas disponibles, o viceversa.
- Se emitirá un informe, identificando causas, acciones, tiempos y nivel del servicio restaurado, registrándose en la Matriz de contingencia de servicio para actualizar los porcentajes de continuidad.

3.3.1.3. Escenario 3:

Lugar de Reunión del Equipo de Recuperación:

Centro de Operaciones Técnicas Alterno, Centro de Capacitaciones, ubicado en Calle de los Cipreses 6425 y Los Helechos, en Quito – Pichincha.

Actividades del Equipo de Recuperación:

- Informada la contingencia, el Equipo de Recuperación Tecnológica se reunirá y tomará decisiones para afrontar la situación, haciendo uso del lugar de reuniones establecido para el mismo.
- El encargado de Dirección de Sistemas de Información, será quien tome a cargo la responsabilidad de ejecutar el Plan de Contingencia en el Centro de Operaciones

Técnicas Alterno, y empezará a ejecutar los procedimientos detallados para tomar el control de los servicios informáticos del Banco.

- El Personal Técnico Operativo designado en el Plan de Contingencia de TIs, se trasladará al Centro de Operaciones Técnicas Alterno, Centro de Capacitaciones, ubicado en Calle de los Cipreses 6425 y Los Helechos, en Quito–Pichincha.
- El administrador de red y su equipo, harán el papel principal en esta recuperación, ya que será quien ejecute el plan de contingencia, realice acciones inmediatas y monitoree los sucesos.
- El responsable del equipo de recuperación comunicará al personal técnico de la SRM para que se revise la disponibilidad de servicios del Centro de Cómputo Alterno.

    1. Servicio de Comunicaciones
    2. Servicio de BDD
    3. Servicio de Aplicaciones WEB
    4. Servicio de Correo Electrónico

- El administrador de red y su equipo, se contactarán con los proveedores de servicios de comunicaciones y de contratos de mantenimiento para reportar el daño o fallo en los equipos de hardware o software donde se presente el incidente.
- El administrador de red y su equipo, deben solventar o reemplazar de manera urgente los equipos o aplicaciones en las que se haya presentado el incidente, con algún equipo de backup si lo hubiere.

- De ser necesario, el Equipo de Recuperación Tecnológica se reunirá y tomará decisiones para afrontar la situación, haciendo uso del lugar de reuniones establecido para el mismo.
- El administrador de red y su equipo, estarán a cargo de ver su recuperación y de dar el apoyo necesario para restablecer los servicios en el menor tiempo posible.
- El responsable de la unidad de tecnología del Banco, el administrador de red y/o el equipo de recuperación, según disponibilidad, podrán tomar la decisión en que momento subir los servicios alternos de la SRM como principales.
- De requerirse equipos computadores adicionales para el trabajo del Personal Técnico Operativo designado en el Plan de Contingencia de TIs, el Equipo Logístico se encargará según lo establecido en el mismo Plan.
- De ser necesario, se contactará con los proveedores, los equipos necesarios durante el desarrollo del plan de contingencia para operar con normalidad desde Centro de Operaciones Técnicas Alterno.
- De requerirse equipos adicionales para solventar la recuperación, se solicitará apoyo el Equipo Logístico designado en el Plan de Contingencia de TIs.
- Una vez que se vayan restaurando los servicios en el Centro de Cómputo de la Matriz, se comprobará su operatividad y se trabajará con normalidad.
- Se emitirá un informe, identificando causas, acciones, tiempos y nivel del servicio restaurado, registrándose en la Matriz de contingencia de servicio para actualizar los porcentajes de continuidad.

3.3.1.4. Escenario 4:

Lugar de Reunión del Equipo de Recuperación:

Oficinas de la Sucursal Regional Manabí del Banco del Estado, ubicado en la Olmedo entre Sucre y Córdova (Edificio la Previsora 1er. Piso), en Portoviejo – Manabí.

Actividades del Equipo de Recuperación:

- El líder del equipo de recuperación de la SRM, revisará la disponibilidad de servicios del Centro Alterno y prepare la liberación de los mismos.

    1. Servicio de Comunicaciones
    2. Servicio de BDD
    3. Servicio de Aplicaciones WEB
    4. Servicio de Correo Electrónico

- El personal técnico informático de la SRM, en caso de no disponibilidad del personal técnico de recuperación de la Matriz, será quien tome a cargo la responsabilidad de ejecutar el Plan de Contingencia de TIs en el centro de cómputo de la SRM.
- Centro de Cómputo de la SRM, tomará el control de la red y los servicios del Banco de manera controlada, siguiendo los siguientes pasos:

    1. Comprobar enlace de comunicaciones con todas las Sucursales, Centros de Operación y Banco Central.

2. Validar la activación del Directorio Activo y Dominio del Banco desde la SRM.
3. Validar servicio de BDD

    - CREDITO (Replicación)
    - CGDATAJL (Replicación)
    - CONTABILIDAD (Respaldo)
    - SEGURIDAD (Respaldo)
    - RECURSOS HUMANOS (Respaldo)
    - REGYCONT (Respaldo)
    - GERENCIAL (Respaldo)
    - SIMWEB (Respaldo)
    - SICEND (Respaldo)

4. Validar servicio de correo electrónico
5. Validar disponibilidad de servicios WEB
6. Solicitar reporte de conectividad desde todas las Sucursales
7. Iniciar operación, caso contrario, regresar a ejecutar desde punto 1, según sea el caso.

