



**UNAPEC**  
**UNIVERSIDAD APEC**

**DECANATO DE POSGRADO**

**Tesis de Maestría para optar por el título de:  
Maestría en Gerencia y Productividad**

**“Modelo de revisión de Plan de Recuperación Ante Desastres de Tecnología  
en un Banco Múltiple, para el año 2019”**

**SUSTENTANTE:**

Luis Montas  
2005-0632

**ASESORA:**

Dra. Iara V. Tejada

Santo Domingo, República Dominicana.  
Julio 2019

**MODELO DE REVISIÓN DE PLAN DE RECUPERACIÓN  
ANTE DESASTRES DE TECNOLOGÍA EN UN BANCO  
MÚLTIPLE, PARA EL AÑO 2019.**

## **RESUMEN**

El presente trabajo de investigación tiene como objetivo proponer un modelo de revisión de Plan De Recuperación Ante Desastres De Tecnología en un Banco Múltiple; el principal objetivo es la revisión del Plan De Recuperación Ante Desastres De Tecnología para mantener la operatividad de la organización en caso de incidente o desastres natural, este plan está focalizado en la estrategia de recuperación de una organización que aporta la continuidad de la misma aportando beneficios directo a la empresa incorporando áreas y procesos críticos y al mismo tiempo crear cultura de la gestión de continuidad del negocio en la organización. El Plan De Recuperación Ante Desastres De Tecnología que contempla todos los componentes de la norma ISO 22301, sobre implementación de Gestión de Continuidad del Negocio, así como también otros autores redactan diferentes definiciones de Plan de Recuperación Ante Desastres de Tecnología y lo que es la Gestión de Continuidad del Negocio alineado a la Gestión en las empresas u organización. Para esta investigación se realizará una evaluación del modelo de Plan De Recuperación Ante Desastres De Tecnología de un Banco Múltiple y con este realizar una propuesta para modelo de revisión del mismo, mediante reuniones con representantes del área de TI, recolección de datos y observaciones a los diferentes planes que veamos, adicionalmente esta investigación será apoyada por el conocimiento y la experiencia del tema tratado. En resumen, los resultados arrojaron que hay diferentes métodos para la recolección de datos para realizar el Plan de Recuperación ante Desastres de Tecnología.

## **Dedicatorias y Agradecimientos:**

El presente trabajo de investigación está dedicado primero a Dios, por la salud que nos brinda, darnos la fortaleza necesaria en los momentos de dificultades y en el proceso de conseguir nuestra metas y proyectos que nos proponemos.

A mis padres Mélida Rojas y Claudio Montas por su amor incondicional, todo el trabajo, formación, comprensión, sacrificio y toda la confianza en todos estos años, gracias a ustedes y a todo su esfuerzo he logrado llegar a donde estoy y ser quien soy hoy. Gracias infinitas por los valores y principios que con mucho esfuerzo me brindaron a mi como también a mis hermanos, siempre me dijeron ese sabio consejo que me prepare a nivel profesional, les puedo decir que les cumplí y no los defraudare. Puedo decir que he sido bendecido por Dios y siento un gran orgullo de tenerlos ustedes como mis padres, son los mejores padres del mundo, Simplemente GRACIAS.

A mis hermanos Erick Montas y Pavel Montas por siempre estar presente, con su apoyo incondicional desde siempre y estar conmigo en todos los momentos malos y buenos.

A toda mi familia y familia de mis esposas porque también forman parte de mi crecimiento y de esta meta que acabo de cumplir por sus oraciones, sus consejos y palabras de aliento que de una u otra forma me ayudaron y me siguen ayudando todo el tiempo.

A mi esposa Solanyi Pujols y mi hija Camila Montas Pujols, que son mi razón para seguir avanzando, gracias por el apoyo, comprensión en todo este proceso agotador, las amo con todo mi corazón a ambas.

Finalmente agradecer a mis compañeros de tesis, a todos los docentes de la Universidad APEC, por compartir sus conocimientos, por apoyarnos en este proceso, a todos muchas gracias por abrirnos las puertas y servirnos de guía en esta maestría.

# INDICE

|                                                                                                                 |    |
|-----------------------------------------------------------------------------------------------------------------|----|
| INTRODUCCIÓN                                                                                                    | 1  |
| CAPÍTULO I: FUNDAMENTOS PLAN DE RECUPERACIÓN ANTE DESASTRES DE TI                                               | 4  |
| 1.1 Concepto Plan de Recuperación ante Desastres de TI .....                                                    | 4  |
| 1.2 Componentes del Plan de Recuperación ante Desastres de TI.....                                              | 5  |
| 1.3 Análisis de Impacto de Negocio (BIA).....                                                                   | 10 |
| 1.4 Norma ISO 22301 .....                                                                                       | 12 |
| 1.5 Los procesos críticos .....                                                                                 | 13 |
| 1.6 Importancia de la implementación de un Plan de Recuperación ante Desastres de TI                            | 14 |
| CAPÍTULO II: ANÁLISIS DE LA ENTIDADES FINANCIERA DE CARA A UN PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA | 18 |
| 2.1 Historia del Plan de Recuperación Ante Desastres de Tecnología de una empresa                               | 18 |
| 2.2 Plan estratégico y estructura organizacional de una organización.....                                       | 19 |
| 2.3 Diagnostico de las Empresas de Cara a un Plan de Recuperación Ante Desastres de Tecnología. ....            | 20 |
| 2.4 Nivel de Madurez de cara a Plan de Recuperación ante Desastres de TI                                        | 32 |
| 2.5 Proceso de documentación y aprobación en la organización .....                                              | 33 |
| 2.5.1 Documentación .....                                                                                       | 34 |
| 2.5.2 Evaluación .....                                                                                          | 35 |
| 2.5.3 Mejora Continua.....                                                                                      | 38 |

|                                                                                                                                                   |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----|
| CAPÍTULO III: PROPUESTA DE IMPLEMENTACIÓN DE MODELO DE REVISIÓN<br>DE PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA EN UN<br>BANCO MÚLTIPLE   | 43 |
| 3.1 Impacto de en las entidades financieras .....                                                                                                 | 53 |
| 3.2 Requisitos para realizar una Plan de Recuperación ante Desastres de TI.<br>55                                                                 |    |
| 3.3 Beneficios que tienen las entidades financieras de tener un Plan de<br>Recuperación ante Desastres de TI alineado a las buenas prácticas..... | 56 |
| CONCLUSIONES                                                                                                                                      | 60 |
| BIBLIOGRAFIA                                                                                                                                      | 62 |

## LISTA DE GRÁFICOS

| GRÁFICO | DESCRIPCIÓN                                                                                                                                                                  | PÀG |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1       | Ejemplo de planes que están incluidos en la Gestión de Continuidad del Negocio                                                                                               | 09  |
| 2       | Estructura organizacional la Área de Riesgo y Área de TI                                                                                                                     | 20  |
| 3       | La empresa cuenta con un Plan De Recuperación Ante Desastres De Tecnología                                                                                                   | 23  |
| 4       | Tiene acceso a poder ver el documento                                                                                                                                        | 24  |
| 5       | Sabe usted quienes son los responsables de documentar/actualizar estos documentos                                                                                            | 25  |
| 6       | Tiene usted conocimiento de las pruebas de contingencia que se realizan en su organización                                                                                   | 26  |
| 7       | Considera usted importante que su organización tenga un Plan De Recuperación Ante Desastres De Tecnología                                                                    | 27  |
| 8       | Entiende usted que el Plan De Recuperación Ante Desastres De Tecnología abarca todas las aplicaciones críticas de su organización                                            | 28  |
| 9       | Considera que se debe agregar algún punto o algún anexo al Plan De Recuperación Ante Desastres De Tecnología                                                                 | 29  |
| 10      | Tiene conocimiento si cuando se realizan las pruebas de contingencia las mismas tienen los procesos bien documentado en el Plan De Recuperación Ante Desastres De Tecnología | 30  |
| 11      | Sabes cuál es el flujo de aprobación para el plan                                                                                                                            | 31  |
| 12      | Entiende que el Plan De Recuperación Ante Desastres De Tecnología está alineado con la estrategia de la organización                                                         | 32  |
| 13      | MODELO DE REVISIÓN DE PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA                                                                                                      | 45  |

## LISTA DE TABLAS

| TABLA | DESCRIPCIÓN                               | PÀG |
|-------|-------------------------------------------|-----|
| 1     | Resultado de entrevista de la pregunta 1  | 22  |
| 2     | Resultado de entrevista de la pregunta 2  | 23  |
| 3     | Resultado de entrevista de la pregunta 3  | 24  |
| 4     | Resultado de entrevista de la pregunta 4  | 25  |
| 5     | Resultado de entrevista de la pregunta 5  | 26  |
| 6     | Resultado de entrevista de la pregunta 6  | 27  |
| 7     | Resultado de entrevista de la pregunta 7  | 28  |
| 8     | Resultado de entrevista de la pregunta 8  | 29  |
| 9     | Resultado de entrevista de la pregunta 9  | 30  |
| 10    | Resultado de entrevista de la pregunta 10 | 31  |



# INTRODUCCIÓN

## INTRODUCCIÓN

El plan de recuperación ante desastres de tecnología es fundamental para una entidad financiera, teniendo en cuenta cuáles son sus aplicaciones más críticas sus respectivas estrategias de recuperación y procedimientos en caso de incidentes, esto siempre referenciado de la norma ISO 22301.

De acuerdo a la norma ISO 22301 existen elementos que son esenciales para un plan de recuperación ante desastres de tecnología sin embargo dependiendo de la madurez de la entidad financiera se realizara el plan sin dejar de colocar estos elementos esenciales.

Por el conocimiento y experiencia en general de la empresa, se realizan diferentes procesos antes de tener el documento de Plan De Recuperación Ante Desastres De Tecnología, dentro de ellos está la recolección de datos observación para obtener las informaciones, se evaluará los planes de negocios y el análisis de impacto de las aplicaciones y así tener base para la realización del modelo.

Esta propuesta es basada en la experiencia y conocimiento en el plan de recuperación ante desastres de tecnología enfocado en la mejora continua, con la finalidad de poder implementar esta propuesta.

Las instituciones financieras en la Republica Dominicana, están reguladas por la Ley Monetarias y Financieras del año 2002 (Ley No. 183-02), en la Sección V: de la transparencia financiera, el Artículo 51: de la Documentación de las operaciones y suministro de informaciones: establece la obligatoriedad de las entidades financieras a documentar las operaciones y el tiempo de custodia de estas. (Superintendencia de Bancos, 2002)

Al mismo tiempo está el Depto. de Auditoría quien a su vez realiza revisión de toda la documentación de la entidad, para esto cada departamento debe considerar proceso o procesos para tener la documentación con fácil acceso y actualizado al momento que las áreas pertinentes le soliciten. La información documentada sirve como evidencia de las actividades y al mismo tiempo sirve como insumo para las diferentes áreas que requieran apoyare en la misma.

Entendiendo lo anteriormente mencionado las organizaciones debería de tener un plan de recuperación ante desastres de tecnología, actualizarlo anualmente y al mismo tiempo realizarlo pruebas de contingencia periódicamente esto ayuda a optimizar el mismo e ir aplicando la mejora continua en procesos críticos y sistemas que ameriten la inclusión de proveedores o áreas que formen parte de la organización.

Por esta razón se necesita mucha responsabilidad por parte de las partes pertinentes que administran el plan de recuperación ante desastres de tecnología tanto TI como el área de Riesgos deben implementar métodos de para la realización revisión y actualización del mismo cuando sea necesario y en caso de que el plan amerite cambio.