- De ser posible, el Personal Técnico Operativo designado en el Plan de Contingencia de TIs, se trasladará a la Sucursal Regional Manabí y/o a la Sucursal más cercana para brindar su contingente según lo establecido en el Plan.

- De requerirse equipos computadores adicionales para el trabajo del Personal Técnico Operativo designado en el Plan de Contingencia de TIs, el Equipo Logístico se encargará según lo establecido en el mismo Plan.
- De ser necesario, el Equipo de Recuperación Tecnológica se reunirá y tomará decisiones para afrontar la situación, haciendo uso del lugar de reuniones establecido para el mismo.
- De ser necesario, se contactará con los proveedores, los equipos necesarios durante el desarrollo del plan de contingencia para operar con normalidad desde la SRM.
- Una vez que se vayan restaurando los servicios en el Centro de Cómputo de la Matriz, se comprobará su operatividad y se trabajará con normalidad.

3.3.2. EQUIPO LOGÍSTICO

El equipo de coordinación logística definido en el Plan de Contingencia de TIs, responsable de todo lo relacionado con las necesidades logísticas, en el caso de un incidente y que la parte tecnológica lo requiera, se encargará de:

- Atender las necesidades logísticas de primera instancia tras la contingencia, como el transporte de personas (aéreo, terrestre), de equipos y materiales, etc.
- Contactar con los proveedores para solicitar el material necesario que indiquen los responsables de la recuperación.
- Reservar habitaciones de hotel en Portoviejo para las personas del Equipo de Recuperación que se desplacen hacia esa Sucursal.
- Gestionar el suministro de comida para el personal involucrado.

A continuación se detalla un listado de los principales proveedores de servicios:

Enlace Principal de Comunicaciones:

- Corporación Nacional de Telecomunicaciones (CNT)

  Dirección: Avda. Veintimilla # 1149 y Amazonas, Edificio Estudio Z.

  Ciudad: Quito. País: Ecuador.

  Teléfono: 593-2-2977100

  Contacto: Diego Tierra, Ing.

  Analista de Telecomunicaciones

  GERENCIA DE SOLUCIONES CORPORATIVAS – CNT EP

  Dir: Av. Amazonas y Korea, Ed. Vivaldi

  Telf. : +(5932) 3731 700 Ext.: 21223 (5932) 996183802

  Los números piloto de los enlaces de comunicaciones a nivel nacional:

No. Piloto	Enlace	Dirección Instalación	Dirección Complemento
890151	PORTOVIEJO	AV ATAHUALPA OE1 109 Y AV 10 DE AGOSTO	OLMEDO ENTRE SUCRE Y CORDOVA EDF. BANCO LA PREVISORA PISO 3
890156	LOJA (NORTE)	AV ATAHUALPA OE1 109 Y AV 10 DE AGOSTO	E EGUIGUREN 1441 Y SUCRE
890437	CUENCA	AV ATAHUALPA OE1 109 Y AV 10 DE AGOSTO	AV. 12 DE ABRIL
890155	GYE (NORTE)	AV ATAHUALPA OE1 109 Y AV 10 DE AGOSTO	AV. 9 DE OCTUBRE 1322 Y MACHALA
801568	ENLACE PRINCIPAL	AV ATAHUALPA OE1 109 Y AV 10 DE AGOSTO	JORGE DROM Y AV GASPAR DE VILLARROEL
803400	CENTRO DE CAPACITACIÓN (LA CAROLINA)	AV ATAHUALPA OE1 109 Y AV 10 DE AGOSTO	LOS CIPRECES 27L URB. SANTA LUCIA SECTOR COLLALOMA
805640	B. CENTRAL SPI (QUITO CENTRO)	AV ATAHUALPA OE1 109 Y AV 10 DE AGOSTO	GUAYAQUIL 0 Y CALDAS BANCO CENTRAL DEL ECUADOR
809043	RED INTERMINISTERIAL (MARISCAL SUCRE)	AV ATAHUALPA 0 Y AV 10 DE AGOSTO EDF BCO ESTADO	GARCIA MORENO 1043 Y CHILE EDF PALACIO DE CARONDELET - PRESIDENCIA REPUBLICA.