La presente investigación se presentará en 3 capítulos. El primer capítulo se desarrolla conceptos, fundamentos, normas y generalidades de un plan de recuperación ante desastres de tecnología. En el capítulo dos (2), se realizará un análisis las entidades financieras evaluando el nivel de madurez de las misma en cuanto plan de recuperación de ante desastres de tecnología. En el capítulo (3) se presentará una propuesta de implementación de modelo de revisión de plan de recuperación ante desastres de tecnología en un banco múltiple

Cabe destacar que la entidad objeto de estudio no autorizó el uso de la información de por tanto no será posible obtener documentos referentes al tema en gestión por tal razón este informe se basa en la experiencia y resultados de la encuesta. En cuanto la propuesta la implementación permanecerá a consideración.

## **CAPÍTULO I**

# **CAPÍTULO I: FUNDAMENTOS PLAN DE RECUPERACIÓN ANTE DESASTRES DE TI**

En este capítulo se presentarán conceptos de diferentes fuentes, autores sobre Plan De Recuperación Ante Desastres De Tecnología con la finalidad de introducción a los lectores.

## **1.1 Concepto Plan de Recuperación ante Desastres de TI**

En esta sección se transcribirá algunos conceptos de plan de recuperación ante desastres de tecnología.

Según Rodríguez, 2012 un plan de recuperación de desastres es la estrategia que se seguirá para restablecer los servicios de TI dígase Hardware y Software, el mismo se utiliza luego de haber sufrido afectación por catástrofe natural, Fallas masivas (Luz, fallas en edificios, etc.), danos premeditado (secuestro de la información, ransomware, hackeos).

Según Byron Vicente, 2015 es el proceso planificado que una organización utiliza para recupera el acceso a su infraestructura (software, datos y Hardware) que son necesarios para reanudar el ejercicio de las funciones normales de trabajo, críticos después del evento ya sea de un desastre natural o una catástrofe causada por los seres humanos.

Según Beal, 2007 Plan de Recuperación ante Desastres de Tecnología es un plan en el que se establece la recuperación para la continuidad del negocio que afecte un área un proceso critico o el negocio por completo, agregando a esto los equipos de tecnología, base de datos y data center de las organizaciones.

Existe diferentes definiciones de acuerdo a los autores, en conclusión, el Pla de recuperación ante desastres de tecnología es el documento donde se establece las estrategias de recuperación procesos y sistemas o aplicaciones críticas de una organización para en caso de un incidente o desastres mantener la operatividad del

negocio o poder recuperarlo al menor tiempo posible y al menor costo a nivel de pérdida.

## **1.2 Componentes del Plan de Recuperación ante Desastres de TI**

En esta sección se transcribirá algunas terminologías de un Plan De Recuperación Ante Desastres De Tecnología alineados a la norma ISO 22301 y también términos importantes que deben estar en el documento.

El plan de recuperación de desastres de tecnología – Disaster Recovery Plan DRP centra su atención en la recuperación de los servicios de TI y sus recursos, para aquellos casos en lo que algún evento ocasiona una interrupción significativa en su funcionamiento, por ejemplo, explosión, falla prolongada de electricidad, incendio, inundación, terremoto, etc.

Un DRP (Disaster Recovery Plan) o Plan de Recuperación de Desastres, es la forma en que las organizaciones se enfrentan y preparan contra posibles desastres (naturales o no) que puedan dañar su infraestructura tecnológica y por ende poner fin a sus actividades. En pocas palabras, un DRP es la estrategia y acciones a seguir para restablecer los servicios de TI (Hardware y Software) ante cualquier eventualidad.

“RPO (Recovery Point Objective) se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. ¿Las transacciones de cuánto tiempo estamos dispuestos a perder, o a tener que reintroducir al sistema?”

“La respuesta va a depender del volumen de transacciones por unidad de tiempo, y de los mecanismos de backup, pero siempre aumenta el volumen de datos ‘huérfanos’ a medida que pasa el tiempo desde la última copia de seguridad.”

El RPO determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación.

“RTO (Recovery Time Objective) expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.”

“La respuesta dependerá de la criticidad de cada aplicación. Aquí de nuevo debemos analizar cada caso; no será lo mismo la aplicación que da servicio a las cajas en una gran superficie, que la aplicación para el cálculo de la nómina, que se ejecuta una vez al mes.”

Cuando se habla de RTO se tiene que considerar la detección del incidente, razón del mismo (no necesariamente de una vez, pero se debe saber que lo ocasionó), como se va a reaccionar, planes, movilización de personas y proveedores, procesos o personal críticos, tiempo de la decisión para activar plan o planes, se debe determinar qué áreas son la más críticas si se pueden movilizar a otra área, de acuerdo a RTO o RPO, que posibles error pudiera pasar como solventarlo documentarlo para próximas situaciones, documentar también las lecciones aprendidas darle seguimiento a las mismas.

En el momento que ocurre una crisis la activación de los planes es una decisión de la empresa dígase tiempo para la misma y tolerancia existen otros casos que son los riesgos que tiene empresa costos perdidas por lo que etsa decisión no es fácil.

Dentro de un Plan de Recuperación de Desastres de Tecnología existe también el MBCO (Minimun Business Continuity Objective. La principal tarea de este término es establecer el mínimo tiempo que la empresa o negocio puede mínimo nivel aceptable para mantener un servicio con la finalidad de alcanzar sus metas o acuerdos de negocios en caso de un desatares o emergencia.

También dentro del Plan de Recuperación de Desastres de Tecnología está el MTPD (Maximun Tolerable period of disruption) tiempo máximo tolerable que puede aceptar una organización sin tener disponible un servicio proceso u operación

del negocio, el mismo se debe definir antes del RTO ya el tiempo que se puede tolerar la indisponibilidad sería igual al MTPD.

Este es un componente esencial para la gestión de continuidad del negocio con la finalidad de saber qué tiempo puede aguantar un proceso que el mismo no esté disponible por tanto se debe ser bien preciso para identificar este tiempo MTPD ya que el mismo no puede ser igual que el RTO se debe evaluar todos los elementos no exagerar de la flexibilidad, ya que este elemento puede brindar a los responsables de cada proceso evaluar y analizar muchos componentes antes de activar plan.

Partiendo que la recuperación de desastres es el método para responder ante un incidente que interrumpa los servicios críticos de la organización existen procesos o documentación que están para restablecer las funciones críticas de la empresa. Adicionalmente pruebas y análisis de cantidad considerable de pérdida en caso que el incidente que afecte directamente la operatividad del negocio.

El proceso de recuperación de los sistemas va atado a muchas aristas adquirir nuevos equipos (Hardware) mantenimiento constante, pruebas entre otros, contacto directo con proveedor para actualización de software, parche de seguridad, mantener el servicio en condiciones óptimas para su uso en caso de emergencia pueda funcionar de la mejor manera posible, capacidad de almacenamiento en caso que el sistema amerite, back up necesarios para uso en caso que se necesite, análisis de tiempo estimado de recuperación para cuando se necesite utilizar el sistema alternativo o backup, (RPO) para este se necesita realizar pruebas de contingencia de forma periódica y validar que todo los sistemas funcionen y estén dentro del SLA y RPO acordado.

Adicionalmente las estrategias de respaldo y siempre monitoreo de los sistemas con la finalidad de estar al tanto de cada situación para mejora continua en los sistemas. El proceso de monitoreo se hace en conjunto con el área de Tecnología ya que ellos tienen sus aplicaciones y colaboradores designados para esta tarea y establecer protocolos para notificación de cara afectación de los sistemas o aplicaciones críticas de la organización.



SLA acuerdo de nivel de servicio la finalidad de los SLA es tener documentados lo compromiso u objetivos que se deberían cumplir con los clientes o suplidor. SLA detallan los acuerdos o los compromisos acordados entres suplidor y cliente.

OLA es muy parecido a los SLA sin embargo este es acuerdo a nivel operación con los usuarios de la organización, se enfoca mucho en compromiso acordado en TI y los usuarios quienes demandan soluciones a equipo técnico ya sea TI completo o equipo de seguridad de información. En algunas organizaciones se firman documento o se presenta documentación para quede como documentación y así se establece la responsabilidad de los servicios que se necesitan entregar con su tiempo estimado y siempre con la autorización y aprobación de ambas partes por ejemplo área de desarrollo y área de negocios.

BCP y DRP estos dos términos son muy utilizados en las organizaciones, pero se debe tener bien claro la diferencias de los mismos, ambos son utilizados para recuperación de operaciones o procesos críticos del negocio u organización en caso de que un incidente afecte el mismo. Sin embargo, existan algunas diferencias entre BCP y DRP unas de las más evidentes o principales diferencias que tiene estos planes es el alcance que tiene para una organización.

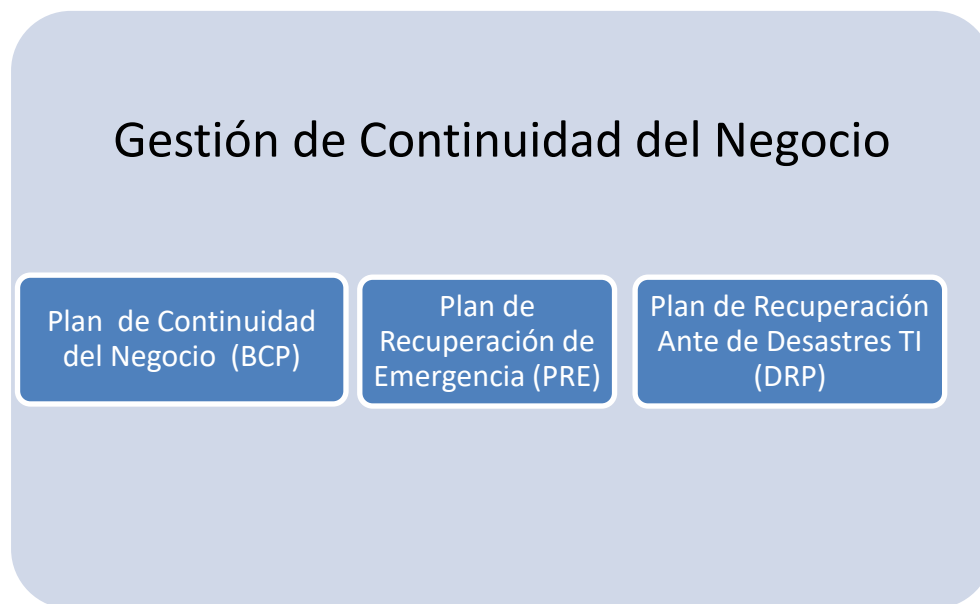
BCP Business Continuity Plan proceso que involucra prevención recuperación ante incidentes o que tan rápido se puede recupera ante un desastre. DRP recuperación de la organización que abarca los datos (hardware y Software). Ambos términos son herramientas importantes para la recuperación de sistemas críticos, esté disponible cuando se requiera o se necesite por tanto el DRP va orientado a los procesos de TI del negocio, y está incluido dentro BCP que está orientado al negocio.

La continuidad en las organizaciones está orientada a que cuando la mismo deje de funcionar por algún incidente desastres o sea ocasionado por sistemas, algo natural (onda tropical), humano, robo, siniestro huracán entro otros, entre en acción el BCP (Business Continuity Plan) plan de continuidad del negocio. Este tiene documentado el procedimiento especifico o que se debe hacer, a quien llamar, que

proceso son los más críticos, que recursos se necesitan para que la organización pueda restablecerse esto va de la mano con RPO y RTO que están incluido en el DRP con los sistemas o aplicaciones críticas del negocio.