Enlace Alterno de Comunicaciones:

- TELCONET

  Quito: 593 -2- 3963100 / 1800-567567

Guayaquil: 593 - 4 -2680555

Cuenca: 593 -7- 2849508

Loja: 593- 7- 2585848

Contacto: Andrés Marzo

Ing. de Soporte - Dpto. de Bancos

Tel. (593)-4-3900111 ext. 4431

Cel. (593)-9-98801984

Kennedy Norte, Mz. 109 Solar 21, Guayaquil - Ecuador

Escalamiento para Telefonía

- Primer Nivel: Contact Center 1800 268267
- Segundo Nivel: Wilson Yunda 096183944
- Tercer Nivel: Juan Carlos Cruz 096183941

Escalamiento para Internet

- Primer Nivel: Contact Center 1800 268 267
- Segundo Nivel: Carlos Mejía 096183191
- Tercer Nivel: Juan Carlos Cruz 096183941

Escalamiento para Datos

- Primer Nivel: Contact Center 1800 268 267
- Segundo Nivel: Fernanda Caiza 095084160
- Tercer Nivel: Edwin Logroño 096183940

UPS

CELCO

- Quito, Dir. Telégrafo Primero No. 163 y Av. De la Prensa

  Telf: 02-2468-768 / 09-610-8549
- GYE, Cuidadela Urdenor II, segunda pasaje y calle 16ª /Mz. 236 Solar 9

  Telf: 04-288-9999 / 09-604-2288
- Cuenca, Gran Colombia 661 y Hermano Miguel

  Telf: 07-283-0126 / 09-570-0700

Aire Acondicionado y Sistema de Incendio

PROTECOMPU

- Sucursal Matriz- La Paz, Quito - Ecuador

  Dirección: Whimper # 780 y Av. 6 de Diciembre

  Teléfonos: +(593 2) 250-8783, +(593 2) 250-8784, +(593 2) 256-0845, +(593 2)

256-8223, +(593 2) 252-4225, +(593 2) 252-5744

Divisiones: Administrativa, Financiera, Comercial, (Show Room - Data Center), TI

- Sucursal Técnica - Parkenor, Quito - Ecuador

  Dirección: Panamericana Norte km. 5 1/2 Complejo Industrial Parkenor, Bodegas 47 - 48

  Teléfonos: +(593 2) 248-3407, +(593 2) 248-3408, +(593 2) 248-3685, +(593 2) 248-3728

  Divisiones: Técnica, Bodegas

- Sucursal Producción - Alfaro, Quito - Ecuador

  Dirección: Calle Chediak N72-A y Av. Eloy Alfaro,

  Teléfonos: + (593 2) 247-3323, + (593 2) 280-1115,

  Divisiones: Planta de Producción

- Sucursal Comercial Kennedy Norte, Guayaquil - Ecuador

  Dirección: Av. Miguel Alcívar # 407 y Angel Barrera, Edificio Arquetipo III, oficina 2

  Teléfonos: + (593 4) 268-4212, + (593 4) 268-4236, + (593 4) 268-4288, + (593 4) 268-2863, + (593 4) 268-2864

  Divisiones: Comercial, (Show Room - Data Center)

- Sucursal Técnica, bodegas y administrativa, Guayaquil - Ecuador

Dirección: Cdla. Industrial Satrion Av. Felipe Pezo Campuzano y III Pasaje 32 N.O. Bodegas La Carlota, # 26. (Frente a la 10ma. Etapa de la Alborada)

Teléfonos: + (593) 04 2279 614, + (593) 04 2245 622

Divisiones: Administrativa, bodegas y técnica

3.3.3. 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.

3.3.4. DESARROLLO DE PROCEDIMIENTOS

3.3.4.1. Elaborar procedimientos de la etapa de alerta

3.3.4.1.1. Elaborar procedimiento de notificacion de desastres

Cualquier funcionario de informática de la Matriz o Sucursales del Banco del Estado, que identifique un incidente grave que pueda afectar a la institución, debe comunicarlo a alguno de los integrantes del Equipo de Recuperación, proporcionando el mayor detalle posible en la descripción de los hechos, para que el comité evalué la situación.

3.3.4.1.2. Elaborar procedimiento de ejecución del plan

El Comité de Crisis reunido en el punto de encuentro evaluará la situación. Con toda la información de detalle sobre el incidente, se decidirá si se activa o no el Plan de Contingencia de TIs. En caso afirmativo, se iniciará el procedimiento de ejecución del Plan.

En el caso de que el Comité decidida no activar el Plan de Contingencia porque la gravedad del incidente no lo requiere, sí será necesario gestionar el incidente para que no aumente su gravedad.