Dentro de la organización existen planes estratégicos todos estos planes deben estar alineados a la estrategia del negocio de ninguna manera no debería ser así esto está establecido en la norma ISO 22301 que se hace referencia en esta propuesta, por tanto, el punto inicial o punto de partida para realizar el BCP o DRP dentro de una organización seria que ambos deben estar alineado a la estrategia de la organización o empresa que requiera estos planes. Ver ejemplo en Gráfico 1.

**Gráfico 1:** Ejemplo de planes que están incluidos en la Gestión de Continuidad del Negocio.



**Fuente:** Elaboración Propia

La columna vertebral de un BCP o DRP o de la continuidad el negocio a nivel general es el BIA en este se documenta todos los procesos de todas las áreas se establecen los RTO o RPO MTPD.

Dentro del Plan De Recuperación Ante Desastres De Tecnología existe diferentes términos que cada uno de ellos tiene su importancia dentro del plan cada uno de estos elementos forman parta de indicadores para definición del proceso y

orden de recuperación en cuanto a los diferentes sistemas que tiene un Plan De Recuperación Ante Desastres De Tecnología.

Luego que se establecen estos tiempos en conjunto con el área de tecnología se debe validar esta información con las áreas que interactúan con estas aplicaciones específicamente con los líderes estos a su vez cuando tengan sus respectivos planes de negocios debe validar que estas informaciones estén alineadas entre el Plan De Recuperación Ante Desastres De Tecnología y el plan del negocio.

Como ya tenemos el conocimiento el Plan De Recuperación Ante Desastres De Tecnología debe estar alineado a la estrategia del negocio actualmente las organizaciones están muy orientadas a lo digital por ende todo este tema de Plan De Recuperación Ante Desastres De Tecnología es de suma importancia en la vida útil de una organización.

Cabe destacar que las organizaciones tienen diferentes política y método para la elaboración, documentación y divulgación del Plan De Recuperación Ante Desastres De Tecnología, así como también de los otros planes también la multiplicación, cultura y concientización dentro de los colaboradores que interactúan o no con los planes para mantener la operatividad del negocio. Sin embargo, todas deberían estar alineado a la norma ISO 22301 así como también a los requerimientos por las auditoría internas y externas y también por la Superintendencia de Banco que sirve como regulador de las entidades financieras.

### **1.3 Análisis de Impacto de Negocio (BIA)**

En este acápite se transcribirán algunas definiciones de Análisis de Impacto de Negocio, importancia y beneficio del mismo.

Según Amayá, 2012 El análisis de impacto al negocio (Business Impact Analysis o BIA por sus siglas en inglés) es otro elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.

Según Cobser, un Análisis de Impacto en el Negocio (BIA, en sus siglas en inglés) es un estudio detallado de departamentos, actividades, dependencias e infraestructuras que proporciona una comprensión de cómo la organización proporciona a sus clientes productos y servicios críticos y el coste que supondría una interrupción de negocio a la organización a medida que avance el tiempo sin volver a la normalidad.

Según Juan Martínez, un Análisis de Impacto es proporcionar a la dirección la información necesaria para que pueda tomar decisiones en el desarrollo de su estrategia de continuidad. Para ello, el Análisis de Impacto debe determinar el grado de criticidad de dichas funciones en la razón de ser de la organización y el tiempo máximo a partir del cual, la interrupción de cada una de ellas es inaceptable.

El Análisis de Impacto de Negocio (BIA) es un proceso sistematizado donde se identifican los procesos neurálgicos de su negocio y se realiza una evaluación sobre qué sucedería si ese proceso se afecta por algún evento tecnológico.

El objetivo principal de análisis de impacto de negocio es delimitar los procesos, establecer mínimos y máximos de la recuperación de los procesos para que en caso de interrupción saber el impacto de cada proceso en la entidad financiera.

Adicionalmente cuales serían los recursos, proveedores que se necesitarían para recuperar un área incluyendo todos los aspectos relevantes en este proceso de recuperación.

Los beneficios del BIA (Análisis de Impacto de Negocio) definición de procesos y/servicios críticos relacionado en cada producto y servicios, definir vulnerabilidades que tiene la entidad financiera para la continuidad de las operaciones, validar que los planes de negocio cubran las necesidades de la entidad, la realización del BIA es vital para la realización de estrategia de recuperación.

Así como también analizar los impactos que puedan verse afectado en una entidad financiera de cara a las operaciones del negocio dentro de estos impactos

y dependiendo de la organización podemos mencionar el impacto financiero, reputación, legal y clientes.

En conclusión, el Análisis de Impacto al Negocio BIA es la columna vertebral de la Gestión de Continuidad Negocio por ende es parte fundaméntela para la realización del plan de recuperación ante desastres de tecnología ya que el en BIA se evalúa las áreas y procesos y ahí parte cuales son los sistemas más críticos de la organización y que estrategia se debería tener para estos procesos o aplicaciones.

#### **1.4 Norma ISO 22301**

En esta sección se citará la norma ISO 22301 la cual establece la realización de un plan de recuperación ante desastres de tecnología, así como también los requerimientos que debe tener el mismo.

Norma ISO 22301 este estándar internacional especifica requerimientos para establecer y gestionar un efectivo sistema de gestión de continuidad del negocio (SGCN), la importancia del mismo es entender la continuidad y necesidades de preparación y la necesidad de establecer una política de gestión de continuidad y objetivos, mejora continua basada en mediciones objetivas, implementar y operar controles y medidas para las gestiones globales de los riesgos.

Un Plan de Continuidad del Negocio BCP (o sus siglas en inglés BCP, por Business Continuity Plan) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre. En los Estados Unidos, las entidades gubernamentales se refieren al proceso como planificación de continuación de operaciones (en inglés Continuity Of Operations Planning, o sus siglas COOP).

La Norma ISO 22301 es como el patrón a seguir para la implementación de un Plan De Continuidad Del Negocio y al mismo tiempo el Plan De Recuperación

Ante Desastres De Tecnología, establece las normas y pautas, cuales aspectos considerar para los planes antes mencionados.

### **1.5 Los procesos críticos**

En este acápite se definirá conceptos de Procesos críticos y la importancia de los mismos en una entidad financiera.

Los procesos críticos son aquellos que al no realizarse sería difícil garantizar el cumplimiento de los objetivos, son procesos significativos a los resultados planteados por una organización y si el desempeño no es el adecuado podrían presentar problemáticas de toda índole.

Dentro de una empresa existen procesos y servicios críticos que son vitales para el funcionamiento y operatividad de la empresa, deben estar bien definidos y documentados por cada área, estos deben estar alineados a la estrategia de la empresa, en caso de una interrupción de algún proceso crítico se debe tener contingencia del mismo ya sea estrategia de recuperación manual o a través de sistemas alternos al mismo, al mismo tiempo cada líder debe determinar el impacto de una interrupción de su proceso crítico.

Según Diego Muñoz podemos definir un proceso crítico como un conjunto de tareas que recorre funcionalmente a una empresa en orden a generar un producto o servicio que es recibido por un cliente.

Los procesos críticos para una organización es la unas de las partes que se deben evaluar los mismo se identifican con cada líder de área, analizando costo por perdida, impacto al negocio, ya sea financiero, cliente, reputación, legal, y se documenta en los Planes De Continuidad De Negocio BCP y Análisis de Impacto al Negocio.

En conclusión, los procesos críticos se documentan en los planes de negocios y estos a su vez con los sistemas en que trabajan estos procesos antes mencionados se documenta en el Plan De Recuperación Ante De Destres De

Tecnología que es en donde se establece también las estrategia y tiempo para recuperación de los procesos críticos.

### **1.6 Importancia de la implementación de un Plan de Recuperación ante Desastres de TI**

En este acápite se citará la importancia de la implementación de un plan de recuperación ante desastres de tecnología en una entidad financiera.

Mediante va pasando el tiempo las organizaciones van creciendo a y necesitan más tecnología, más espacios físicos de ahí parte la importancia de implementación de un Plan De Recuperación Ante Desastres De Tecnología, para establecer estas diferentes estrategias que garanticen la operatividad del negocio ante un incidente.

Según Busto, 2017 Cuando una organización va creciendo con el apoyo de la tecnología y va tomando las medidas necesarias para proteger su información (su bien más importante) y establece las estrategias pertinentes (mediante un DRP) para recuperarla en caso de alguna contingencia (desastre, siniestro), podrá asegurar la continuidad de sus servicios y asegurar la atención de sus clientes, manteniéndose al día con la exigencia de su mercado.

Según Alfaro, 2018 un plan de recuperación establece método de recuperación y continuidad operativa tanto percances menores como también para problemas mayores e indica en 5 pasos la importancia de la implementación de un Plan De Recuperación Ante Desastres De Tecnología, se debe analizar las necesidades de la empresa, realizar evaluación de riesgos, establecer protocolos de recuperación y continuidad operativa capacitar al equipo y probar planes y por ultimo actualizar mantener y mejorar Plan De Recuperación Ante Desastres De Tecnología.

La importancia de implementar un Plan De Recuperación Ante Desastres De Tecnología ayuda a las organizaciones a evitar pérdidas monetarias, óseo impacto financiero, al mismo tiempo una entidad financiera corre otros riesgo o impactos

tales como impacto legal, reputación y de clientes todos estos tienen que ver con que la organización esté operando para los clientes.

En ese mismo orden el compromiso y responsabilidad que debe tener las áreas pertinentes al momento de implementar un Plan De Recuperación Ante Desastres De Tecnología debe ser prioridad ya que afecta directamente con la imagen de la institución u organización que requiera tener este plan.

No solamente es la implementación del Plan De Recuperación Ante Desastres De Tecnología se debe implementar, actualizar, probar ósea realizarle pruebas periódicas de contingencia en el año y aplicarle la mejora continua. Por estos elementos el plan se fortalece año tras año la estrategia de recuperación se debe fortalecer también con mejoras y actualización en los sistemas con la finalidad que se mantengan en óptimas condiciones al momento que se necesite activar el Plan De Recuperación Ante Desastres De Tecnología.

La implementación del Plan De Recuperación Ante Desastres De Tecnología tiene que ir alineado a la estrategia del negocio al mismo tiempo se debe rea concientización y la cultura en las organizaciones del conocimiento de que existe este plan no modo muy técnico sin embargo los líderes de las diferentes áreas deben tener el conocimiento del plan y conocer temas de las estrategias de recuperación ya que las mismas se documentan en los BCP Planes de Continuidad de negocio. Adicionalmente el área de riesgos o continuidad del negocio deben impartir talleres o información vía mail para conociendo del plan con la finalidad de fortalecer cada vez más y orientar a cada colaborado de la existencia de un Plan De Recuperación Ante Desastres De Tecnología.

Estos talleres o reuniones sería con la finalidad de entendimiento de las áreas del Plan De Recuperación Ante Desastres De Tecnología, de hacerle entender la importancia del mismo y saber que su información o sus necesidades en cuanto a las aplicaciones deben estar alineada tanto a sus planes de negocio como también a la estrategia del negocio.



Cabe destacar como mencionamos anteriormente este plan tiene muchos termino muy propio del mismo sin embargo se debe realizar en conjunto con el departamento de tecnología cápsulas o mensajes masivos en caso de no poder realizar o coordinar los talleres, es recomendable comenzar por los líderes de áreas y con la ayuda de estos que se multipliquen los conocimientos en los demás líderes de sus respectivas áreas.

Es importante tener presente que la ayuda el apoyo y seguimiento de las líderes de áreas ósea VP, Gerentes de áreas es de vital importancia para el flujo de la información, conocimiento de las diferentes áreas por tanto el Riesgos de tener un seguimiento a esta tarea a través de pruebas, reuniones talleres entre otros.

Si esta ayuda sería muy difícil la implementación de este plan o también se podría implementar, pero para las pruebas y actualización sería complicados ya que Plan De Recuperación Ante Desastres De Tecnología es una documentación de mejora continua por tanto todos los años ya sea 2-3 y hasta cuatro veces podría actualizarse este documento.

Por esta razón es necesario el aval de la alta gerencia para que el flujo de aprobación en los comités en el área crítica sea de suma importancia la información manejada con la finalidad de la documentación apropiada en el Plan De Recuperación Ante Desastres De Tecnología.

## **CAPÍTULO II**

## **CAPÍTULO II: ANÁLISIS DE LA ENTIDADES FINANCIERA DE CARA A UN PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA**

En este capítulo se presentarán como ha sido el proceso de un Plan De Recuperación Ante Desastres De Tecnología con la finalidad de que los lectores entiendan el proceso de cómo se forma y de donde proviene todo lo relacionado a continuidad del negocio y un Plan De Recuperación Ante Desastres De Tecnología en una organización.

### **2.1 Historia del Plan de Recuperación Ante Desastres de Tecnología de una empresa**

En esta sección se transcribirá historia de un plan de recuperación ante desastres de tecnología de una empresa, responsables, como es manejado como es su flujo de aprobación, entre otros

En las instituciones el Plan De Recuperación Ante Desastres De Tecnología es manejado por el área de Riesgo y continuidad de negocio, así como también el departamento de Tecnología tener en cuenta que existen diferentes entidades que tiene diferentes estructuras organizacionales por tanto no necesariamente están en esta orden.

El área de continuidad del negocio comenzó a organizarse desde 2015 partió haciendo pruebas de contingencia por el área de TI incluyendo también áreas Auditoría Cumplimiento, Riesgos entre otras, desde ese año fue que comenzaron a armar los Planes de Continuidad Negocio, Análisis de Impacto al Negocio y Plan de Recuperación Ante Desastre de Tecnología.

A través del tiempo las organizaciones han sufrido varios cambios por tanto los planes fueron cambiando y actualizando los procesos, sistemas, estrategias fueron también cambiando, siempre alineados a la norma ISO 22301 y al mismo tiempo alineados a la estrategia de la institución.

Ya para la fecha las instituciones tienen un nivel de madurez bastante alto por el tiempo, la experiencia y las constantes pruebas realizadas al Plan De Recuperación Ante Desastres De Tecnología, que tiene mucho que ver con la mejora continua a plan y a los sistemas que están en el plan sin olvidarnos de la estrategia de recuperación que ayuda a recuperar los sistemas.

## **2.2 Plan estratégico y estructura organizacional de una organización.**

El plan estratégico de una organización muy orientado a lo digital comenzando desde 2016 y tiene como objetivo la transformación digital, por tanto, tiene mucho que ver con el Plan De Recuperación Ante Desastres De Tecnología. Este plan juega un papel fundamental a este plan estratégico ya que las documentaciones procesos todo pasara o la mayoría a ser digital y por ende se necesita estrategia de recuperación planes etc., para mantener la operatividad de la entidad.

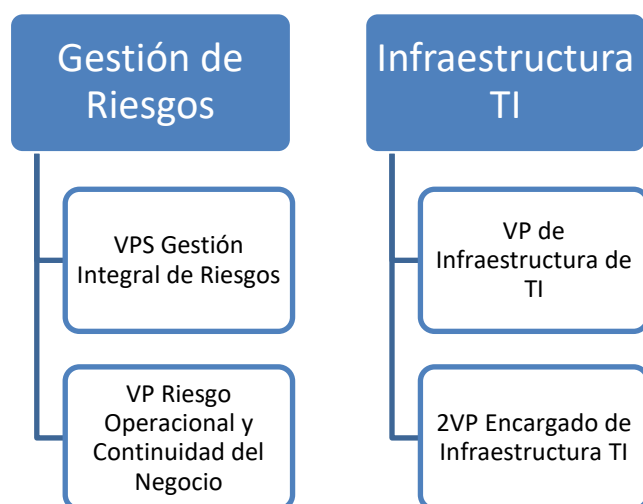
Dentro del plan estratégicos existen aplicaciones nuevas o aplicaciones que se actualizarían debido al gran volumen de información recibidas para las nuevas se deben evaluar la criticidad de las mismas y así analizar si las mismas se incorporan en la estrategia de recuperación. Para la evaluación se debe validar que impacto puede ocasionar estas aplicaciones en caos que no esté disponible ya se impactó financiero legal cliente o reputación.

En la fecha actual existen ya diferentes nuevas aplicaciones que las mismas van a sustituir algunas aplicaciones críticas estas se deben actualizar en el Plan De Recuperación Ante Desastres De Tecnología, así como también en los planes de continuidad del negocio y BIA y cualquier otra documentación que tenga que ver con esta aplicación.

Las estructuras de una organización son muy parecidas en las diferentes entidades financieras partiendo de consejo de administradores presidente, gerente general, VP, 2 VP entre otros como el objetivo principal de esta investigación es el Plan De Recuperación Ante Desastres De Tecnología y por no divulgar la

información debajo podrán ver la estructura organización de dos áreas la de Riesgos y TI que son las áreas responsables de este documento. Ver Gráfico 2.

**Gráfico 2:** Estructura organizacional la Área de Riesgo y Área de TI



**Fuente:** Elaboración Propia

### **2.3 Diagnóstico de las Empresas de Cara a un Plan de Recuperación Ante Desastres de Tecnología.**

El Plan De Recuperación Ante Desastres De Tecnología es un documento que no es manejado o no es de conocimiento por toda la organización ya que documento muy técnico sin embargo los líderes de áreas deberían de tener conocimiento del mismo.

La investigación se realizó con una muestra de 40 personas, distribuidos de la siguiente manera 10 del área de TI BHD (3 gerentes, 5 sub gerentes, 2 analistas), 10 de área de TI Banco Caribe (3 Encargado y 7 analistas, 10 departamento de seguridad de información de BHD (sub gerente y analistas, 3 de Banco popular (un gerente y 2 líderes de proyectos), 7 de seguridad Banco Caribe.



Este cuestionario tiene como objetivo el desarrollo del trabajo de investigación para la tesis de Luis Montas, para optar por el título de Master en Gerencia y Productividad

Muchas gracias por el apoyo.

Nombre y apellido: \_\_\_\_\_

Nombre de la empresa: \_\_\_\_\_

Área que labora: \_\_\_\_\_

Leyenda:

S: SI    N: NO    DT: DESCONOCE DEL TEMA

Cuestionario para propuesta de modelo de revisión de Plan De Recuperación Ante Desastres De Tecnología.

| Nr<br>o. | Pregunta                                                                                                                            | S | N | DT |
|----------|-------------------------------------------------------------------------------------------------------------------------------------|---|---|----|
| 1        | ¿La empresa cuenta con un Plan De Recuperación Ante Desastres De Tecnología?                                                        |   |   |    |
| 2        | ¿Tiene acceso a poder ver el documento?                                                                                             |   |   |    |
| 3        | ¿Sabe usted quienes son los responsables de documentar/actualizar estos documentos?                                                 |   |   |    |
| 4        | ¿Tiene usted conocimiento de las pruebas de contingencia que se realizan en su organización?                                        |   |   |    |
| 5        | ¿Considera usted importante que su organización tenga un Plan De Recuperación Ante Desastres De Tecnología?                         |   |   |    |
| 6        | ¿Entiende usted que el Plan De Recuperación Ante Desastres De Tecnología abarca todas las aplicaciones críticas de su organización? |   |   |    |

|    |                                                                                                                                                                                |  |  |  |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| 7  | ¿Considera que se debe agregar algún punto o algún anexo al Plan De Recuperación Ante Desastres De Tecnología?                                                                 |  |  |  |
| 8  | ¿Tiene conocimiento si cuando se realizan las pruebas de contingencia las mismas tienen los procesos bien documentado en el Plan De Recuperación Ante Desastres De Tecnología? |  |  |  |
| 9  | ¿Sabes cuál es el flujo de aprobación para el plan?                                                                                                                            |  |  |  |
| 10 | ¿Entiende que el plan de recuperación ante desastres de tecnología está alineado con la estrategia de la organización?                                                         |  |  |  |

Los resultados a nivel general fueron buenos ya que existe un nivel de madurez alto en las organizaciones evaluadas de todas maneras existe algunas oportunidades de mejoras. Debajo los resultados de la encuestas, como se muestra tabla 1 y gráfico 3

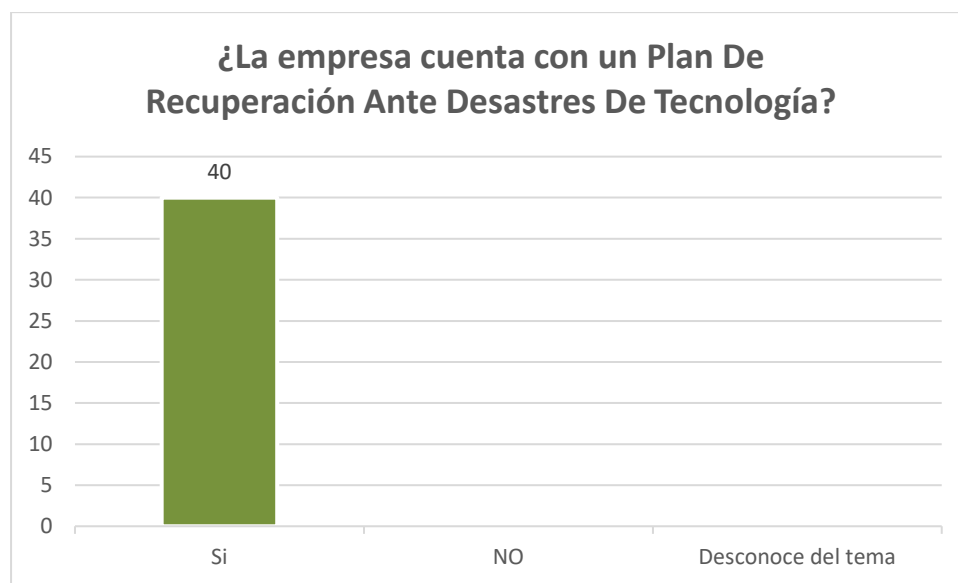
### 1. ¿La empresa cuenta con un Plan De Recuperación Ante Desastres De Tecnología?

**Tabla 1:** Resultado de entrevista de la pregunta 1.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 40         | 100%        |
| NO                 | 0          | 0%          |
| Desconoce del tema | 0          | 0%          |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 3:** La empresa cuenta con un Plan De Recuperación Ante Desastres De Tecnología.



En cuanto a esta pregunta todos respondieron SI ya que el Plan De Recuperación Ante Desastres De Tecnología ya es una obligación tenerlo en las entidades financiera por orden de la superintendencia de bancos y auditorías internas. Ver en tabla 1 gráfico 3 los resultados de la pregunta 1.