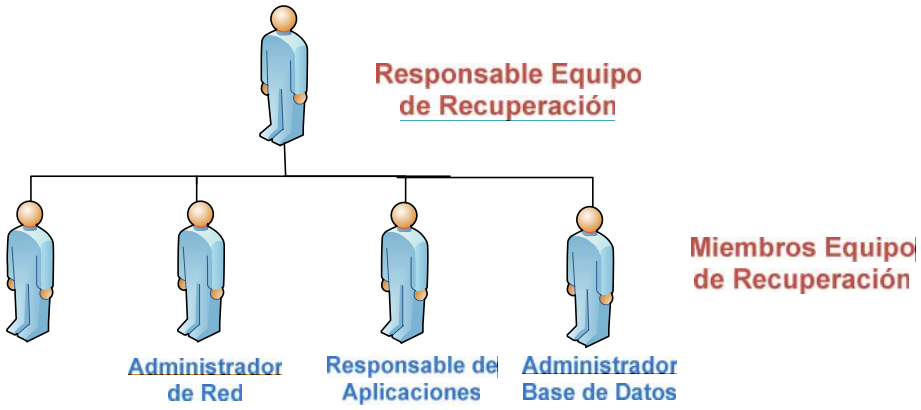
Entre las acciones a realizarse para ejecutar el Plan están:

1. Analizar la situación actual con respecto a los controles y acciones preventivas y detectivas definidas para mitigar los riesgos.
2. Seleccionar los métodos operativos alternativos que se van a utilizar una vez sucedido un incidente que haya provocado una interrupción en los servicios. Se encajará el incidente en uno de los escenarios determinados en la una de las etapas para proceder con la restauración de los servicios.
3. El método seleccionado garantizará la restauración de los procesos afectados en los tiempos determinados por el Análisis de Impacto.
4. Se analizará la situación actual con respecto a los tiempos de respuesta requeridos por las aplicaciones críticas.
5. Se definirá un plan de trabajo y presupuesto requeridos, para implementar las acciones e infraestructura para cumplir con los tiempos de restauración establecidos en el Plan en la Etapa de Transición.
6. Evaluar el análisis de impacto de la situación actual una vez ejecutado el Plan de vuelta a la normalidad.
7. Ejecutar de pruebas.

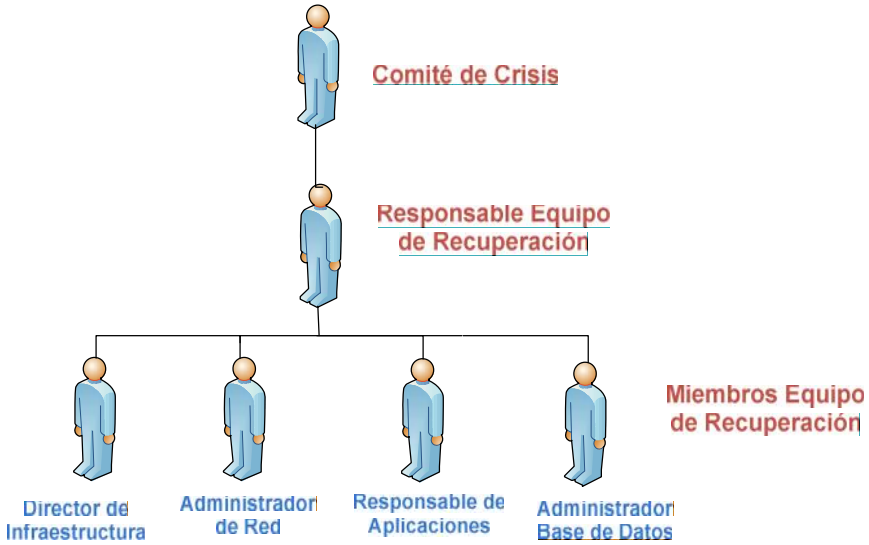
3.3.4.1.3. Elaborar procedimiento de notificación de ejecución del plan

Activar el árbol de llamadas para avisar a los integrantes de los diferentes equipos que van a participar en el Plan:

1. **Que exista un incidente de carácter técnico**:



2. **Que exista un incidente declarado por el Comité de Riesgos**



3.3.4.2. Elaborar procedimientos de la etapa de transición

3.3.4.2.1. Elaborar procedimiento de concentracion y traslado de equipos

Una vez avisados los equipos y puesto en marcha el Plan de Contingencia, deberán acudir al centro de reunión indicado. Además del traslado del personal al centro de cómputo alterno en la SRM, hay que trasladar todo el material y equipos necesarios de ser el caso, para poner en marcha el centro de recuperación, a pesar de que la instalación del centro de cómputo alterno, cuenta con todo el equipo físico suficiente para operar con normalidad con datos actualizados y sin pérdida alguna. Esta labor se cumplirá con el apoyo del equipo logístico.

El equipo de recuperación solicitará al equipo de logística cualquier tipo de material extra que fuera necesario para la recuperación.