## 2. ¿Tiene acceso a poder ver el documento?

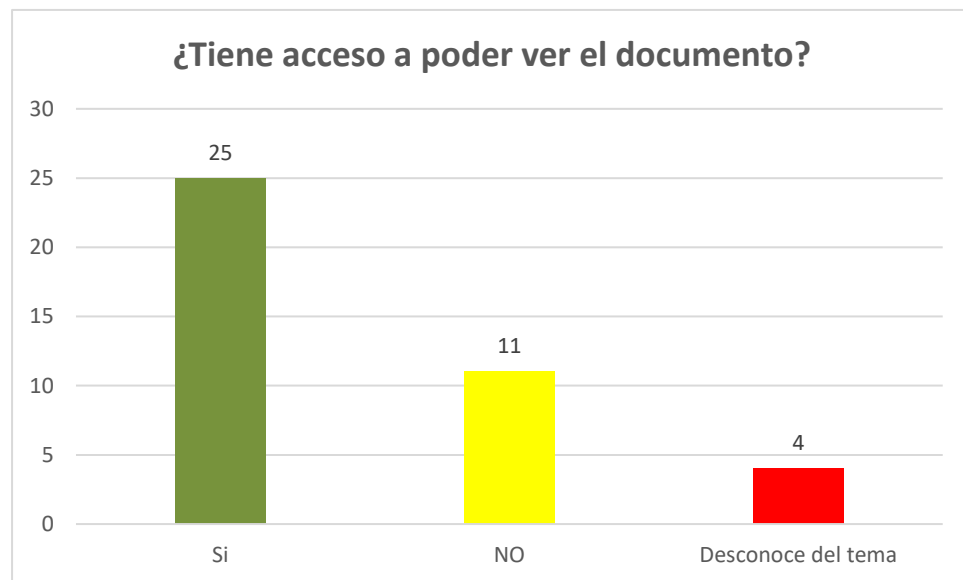
**Tabla 2:** Resultado de entrevista de la pregunta 2.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 25         | 63%         |
| NO                 | 11         | 28%         |
| Desconoce del tema | 4          | 10%         |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia



**Gráfico 4:** Tiene acceso a poder ver el documento



En la segunda pregunta 25 personas respondieron que SI, 11 respondieron que NO, y 4 desconocen del tema, este último tiene que ver con que no saben la ubicación de donde poder ver el documento esta puede ser que no esté publicado puede ser por permiso para verlo entre otras cosas. Ver en la tabla 2 y gráfico 4 se muestran los resultados de la pregunta número de la entrevista.

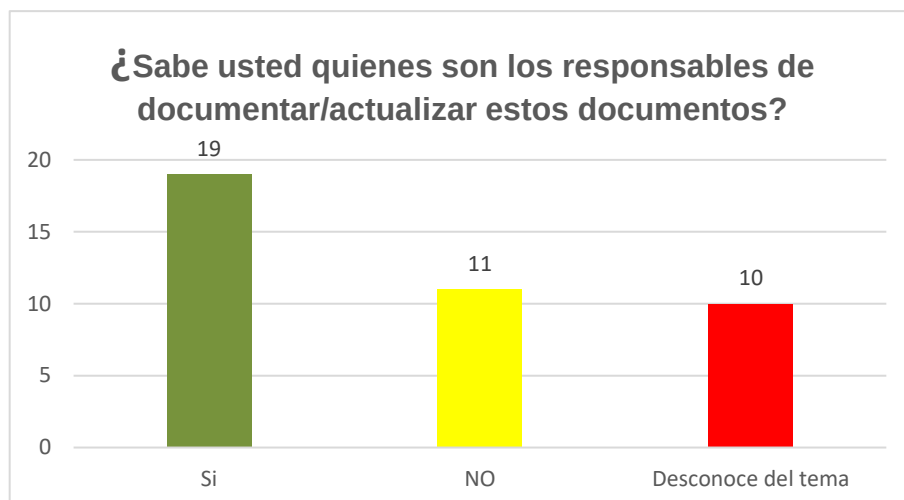
**3. ¿Sabe usted quienes son los responsables de documentar/actualizar estos documentos?**

**Tabla 3:** Resultado de entrevista de la pregunta 3.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 19         | 48%         |
| NO                 | 11         | 28%         |
| Desconoce del tema | 10         | 25%         |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 5:** Sabe usted quienes son los responsables de documentar/actualizar estos documentos



En la pregunta 3 19 contestaron que SI, 11 respondieron que No y 10 desconocen del tema, en este último sería desconocen de las personas que están responsable de la documentación del Plan De Recuperación Ante Desastre De Tecnología. Ver en la tabla 3 y gráfico 5 se muestran los resultados de la pregunta 3.

**4. ¿Tiene usted conocimiento de las pruebas de contingencia que se realizan en su organización?**

**Tabla 4:** Resultado de entrevista de la pregunta 4.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 32         | 80%         |
| NO                 | 8          | 20%         |
| Desconoce del tema | 0          | 0%          |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 6:** Tiene usted conocimiento de las pruebas de contingencia que se realizan en su organización



En la pregunta 4, 32 personas respondieron que SI, 8 personas respondieron que No, esto por razón que cuando se realizan pruebas se envía comunicación a toda la organización sobre las mismas. Ver en la tabla 4 y gráfico 6 se muestran los resultados de la pregunta 4.

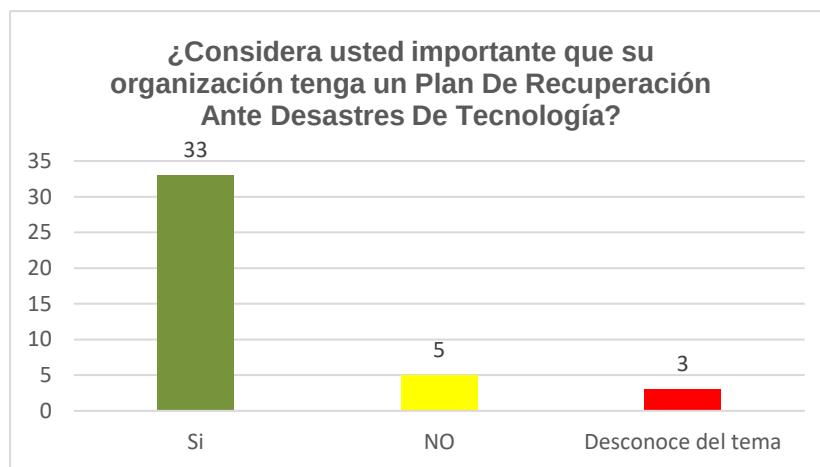
**5. ¿Considera usted importante que su organización tenga un Plan De Recuperación Ante Desastres De Tecnología?**

**Tabla 5:** Resultado de entrevista de la pregunta 5.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 33         | 83%         |
| NO                 | 5          | 13%         |
| Desconoce del tema | 3          | 8%          |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 7:** Considera usted importante que su organización tenga un Plan De Recuperación Ante Desastres De Tecnología



En la pregunta 5, 33 personas respondieron que Si, 5 personas respondieron que No y 3 personas desconocen del tema, esto último puede ser que no saben el beneficio de este plan. Ver en la Tabla 5 y gráfico 7 se muestran los resultados de la pregunta 5.

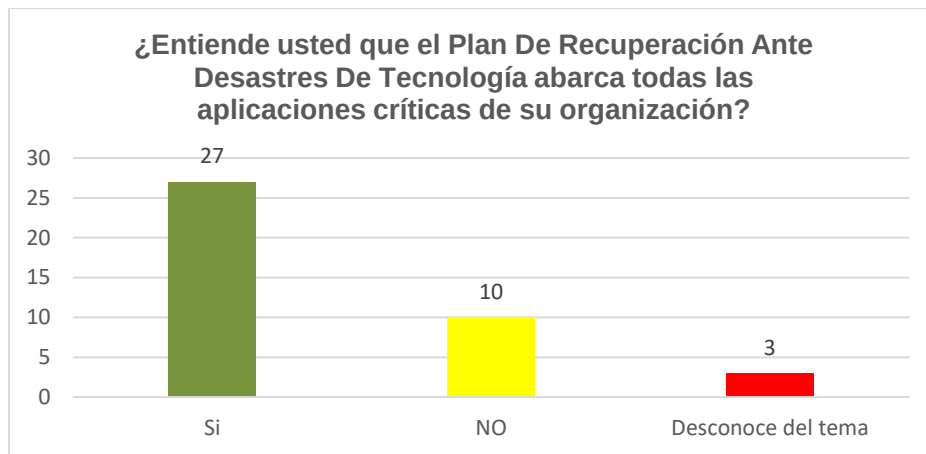
**6. ¿Entiende usted que el Plan De Recuperación Ante Desastres De Tecnología abarca todas las aplicaciones críticas de su organización?**

**Tabla 6:** Resultado de entrevista de la pregunta 6.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 27         | 68%         |
| NO                 | 10         | 25%         |
| Desconoce del tema | 3          | 8%          |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 8:** Entiende usted que el Plan De Recuperación Ante Desastres De Tecnología abarca todas las aplicaciones críticas de su organización



En la pregunta número 6, 27 personas respondieron que Si, 10 personas respondieron que No y 3 personas desconocen del tema, básicamente este tema es muy manejado por las personas que manejan y están presente en las pruebas de contingencia e interactúan con el BIA y así conocer bien cuáles son las aplicaciones críticas del negocio. Ver en la tabla 6 y gráfico 8 se muestran los resultados de la pregunta 6.

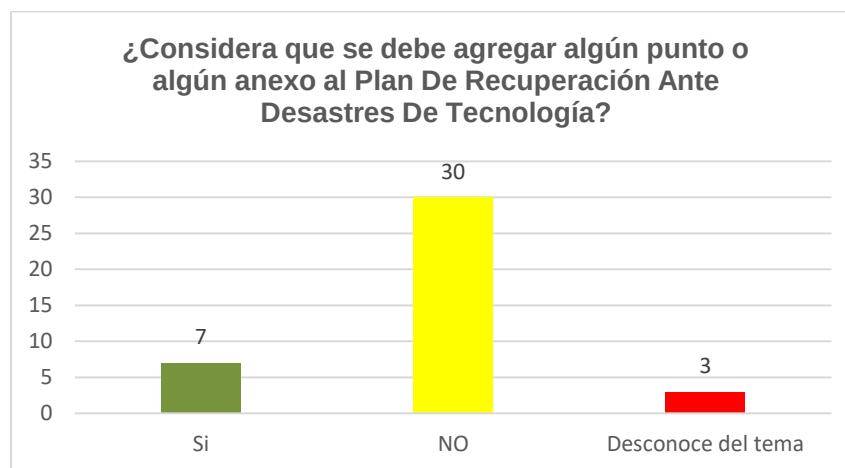
**7. ¿Considera que se debe agregar algún punto o algún anexo al Plan De Recuperación Ante Desastres De Tecnología?**

**Tabla 7:** Resultado de entrevista de la pregunta 7.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 7          | 18%         |
| NO                 | 30         | 75%         |
| Desconoce del tema | 3          | 8%          |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 9:** Considera que se debe agregar algún punto o algún anexo al Plan De Recuperación Ante Desastres De Tecnología



En la pregunta 7, 7 personas respondieron que Si, 30 personas respondieron que No, 3 personas desconocen del tema, este punto es parte de las personas responsables de las de la documentación del Plan De Recuperación Ante Desastres De Tecnología. Ver en la tabla 7 y gráfico 9 los resultados de la pregunta 9.

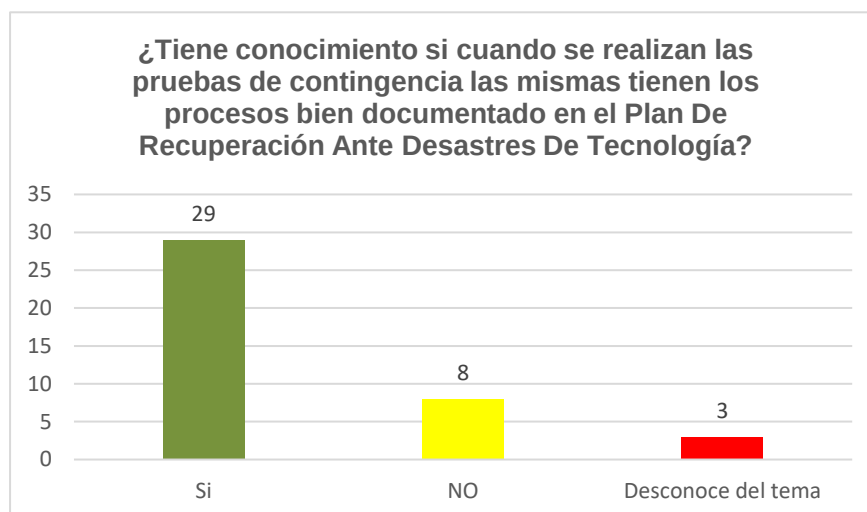
**8. ¿Tiene conocimiento si cuando se realizan las pruebas de contingencia las mismas tienen los procesos bien documentado en el Plan De Recuperación Ante Desastres De Tecnología?**

**Tabla 8:** Resultado de entrevista de la pregunta 8.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 29         | 73%         |
| NO                 | 8          | 20%         |
| Desconoce del tema | 3          | 8%          |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 10:** Tiene conocimiento si cuando se realizan las pruebas de contingencia las mismas tienen los procesos bien documentado en el Plan De Recuperación Ante Desastres De Tecnología



En esta pregunta 8, 29 personas respondieron que Si, 8 personas respondieron que No, 3 persas respondieron o desconocen el tema, para este punto como mencionamos arriba interactúan más las personas de TI y riesgo que son los responsables de documentar el Plan De Recuperación Ante Desastres De Tecnología. Ver en tabla 8 y grafica 10 resultados de pregunta 8.

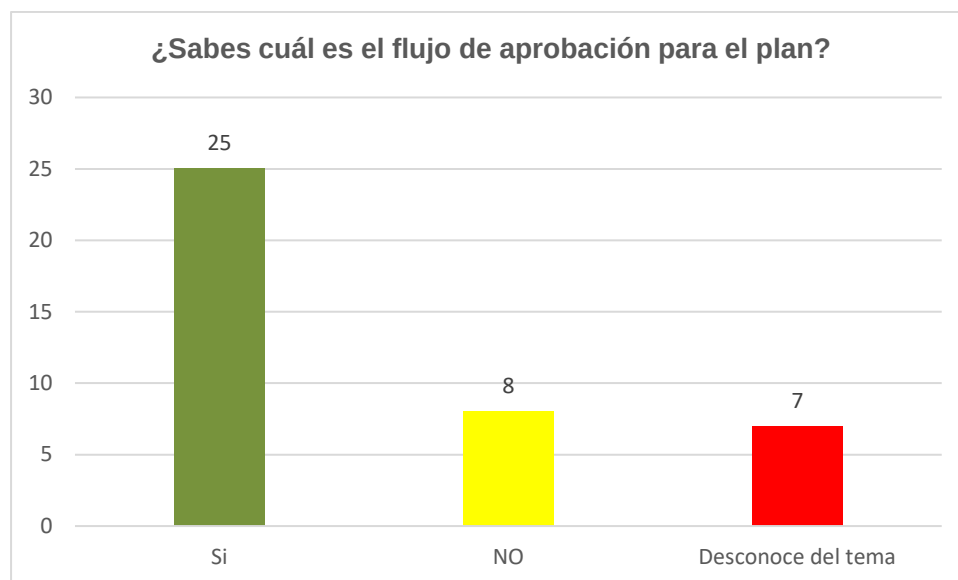
#### 9. ¿Sabes cuál es el flujo de aprobación para el plan?

**Tabla 9:** Resultado de entrevista de la pregunta 9.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 25         | 63%         |
| NO                 | 8          | 20%         |
| Desconoce del tema | 7          | 18%         |
| Total              | 40         | 100%        |

**Fuente:** Elaboración Propia.

**Gráfico 11:** Sabes cuál es el flujo de aprobación para el plan



En la pregunta número 9, 25 personas respondieron que Si, 8 personas respondieron que No, 7 personas desconocen del tema, este tema es manejado por los responsables del documento. Ver en tabla 9 y gráfica 11 los resultados de la pregunta 9.

**10. ¿Entiende que el Plan De Recuperación Ante Desastres De Tecnología está alineado con la estrategia de la organización?**

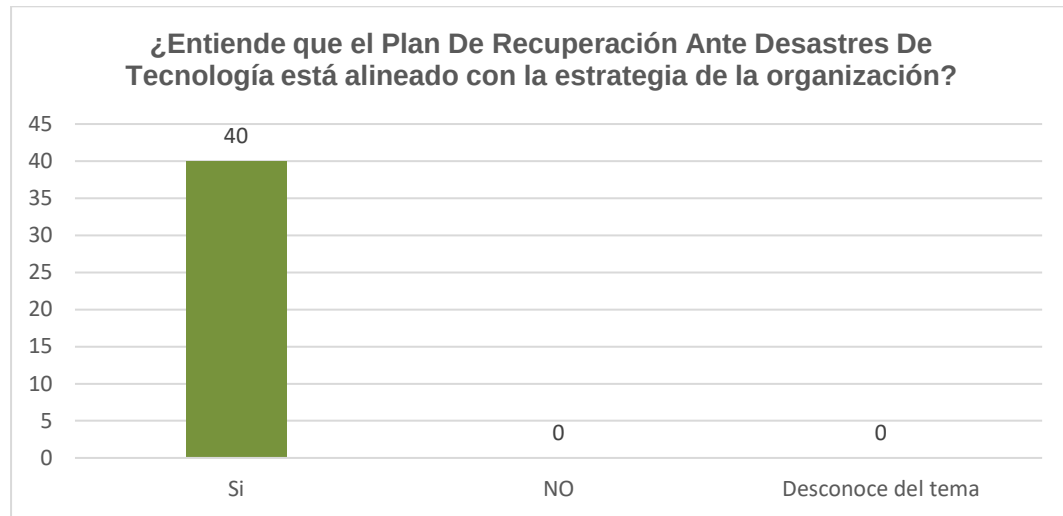
**Tabla 10:** Resultado de entrevista de la pregunta 10.

| Leyendas           | Respuestas | Porcentajes |
|--------------------|------------|-------------|
| Si                 | 40         | 100%        |
| NO                 | 0          | 0%          |
| Desconoce del tema | 0          | 0%          |
| Total              | 40         | 100%        |



**Fuente:** Elaboración Propia.

**Gráfico 12:** Entiende que el Plan De Recuperación Ante Desastres De Tecnología está alineado con la estrategia de la organización.



En la pregunta número 10, 40 personas respondieron que Si para una totalidad de un 100%, estando de acuerdo que el plan de recuperación ante desastres de tecnología está alineado a la estrategia de la organización. Ver en tabla 10 y gráfico 12 los resultados de la pregunta 10.

## **2.4 Nivel de Madurez de cara a Plan de Recuperación ante Desastres de TI**

El nivel de madurez tiene que ver con una visión general de todos los pormenores de un proceso o tema en cuestión, colocando el Plan De Recuperación Ante Desastres De Tecnología como parte principal de esta investigación seria el conocimiento en una escala de 1 al 5 que debe tener los colaboradores en cuanto al plan.

Para realizar una evaluación de nivel de madurez se realiza analizando las diferentes áreas que interactúa con el documento para saber el conocimiento y dominio que tiene del mismo. Adicionalmente se contrata un ente externo para que colabore con la evaluación así la entidad o lo colaboradores que interactúa con el documento no son juez y parte.

No todas las áreas interactúan con este documento, el Plan De Recuperación Ante Desastres De Tecnología básicamente lo maneja Riesgos en conjunto con TI y áreas de apoyo cumplimiento Auditoría Seguridad de Información son departamento para revisión del documento. La razón es que en este documento se manejan términos muy técnicos que son de dominio de TI o áreas afines.

El nivel de madurez también es apoyado por el área de auditoría y cumplimiento ya que con estos departamentos realizan revisiones y recomiendan mejoras al plan de recuperación ante de sastres de tecnología al mismo tiempo con las auditorias o informes sirven de evidencias de las pruebas y el buen funcionamiento de las pruebas que se le realizan al plan.

También agregar que aparte del nivel de madurez que lo realiza ente externo también las entidades reguladoras dígase Superintendencia de Bancos exige el documento esa revisión ayuda el nivel de la gestión de continuidad del negocio así que el Plan De Recuperación Ante De Desastres De Tecnología tenga su respectiva revisión por estas entidades es importante para mantener actualizado el plan.

## **2.5 Proceso de documentación y aprobación en la organización**

El proceso de documentación y aprobación en la organización del Plan de Recuperación Ante Desastres de Tecnología como toda documentación importante en el banco tiene su proceso y su política el mismo también tiene su flujo de aprobación.

Iniciando de realizar el Análisis de Impacto al Negocio BIA, documentar todos los procesos luego documentar todos planes de negocios y así tener toda la información necesaria para luego realizar el Plan De Recuperación Ante Desastres De Tecnología.

Como mencionamos anteriormente el Análisis de Impacto al Negocio BIA, es la columna vertebral o talón de Aquiles para una buena gestión de continuidad del negocio, así como también para realizar un óptimo plan de recuperación ante desastres de tecnología, porque del resultado del BIA obtenemos todos los

procesos importantes o críticos de la entidad, así como también recursos y aplicaciones, entre otros.

La documentación del BIA se hace mediante reuniones con los diferentes líderes priorizando los productos y servicios y evaluando cuáles presentan más impacto a la entidad, cuando se listan los productos y servicios se relaciona a cada proceso y evalúan con ayuda del líder del área el impacto financiero, reputación, legal y de clientes.

El Plan De Recuperación Ante Desastres De Tecnología se alimenta de la información documentada en el BIA con cada uno de los procesos cuáles serían las aplicaciones más críticas y así identificarla y de acuerdo a su estrategia de recuperación, nivel de respaldo establecer los tiempos RTO, RPO, MTPD y así recuperarlas en menor tiempo posible y evitando así pérdidas financieras.

Estos tiempos de recuperación ya sea de datos, de aplicación o tiempo de tolerancia se hace en conjunto con el área de riesgo la evaluación general y por el conocimiento y la experiencia del área de tecnología quien son los responsables de realizar el Plan De Recuperación Ante Desastres De Tecnología.

Tener en cuenta que estos tiempos dependen en la organización y la recuperación de la aplicación que se está trabajando, ya que no todas las aplicaciones tienen recuperación igual que otras y en el mismo volumen algunas tienen dos y otras tres estrategias de recuperación ya sea por costo o por la aplicación como tal.

### **2.5.1 Documentación**

La documentación no es más que la recolección de información centralizada de un documento principal que certifica algo, básicamente eso es lo que se realiza en el Plan De Recuperación Ante Desastres De Tecnología, recolectar la información a través del BIA (Análisis de Impacto al Negocio), los líderes de áreas con sus respectivos planes de negocio los cuales nos indican que sistemas o aplicaciones son críticos para su área entre otros.

La tarea de documentación en una organización del Plan De Recuperación Ante Desastres De Tecnología es un trabajo en conjunto por las áreas de Tecnología el área de Riesgos y también área de Seguridad de Información los cuales trabajan para la documentación de la información.

Cuando se realice la documentación de toda la información se debe presentar a los respectivos líderes de las áreas estos a su vez dan el visto bueno a la información documentada y luego se debe presentar al comité ejecutivo para la aprobación del mismo.

Tal y como mencionamos la documentación del Plan De Recuperación Ante Desastres De Tecnología es responsabilidad del área de tecnología y riesgo que lo custodia, por su parte riesgo es responsable de la actualización mejoras y en conjunto con tecnología programas periódicamente en el año pruebas de contingencia, de estas pruebas surgen lecciones aprendidas temas de actualización del plan, cambios de roles, cambios de aplicaciones en caso que aplique o de proceso para recuperar aplicación, contacto de suplidores, contacto de colaboradores primarios, alterno, entre otros.