3.3.4.3. Elaborar procedimientos de la etapa de recuperación

3.3.4.3.1. Elaborar procedimiento de restauración

El orden de recuperación de las funciones se realizará según la criticidad los sistemas:

Proceso	Subproceso	Nombre del Sistema	Necesidades de Recuperación	Criticidad
INGRESAR Y ANALIZAR SOLICITUD DE CREDITO	Registrar y analizar solicitud	SIC	DIA 1-7	2
EFECTUAR EVALUACION DEL	Analizar requisitos para evaluación	SIC	DIA 1-7	2

CREDITO	Efectuar evaluación técnica		DIA 1-7	2
	Efectuar evaluación ambiental	SIC	DIA 1-7	2
	Efectuar evaluación de participación comunitaria		DIA 1-7	2
	Efectuar evaluación económica	SIC	DIA 1-7	2
	Analizar gestión de servicio		DIA 1-7	2
	Efectuar evaluación financiera	SIC	DIA 1-7	2
	Analizar legalmente al crédito		DIA 1-7	2
	Consolidar informe de evaluación		DIA 1-7	2
APROBAR OPERACIÓN DE FINANCIAMIENTO	Calificar operación de financiamiento	SIC	DIA 1-7	1
	Aprobar operación de financiamiento	CGWEB	DIA 1-7	1
LEGALIZAR CRÉDITO	Elaborar y formar contrato de crédito y fideicomiso	SIC	DIA 1-7	1
EFECTUAR SEGUIMIENTO DEL CRÉDITO	Realizar seguimiento del crédito	SIC	DIA 1-7	2
	Efectuar trámites de operación de crédito	SIC	DIA 1-7	2
EFECTUAR DESEMBOLSO DEL CRÉDITO	Elaborar informe de desembolso	SIC	DIA 1-7	1
	Aprobar desembolsos	SIC	DIA 1-7	1
	Entregar recursos	SIC	DIA 1-7	1

Los sistemas con criticidad de (1) son los que deben recuperarse lo antes posible, en las 48 horas siguientes. Los demás sistemas pueden esperar a recuperarse durante los 7 días primeros posteriores al incidente.

3.3.4.3.2. Elaborar procedimiento de gestión y soporte

Una vez recuperados los sistemas, se avisará a los equipos de los departamentos que gestionan los sistemas (listado del equipo de Unidades de Negocio) para que realicen las comprobaciones necesarias que certifiquen que funcionen de manera correcta y pueda continuarse dando el servicio.

Además el Equipo de Seguridad deberá comprobar que existen las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad) antes de dar por terminada la etapa de recuperación.

- **Listado de tiempos máximos de atención en requerimientos de soporte técnico**

Estos requerimientos corresponden a Soporte Técnico Informático de nivel básico, en caso de ser necesario, se escalará a través del Sistema de Mesa de Ayuda "GLPI", considerando tiempos adicionales.

No.	DESCRIPCIÓN	NOMBRE CORTO	TIEMPO MÁXIMO DE ATENCIÓN (min.)
1	Creación de nuevo funcionario en la Red de Datos Institucional: CREACIÓN DIRECTORIO ACTIVO, CUENTA CORREO ELECTRÓNICO, PERMISO EN APLICACIONES, ENTREGA DE CLAVE. Nota: Se requiere que el funcionario haya sido ingresado en el Sistema de Talento Humano.	NUEVO USUARIO BdE	135
2	Creación de Usuario en la Red de Datos (Directorio Activo)	CREACIÓN DIRECTORIO ACTIVO	30
3	Creación de cuenta de Correo Electrónico	CUENTA CORREO ELECTRÓNICO	30
4	Permisos de acceso a BDD y Aplicaciones	PERMISOS EN APLICACIONES	45
5	Entrega de clave	ENTREGA CLAVE	30

6	Configuración y entrega de equipo	CONFIGURACIÓN Y ENTREGA DE EQUIPO	270
7	Instalación, configuración de accesorios Nota: Accesorios disponibles en stock	INSTALACIÓN DE ACCESORIOS	60
8	Instalación y configuración de navegador de internet	CONFIGURAR NAVEGADOR	60
9	Reseteo de contraseña	RESETEO DE CONTRASEÑA	15
11	Resolver problemas de red	CONEXIÓN A LA RED	45
12	Resolver problemas de correo electrónico	CORREO ELECTRONICO	45
14	Configuración de teléfono IP Nota: previa entrega de teléfono físico por DBSG	CONFIGURAR TELÉFONO IP	40
16	Problemas de impresión Nota: cuando no aplique outsourcing	IMPRESIÓN	30
17	Instalación de aplicaciones BdE	INSTALACION DE APLICACIONES BdE	120
18	Instalación de aplicaciones externas	INSTALACION DE APLICACIONES Otras Aplicaciones	180
22	Configuración de SCANNER	SCANNER	180
23	INSTALACIÓN SPI/SPL	INSTALACIÓN SPI/SPL	90
24	ELIMINACIÓN USUARIO BDD	ELIMINACIÓN USUARIO BDD	15
25	ELIMINACIÓN USUARIO (INFRAESTRUCTURA)	ELIMINACIÓN USUARIO (INFRAESTRUCTURA)	15

3.3.4.4. Elaborar procedimientos de la etapa de vuelta a la normalidad

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

La estimación del tiempo en que va a durar la interrupción del servicio, se obtiene luego de evaluar el alcance de las fallas que se presentaron.