Es importante tener claro que la importancia de las pruebas de contingencia van amarrado a las revisiones de Auditorias, revisiones de la Superintendencia de Bancos por tanto esta documentación del Plan De Recuperación Ante Desastre De Tecnología debe permanecer actualizado ósea el Departamento de Riesgo en conjunto con el área de Tecnología colocar en su plan de trabajo la fecha para la actualización así como también los responsable por ambas áreas que vayan a documentar/actualizar el Plan De Recuperación Ante Desastres De Tecnología.

### **2.5.2 Evaluación**

La evaluación del Plan De Recuperación Ante Desastres De Tecnología en una organización tiene proceso diferente dependiendo del flujo de evaluación y aprobación del mismo per a la vez e muy parecido ya que las entidades financieras tienen sus puntos parecidos, aunque algunas cambien de nombre.

Luego que el Plan De Recuperación Ante Desastres De Tecnología está listo, se debe planificar pruebas de contingencia periódicamente en el año para evaluar si todo lo que está documentado es funcional. Sin embargo, no solamente están las pruebas de contingencia para la evaluación del Plan De Recuperación Ante Desastres De Tecnología en adición a esta existe pruebas de escritorio y pruebas de alta disponibilidad que también sirven para evaluar el plan.

La prueba de escritorio también conocida como Table Top que se realiza al Plan De Recuperación Ante Desastres De Tecnología como también a los diferentes planes que están en las organizaciones, es simular un escenario que obligue activar el Plan De Recuperación Ante Desastres De Tecnología e ir paso por paso leyendo el plan y validar que todo lo escrito este correcto.

Las pruebas de alta disponibilidad es también otra opción para la evaluación del Plan De Recuperación Ante Desastres De Tecnología este consiste en seleccionar uno de los equipos o aplicaciones documentadas en el plan y probar la alta disponibilidad del mismo, normalmente los equipos tienen redundancia (un equipo al lado de otro en el centro de cómputo) se realiza un apagado forzado de un equipo y el otro debe asumir la carga y alta disponibilidad apagar todo el equipo y recuperarlo en site alterno.

Dependiendo de la organización que se encuentra las mismas tendrán sus respectivas estrategias de recuperación sin embargo las buenas practicas dicen que se debe tener al menos una estrategia de recuperación de todos los sistemas como plan de contingencia o plan B en caso que ocurra un incidente mayor y afecte el centro de cómputo principal.

En el Plan De Recuperación Ante Desastres De Tecnología se establece todas las estrategias de recuperación ante desastres, con sus respectivos procesos para activar en todos los niveles, así como también retorno al sitio principal.

Estas pruebas se pueden realizar para ambas partes para la parte de redundancia ósea hacer la prueba en el mismo centro de cómputo físicamente y también vía comando en la PC apagando los equipos por los servidores.

Todas estas pruebas la finalidad es la evaluación del Plan De Recuperación Ante Desastres De Tecnología en general sin embargo se puede validar la funcionalidad de los sistemas, la estrategia de recuperación de las aplicaciones y proceso críticos, de las pruebas surgen las lecciones aprendidas, las actualizaciones, inclusión de procesos, aplicaciones, anexos entre otros.

Normalmente cuando se necesite incorporar punto nuevo ya sea anexo aplicaciones o algo nuevo en el Plan De Recuperación Ante Desastres De Tecnología, debe pasar por un flujo de aprobación el mismo está comprendido por el área de Riesgo y el área de Tecnologías estas llegan a un acuerdo para la inclusión de un punto a agregar luego se debe presentar en comité para la aprobación del mismo.

El proceso de evaluación está presente también cuando se adquiere un software nuevo que dependiendo de la criticidad del mismo se debe agregar el Plan De Recuperación Antes Desastres De Tecnología.

Del mismo modo si se sustituye una aplicación que ya está evaluada como crítica y está en el Plan De Recuperación Ante Desastres De Tecnología se debe actualizar el mismo al momento que la aplicación este en producción.

La finalidad de estas inclusiones y evaluaciones es tener siempre actualizado el plan para el momento que sea necesario utilizarlo, así como también los contactos de personal y proveedores la evaluación es importante para así saber a quién llamar en caso que ocurra un incidente.

En el caso de los proveedores deben no deben estar todos lo proveedores ya sea que le brinden servicio a la organización virtual o físico en el Plan De Recuperación Ante Desastres De Tecnología debería estar los proveedores más críticos que interactúan con las aplicaciones crítica documentadas en el plan por ejemplo proveedores de internet.

Tomar en cuenta que no necesariamente todas las aplicaciones que están documentadas estaría sus respectivos proveedores, se debe analizar más bien cuales son lo más importantes tomando como punto de partida del Core principal

(sistema principal) de la organización, soporte y manteniendo del mismo para todas las estrategias de recuperación que están documentadas en el Plan De Recuperación Ante Desastre De Tecnología.

Existe niveles de compromiso o acuerdos con los proveedores que mencionamos anteriormente SLA (acuerdos de nivel de Servicios) que son los acuerdos establecido con dichos proveedores para recuperación de sus sistemas estos también se pueden incluir en el plan de recuperación ante desastres de tecnología como parte de sus anexos, esto dependerá de las organizaciones si los incluyen o no.

En resumen, las evaluaciones que se le realizan al Plan De Recuperación Ante Desastres De Tecnología son de suma importancia y con la finalidad de mejora continua y actualización del mismo por tanto en el año se debe realizar al menos 2-3 pruebas al plan.

Esto va a depender del nivel de madurez de la organización y que tanto les realizan pruebas a sus planes de contingencia teniendo en cuenta que se puede realizar una prueba de escritorio y prueba de alta disponibilidad que también pueden ayudar al Plan De Recuperación Ante Desastres De Tecnología.

### **2.5.3 Mejora Continua**

La mejora continua está orientada en los procesos como a ser mejor a través del tiempo, a reducir los costos de pérdidas, que oportunidades de mejora se pueden agregar o modificar para la optimización.

Para el Plan De Recuperación Ante Desastres De Tecnología, así como también los otros planes que tienen que ver con el negocio y al mismo tiempo pueden generar pérdidas financieras a la organización se debe están en contaste mejora continua el monitoreo, desempeño de los planes cuando ocurre un incidente, definir metodologías, mejorar lo proceso, lecciones aprendidas, entre otros.

En cuanto las lecciones aprendidas son elementos que se le debe dar seguimiento, cuando se realizan pruebas, cuando ocurren incidentes de cualquier

magnitud que afecte o se deba activar el Plan De Recuperación Ante Desastres De Tecnología estas deben ser documentadas y evitar que ocurra los mismos en otra ocasión.

La mejora continua no solamente está en los procesos de TI sino en toda la organización, si en caso que una aplicación se le encuentra una oportunidad de mejora y esta es necesario actualizar el Plan De Recuperación Ante Desastres De Tecnología se debe realizar la actualización ya que es imprescindible tener esa evaluación y actualización al día ya que el momento que se presente un incidente es impredecible.

Siempre que al Plan De Recuperación Ante Desastres De Tecnología se actualice o se le aplica alguna mejora el mismo debe estar documentado en un control de cambio que permite al lector del plan saber qué cambio ha tenido y cómo ha evolucionado a través del tiempo.

El control de cambio no es más que la tabla o matriz con todos los cambios que se le han realizado al Plan De Recuperación Ante Desastres De Tecnología, de acuerdo a las buenas prácticas y haciendo referencia en la Norma ISO 22301, se debe realizar una revisión anual del plan por tanto cualquier mínimo cambio debe quedar registrados en el control de cambios.

Este control de cambios también es utilizado en los demás planes en la metodología y otros, es como un control de todas las tareas realizadas en el mismo, tener en cuenta que cualquier tema es importante indicarlo aquí, con la finalidad de luego presentarlo y publicarlo para conocimiento de las áreas que interactúan con este documento tengan la versión actualizada.

Esta tarea se debe hacer con mucha responsabilidad y compromiso por que cualquier error puede afectar la utilización o activación del Plan De Recuperación Ante Desastres De Tecnología y al mismo tiempo ocasionar pérdidas financieras o algún impacto legal, de clientes o de reputación.

Por esta razón todos y cada uno de los cambios debe estar en flujo de aprobación correspondiente, se documenta se aprueba y se presenta al comité y



luego divulgación del mismo, así se evitan muchos errores nadie alega ignorancia y todas las personas que interactúan con el Plan De Recuperación Ante Desastres De Tecnología estarían al tanto de los cambios.

En resumen, la mejora continua es necesaria para el Plan De Recuperación Ante Desastres De Tecnología, así como también para los demás planes, implementando mejora actualizaciones la finalidad es optimizar el plan lo más que se pueda para la ejecución de los procesos.

Esta mejora continua se puede realizar a través de las pruebas que antes mencionamos como la prueba de contingencia general donde toman las aplicaciones críticas no todas al mismo tiempo sino programados para no afectar la continuidad del servicio y también están las pruebas de alta disponibilidad y de escritorios.

Esta última se puede programar durante el año ya que la misma no afecta la operatividad solo coordinas con las áreas pertinentes y elaborar escenarios para dicha prueba, adicionalmente documentarlos todo y darles seguimiento a las lecciones aprendidas.

Normalmente las pruebas realizadas a estas aplicaciones son 2-3 aplicaciones para no afectar todo el banco sin embargo cuando se prueba el Core bancario o sistema principal en algunas pruebas se coloca solo una aplicación crítica más o dos ya que la finalidad es la no afectación a la organización.

Sin embargo, estas pruebas son de suma importancia se debe realizar las pruebas a las aplicaciones ya a sus respectivas estrategias de recuperación sin embargo en caso que la organización tenga más de dos estrategias de recuperación en una prueba se debe solamente probar una ya que a la misma se le asigna a y tiempo de ida y retorno y también para no afectar la organización.

Por esta razón se realizan las programaciones en las mismas se indican que se probará o sea cual o cuales aplicaciones y cual estrategia se probará por ejemplo en tal mes dos o tres aplicaciones críticas que estén documentadas en el Plan De

Recuperación Ante Desastres De Tecnología y en qué estrategia de recuperación se realizar.

Del mismo modo se seleccionan do o tres más y se establece que se hará en otra estrategia de recuperación para así probar todo el procedimiento desde la ida hasta el retorno de la misma.

Se debe tener en cuenta que en caso que alguna de las aplicaciones falle durante de la prueba se debe documentar las lecciones aprendidas y la misma (aplicación) se debe nuevamente programar para realizarle la prueba en el mismo año.

## **CAPÍTULO III**

### **CAPÍTULO III: PROPUESTA DE IMPLEMENTACIÓN DE MODELO DE REVISIÓN DE PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA EN UN BANCO MÚLTIPLE**

Luego de analizar todas las respuestas de la entrevista realizada sobre el Plan De Recuperación Ante Desastres De Tecnología recolectamos esa información podemos ver que el conocimiento del tema está en un nivel de madurez bueno.

Por tanto, tomando como parámetros todos los planteamientos anteriores es importante que las organizaciones las mayorías tengan conocimiento, realicen sus pruebas y tengan las habilidades para recuperar sus operaciones en la organización ante cualquier incidente.

La propuesta de implementación de un modelo de revisión de Plan De Recuperación Ante Desastres De Tecnología buscamos con esta evitar los errores y en base al a la experiencia y conocimiento proponemos brindar mejora en la documentación y aprobación del plan y la misma se podría implementar en cualquiera organización.