3.3.4.4.1. Elaborar analisis de impacto

Es el momento de realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad. Para ello, el equipo de recuperación junto con el equipo de seguridad del Banco del Estado, realizarán un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como de todo el material que se puede volver a utilizar. Esta evaluación deberá ser comunicada lo antes posible al equipo director para que determinen las acciones necesarias que lleven a la operación habitual lo antes posible.

3.4. ETAPA IV – PRUEBAS Y MANTENIMIENTO

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

El Plan de Contingencia de TIs comprende el desarrollo de un plan experimental de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o si se deben efectuar ajustes para su funcionalidad.

3.4.1. Elaboración del plan de pruebas del plan de contingencia para las tecnologías de información

3.4.1.1. Objetivos de plan de pruebas

El Plan de Pruebas diseñado tiene como objetivos:

- Evaluar la capacidad de respuesta ante una situación de contingencia que afecte a los recursos de la institución.
- Probar la efectividad y los tiempos de respuesta del Plan para comprobar que están alineados con la definición realizada en el diseño.
- Identificar las áreas de mejora en el diseño y ejecución del Plan.
- Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.
- Evaluar si los involucrados están suficientemente familiarizados con la operativa en situación de contingencia.
- Concienciación y formación para los empleados a través de la realización de pruebas.
- Validar la habilidad de los funcionarios y la consistencia de los procedimientos en eventos de recuperación de siniestros.
- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Facilitar la divulgación y el entrenamiento de los procedimientos y guías de recuperación.
- El responsable del Equipo de Recuperación Tecnológica deberá evaluar que sean definidas las responsabilidades de las pruebas del plan, tales como:
- Personal de administración: Grado de participación y compromiso, niveles jerárquicos de aprobación y asignación de recursos, capital y tiempo.
- Personal involucrado del área de tecnología como área de desarrollo, infraestructura, seguridad y soporte técnico.
- Grupo de usuarios por Unidad Administrativa.

- Personal externo: proveedores y grupos de apoyo internos o externos.

3.4.1.2. Caracteristicas de las pruebas

Para efectuar las pruebas del Plan de Contingencia de TIs, se deben considerar dos características principales:

3.4.1.2.1. Realismo

La utilidad de las pruebas se reduce con la selección de escenarios reales. Por ello es importante reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.

3.4.1.2.2. 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 para el negocio, este tipo de pruebas se las realizará de manera programada y en horas que no impacte al normal desenvolvimiento de las actividades del negocio.

3.4.1.3. Requerimientos generales

Los involucrados en el Plan de Contingencia de TIs de la Dirección de Sistemas de Información, que constan en la ETAPA III- DESARROLLO DEL PLAN, ORGANIZACIÓN DE LOS EQUIPOS DE RECUPERACIÓN, deben ser capacitados en los siguientes aspectos:

- Introducción al Plan de Contingencia de TIs.
- Arquitectura de la red LAN y WAN del Banco del Estado.

Lo anterior les faculta para estar en conocimiento de la plataforma tecnológica institucional; así como también estar en conocimiento de las labores que deben desempeñar en caso de una contingencia tecnológica.

El Equipo de recuperación tecnológica y el personal de la Dirección de Sistemas de Información identificarán y documentarán los niveles de prueba del plan. Estos pueden ser por segmentos, por aéreas relacionadas o en gran escala como prueba global del plan, según los lineamientos que establezca el Plan de Contingencia de TIs.

3.4.1.4. Tipos de pruebas

Como métodos de prueba se plantean: simulación o real, parcial o global del plan, a realizarse a criterio del responsable del Equipo de Recuperación Tecnológica.

3.4.1.5. Elaboración de pruebas y cronogramas

Es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y del personal se han ensayado durante un período de tiempo.

Para el desarrollo de las pruebas, y dado que existen muchas combinaciones posibles de los escenarios descritos, se sugiere como mínimo el siguiente un cronograma de pruebas:

PRUEBA	ESCENARIO	TIPO DE PRUEBA	AREAS INVOLUCRADAS	PERIODO SUGERIDO DE PRUEBA
A	1	PARCIAL	DSI	CADA TRIMESTRE
B	2	PARCIAL	DSI	CADA TRIMESTRE
C	3	PARCIAL	DSI	CADA TRIMESTRE
D	4	GLOBAL	DISPONE PCN	DISPONE PCN
E	5	PARCIAL	SUCURSAL REGIONAL	DISPONE PCN

Se considera efectuar los siguientes pasos para conducir la prueba, en los que el responsable de la Dirección de Sistemas de Información indicará al representante del Equipo de Recuperación Tecnológica el esquema ordenado de las pruebas conforme lo siguiente:

1. Selección del funcionario/s o área/s que intervendrán en la prueba para identificar los aspectos o capítulos del plan que están siendo evaluados.
2. Descripción de los objetos de la prueba y mecanismos de medición.
3. Comunicación formal de una prueba anunciada con los factores críticos a considerar y el tiempo estimado de la prueba.
4. Consolidación de resultados.
5. Evaluación de resultados: progresos, inconvenientes y logros.
6. Determinación de las implicaciones de los resultados de la prueba. Se debe analizar si el resultado de un caso simple o no.
7. Generación de recomendaciones para cambios o ajustes; se incluirán definiciones de fechas límite para respuesta y gestión.
8. Notificación de resultados de las pruebas a los equipo del Plan de Contingencia de TIs o a las autoridades pertinentes de ser el caso.

9. Efectuar los cambios en documentos de las recomendaciones emitidas de ser el caso.

3.4.1.6. Elementos a evaluar en los planes de pruebas

Para la ejecución de un plan de pruebas se requerirá de la ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y Centros Alternos de Operaciones (Manabí) para asegurar un rendimiento adecuado.

Los elementos que el equipo de pruebas evaluará y verificará en un ejercicio de simulación son:

- Los Procedimientos de:
    - Emergencia.
    - Notificación Servidores / Clientes.
    - Recuperación de archivos y documentación almacenados en lugares externos.
    - Recuperación de datos (BDD).

- Conectividad de:
    - Líneas de telecomunicaciones de backup.
    - Capacidad y rendimiento del hardware.
    - Portabilidad del software.
    - Accesibilidad al Centro Alterno de Cómputo.

- La Disponibilidad de:
    - Equipos de soporte (aire acondicionado, unidades ininterrumpidas de corriente eléctrica).
    - Soporte logístico: provisiones, transporte y comunicaciones.

- Las habilidades de:
    - Movilización de los equipos de trabajo.
    - Resolución del Equipo de Recuperación Tecnológica para determinar la prioridad de sistemas cuando se procesa recursos computacionales limitados.
    - Habilidad para recuperar y procesar en forma satisfactoria sin personal clave, asumiendo la ausencia de personal.
    - Habilidad de entrada de datos para alimentar sistemas críticos utilizando las instalaciones del área de soporte externo.
    - Habilidad de los usuarios para continuar con las operaciones normales de la entidad para los sistemas clasificados como no críticos.
    - Habilidad para establecer contacto en un periodo definido por emergencia y de manera organizada, con el personal clave o sus designados alternos.
    - Nivel de cumplimiento de los estándares normativos aprobados por la entidad.
    - Aplicación parcial, total o nula de medidas de seguridad durante el periodo de emergencia.
    - Mecanismos de recuperación de información perdida en caso de sistemas en línea.
    - Análisis de tiempos durante las pruebas.

3.4.1.7. Sugerencias Adicionales

Los ejercicios de test son ejercicios planificados que implican la restauración real de la capacidad del Centro de Cómputo Principal (Quito) y Alterno (Manabí). Generalmente, los procesos en producción no son interrumpidos, pero se puede planificar su restauración y validación en el Centro Alterno de Cómputo.

Este tipo de prueba, es guiado por el Plan de Contingencia de TIs Institucional y requiere la participación de toda la institución, incluyendo usuarios, personal técnico y de operaciones.

3.4.2. ELABORACIÓN DEL PLAN DE MANTENIMIENTO DEL PLAN DE CONTINGENCIA DE TIs.

Por la propia dinámica de negocio del Banco del Estado, 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 Contingencia de TIs evitará que quede en poco tiempo obsoleto y que en caso de contingencia no se pueda dar respuesta a las necesidades.

Periódicamente se efectuará las siguientes tareas para verificar que el Plan de Contingencia esté actualizado:

- Revisar si no haya existido alguna modificación en algún componente de infraestructura o hardware, así como en alguno de los sistemas o aplicaciones que impliquen realizar alguna adición o modificación a los procedimientos o procesos descritos en el Plan de Contingencia de TIs.
- Llamar a los teléfonos de los miembros del Equipo de Recuperación Tecnológica, detallados en el Plan de Contingencia de TIs.
- Verificar los procedimientos que se emplean para almacenar y recuperar los datos (proceso de backup).

3.4.3. Avisos de cambios al plan.

REV	FECHA	ALTERACION	OBSERVACIONES
00	01/2014	Generación del documento Plan de Contingencia Informático	
01	03/2014	Actualización el los integrantes del Equipo de Recuperación Tecnológica	
02	04/2014	Actualización del Índice de Contenidos	
03	05/2014	• Inclusión de hoja de Descripción de las Revisiones • Actualización de registro de Integrantes del Equipo de Recuperación • Inclusión del escenario 4, fallas en alguna Sucursal Regional	
04	06/2014	Ampliación de la FASE IV – PRUEBAS Y MANTENIMIENTO	
05	08/2014	Revisión completa del documento	En proceso

4. CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- La aplicación de esta guía para el desarrollo de Planes de Contingencia para tecnologías de información, servirá de gran aporte a las instituciones que apalanquen sus procesos de negocio en las tecnologías de información, logrando mejorar la disponibilidad de su infraestructura tecnológica y brindando confianza a los usuarios internos y externos de la entidad. El principal efecto será mejorar la productividad del negocio de la organización, debido que se podrá contar con una infraestructura tecnológica más confiable, con menos caídas y se podrá contar con mejores tiempos de respuesta en lo que a resolución de problemas en procesos tecnológicos se refiere.

- El proceso de investigación para el desarrollo del Plan de contingencia para las tecnologías de información, propuesto en esta tesis, permite además de los beneficios ya conocidos evaluar y diagnosticar el estado actual de la infraestructura tecnológica de las empresas, para el caso de estudio de esta investigación "Banco del Estado", gracias al análisis de cada proceso se pudieron determinar vulnerabilidades importantes. Al contar con estudios de Ethical Hacking que sirvieron de guía para esta investigación se pudieron determinar y minimizar diferentes riesgos de seguridad informática

- La diferencia para las empresas entre contar o no con un Plan de Contingencia para las tecnologías de información, puede contemplar inclusive el cese de las actividades de negocio en caso de un incidente tecnológico de alta magnitud, que perjudique sus principales procesos. Por ello, como parte de la gestión de seguridad, es importante considerar como prioritario desarrollar un Plan de Contingencia para estar preparados ante cualquier incidente.

- Para el caso de estudio de esta tesis "Banco del Estado", el Plan de Contingencia generó una base de datos de la infraestructura tecnológica de la empresa, que permite documentar a un nivel de detalle los elementos que componen los procesos tecnológicos, de forma que se optimizan los tiempos de los trabajos técnicos de actualización o corrección de los diferentes elementos que conforman la infraestructura tecnológica y estos se los pueda realizar con seguridad.

- Esta guía está orientada a contemplar la contingencia de los principales procesos tecnológicos de las empresas sin embargo no existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que se realizan en los diferentes tipos de negocios y en sus respectivos Centro de Procesamiento de Datos, sin embargo esta investigación se ha centrado en incorporar las etapas esenciales de un plan de contingencia de TIs, para aplicarlos a nivel general en cualquier giro de negocio, muestra de esto es la aplicación para el caso de estudio "Banco del Estado".

- Es importante mencionar que para que una empresa pueda reaccionar adecuadamente ante procesos críticos en su infraestructura tecnológica, es fundamental poner en práctica la etapa de pruebas y el mantenimiento del Plan de Contingencia, de esta manera se podrán realizar los cambios necesarios al plan desarrollado.

4.2. Recomendaciones

- Es importante programar las actividades propuestas en el presente Plan de Contingencias para las tecnologías de información, de esta manera se podrá contar con un verdadero contingente para las tecnologías de información y se podrá contar con un respaldo de los principales procesos tecnológicos de las empresas, logrando así la continuidad en las actividades del negocio.

- Se debe informar a todo el personal que labora en las diferentes empresas, para el caso de estudio de esta tesis “Banco del Estado”, es importante que cada uno de los funcionarios de esta entidad, conozcan a nivel general el contenido del presente Plan de Contingencia para las tecnologías de información, con la finalidad conocer las diferentes funciones que cada área desempeñará en caso de activarse una contingencia.

- Es importante mantener actualizado y realizar pruebas periódicas al Plan de Contingencia para las tecnologías de información, para verificar la efectividad de las acciones en caso de la ocurrencia de diversos incidentes contemplados en esta

investigación para tener la seguridad de que se cuenta con una contingencia adecuada.

5. BIBLIOGRAFÍA

- Documento de referencia Plan de Recuperación, materia de curso gestión de Redes de telecomunicaciones, Maestría en redes de comunicaciones - http://pucemoodle.puce.edu.ec/pluginfile.php/66785/mod_resource/content/1/documentos_curso/documento_maestria_puece.pdf
- http://www.disaster-recovery-guide.com/ - Información y guías sobre Continuidad
- http://www.nist.org/ - Mejores prácticas en Seguridad Informática
- http://www.contingencyplanning.com/ - Revista de Continuidad de Negocio
- http://www.globalcontinuity.com/ - Portal de Business Continuity Plan
- http://www.thebci.org/pas56.htm - Business Continuity Institute
- http://www.securityfocus.com/ - Base de datos de vulnerabilidades
- http://www-5.ibm.com/services/es/portfolios/recuperacion.html - Proveedor de Servicios de Continuidad de Negocio
- Anexos proporcionados por la Entidad.

ANEXOS