Cabe señalar que el Plan De Recuperación Ante Desastres De Tecnología es un documento que en algunas instituciones está en un nivel de madurez muy alto, sin embargo, la propuesta que tendíamos seria para optimizar la documentación y tener un modelo para la revisión del plan seria:

Elementos a tomar en cuenta para una correcta documentación del Plan De Recuperación Ante Desastres De Tecnología

1. Proporcionar información necesaria de los colaboradores incluyendo contacto de colaboradores que ya no están en las instituciones y otros que cambiaron de áreas.
2. Concientizar a los colaboradores del departamento de TI de la importancia de la organización y buena documentación de los procesos crítico de la organización.

3. Orientar a los colaboradores que interactúan con este documento, sobre las actualizaciones y ubicación del documento tenga fácil acceso.
4. Contribuir con el departamento responsable de documentar las informaciones para el Plan De Recuperación Ante Desastres De Tecnología.
5. Divulgar el plan a través de las vías disponibles para crear cultura del plan.
6. Contribuir a que los colaboradores entiendan la importancia del plan.

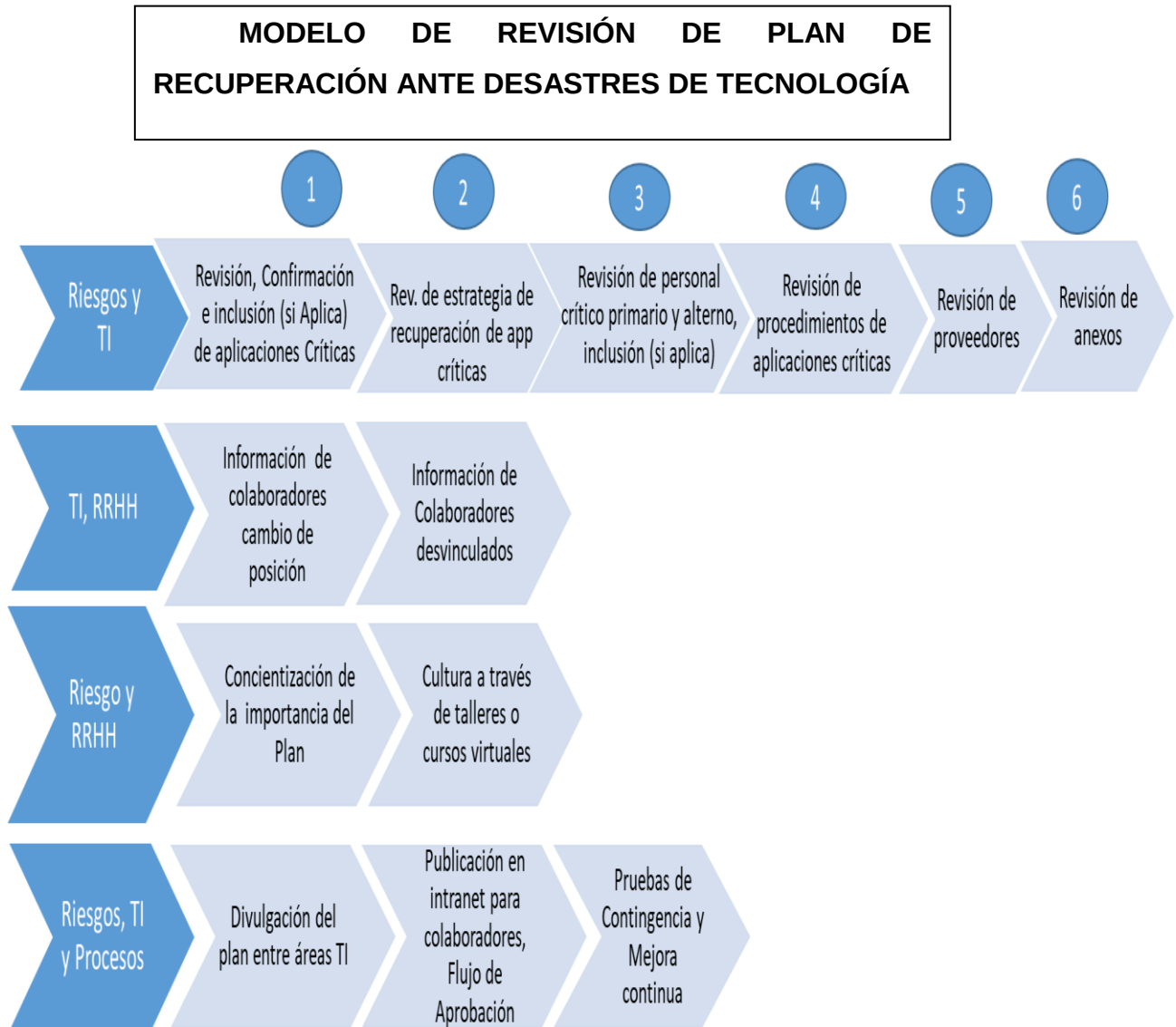
Estas serían los elementos que proponemos tener en cuenta para una correcta documentación del Plan De Recuperación Ante Desastres De Tecnología, estas se podrían implementar en cualquier organización ya que las mismas están alineadas a las buenas practicas ósea a la norma ISO 22301.

Todos los elementos anteriormente mencionados sería un trabajo en equipo por parte del área de Riesgo y el área de TI, adicionalmente estaría el área de Seguridad de Información como área de apoyo.

Teniendo en cuenta que todo debe estar en el correcto flujo de aprobación en ambas partes responsables de la documentación, aprobarlo y presentarlo a comité que sea necesario.

Cabe destacar que cada año se realiza revisiones del Plan De Recuperación Ante Desastres De Tecnología, estos elementos pueden ayudar a la optimización del mismo, si se realiza con las pautas necesarias y entendiendo la importancia de este plan se puede evitar errores a la hora de activar dicho plan en cualquier incidente que afecte los sistemas o aplicación críticas. Ver gráfico 11

**Gráfico 11: MODELO DE REVISIÓN DE PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA**



**Fuente:** Elaboración Propia.

Este sería la propuesta del modelo a implementar para las organizaciones, con la finalidad de optimizar y tener siempre bien actualizado el Plan De Recuperación Ante Desastres De Tecnología.

**Primero:** Revisión, Confirmación e inclusión (si Aplica) de aplicaciones Críticas.

Se debe realizar una revisión y confirmación de todas las aplicaciones críticas que están documentadas en el Plan De Recuperación Ante Desastres De Tecnología, esto es con la finalidad de que la que están en documento no tengan alguna variación. En caso que exista una nueva aplicación crítica esta debe pasar por el procedimiento de evaluación de riesgos, BIA, Flujo de aprobaciones entre otros, siendo así se debe incluir la aplicación y procedimientos.

Se debe realizar reuniones con el área de tecnología y Seguridad para evaluar si las aplicaciones que están en el Plan De Recuperación Ante Desastres De Tecnologías necesitan cambio o a través del tiempo (un año) sufrió modificación o actualización.

Normalmente cuando una aplicación sufre cambios ya sea de nombre de servidores, aplicación como tal en conjunto con el departamento de Riesgos se debe realizar una evaluación para analizar si la misma en caso que sea nueva aplica para ser documentada en el Plan De Recuperación Ante Desastres De Tecnología. Adicionalmente saber si la misma tiene estrategia de recuperación y se pueda utilizar en caso de un incidente.

Si la aplicación sufrió un cambio de servidor, IP u otros se debe realizar el cambio esto es vital ya que en caso que se requiera activar el plan las misma deben estar bien actualizada con nombre, IP, estrategia y demás nada de esto debe estar sin modificar a la hora de utilizarse.

Para esto es necesario el apoyo del área de tecnología y el área de Seguridad de Información, ya que esta información es muy técnica y estas áreas tiene el dominio de las mismas.

**Segundo:** Revisión de estrategia de recuperación de aplicaciones críticas.

A cada una de las aplicaciones críticas que están documentadas en el Plan De Recuperación Ante Desastres De Tecnología debe tener una estrategia de

recuperación ósea las aplicaciones deben estar incluidas en la estrategia de recuperación que tiene la organización si ocurre el caso que una aplicación no está en la estrategia se debe tomar la iniciativa de incluirla. Existen aplicaciones que no soportan más de una estrategia de recuperación y en otro caso por motivo de costos.

Si la organización pasa por un proceso de reestructuración a nivel de estrategia de recuperación se debe actualizar el Plan De Recuperación Ante Desastres De Tecnología a modo general en las partes que corresponda.

Esto va de la mano con la mejora en funcionamiento ósea la adquisición de nuevos centros alterno o creación de uno nuevo ya sea por desempeño o disminución en este caso cuando ya los centros estén en producción se debe actualizar el plan.

Mientras el proceso de adquisición de centro alterno o mejora no se puede actualizar en Plan De Recuperación Ante Desastres De Tecnología se debe esperar que todo esté listo para comenzar actualizar.

En este proceso se debe incluir en la estrategia todas las aplicaciones críticas documentadas en el plan no se puede quedar sin plan de contingencia, así como también luego que este en producción realizarle pruebas al centro y a las aplicaciones para garantizar la continuidad operativa o de servicios.

No necesariamente hacerles a todas las aplicaciones de una vez sin embargo en conjunto con el área de tecnología programas pruebas y así ir validando todas las aplicaciones funciones en el nuevo centro.

Estas pruebas deben quedar documentadas y tener el apoyo del equipo de auditoría para así tomarlo como referencia para evaluación de desempeño en las aplicaciones tiempo de ejecución tiempo de retorno.

**Tercero:** Revisión de personal crítico primario y alterno, inclusión (si aplica).



A través del tiempo los colaboradores cambian de posición o se van de la organización sin embargo en el Plan De Recuperación Ante Desastres De Tecnología existen lo que llamamos personal critico primario y alterno, estos son colaboradores líderes de diferentes áreas de tecnología de suma importancia en este plan, por tanto, este punto debe estar actualizado con el personal responsable del área y sus respectivos alternos. Del mismo modo incluir en caso de ser necesario.

Esta actividad es un trabajo en equipo del área de Riesgos Tecnología y Gestión de talento, estos últimos indican rotación de personal.

La importancia de esto es que básicamente en el documento están las personas, proveedores críticos de cada aplicación servicios y demás si estos sufren alguna rotación en la organización o son desvinculados no habrá forma en caso que ocurra un incidente y no está actualizado de contar con ese personal.

Por tanto, todo personal primario y alterno debe estar actualizado, este punto es importante ya que a la hora de una revisión el Plan De Recuperación Ante Desastres De Tecnología se enfocan directamente en las aplicaciones, proveedores estrategias, entre otros sin embargo debe estar también enfocado a las personas que son la parte fundamental para correr o ejecutar las aplicaciones y recuperar los sistemas.

La rotación de este personal no es tan grande sin embargo se debe siempre estar al tanto de los cambios, todo esto Gestión de Talento debe colaborar con las personas que están en este plan o en el área de tecnología que sea considerado como personal critico primario y alterno, se puede hacer vía notificación vía mail a las partes responsables en el área de Riesgos y Tecnología y Seguridad.

**Cuarto:** Revisión de procedimientos de aplicaciones críticas.

Cada una de las aplicaciones críticas documentadas en el plan de recuperación ante desastres de tecnología debe tener sus respectivos procedimientos tanto de activación en site principal como recuperación en la o las estrategias de recuperación, así como también el retorno.

Por tanto, en este punto del modelo de revisión se debe validar si los procedimientos estas actualizados a nivel de servicios, servidores, IP, entre otros. Este punto ayuda mucho al tema de cambio de nombre de servidores, numero de IP y otros.

En este punto también es bueno mencionar que cuando estos servidores cambian de nombre el equipo de tecnología debe notificarlo para realizar los cambios esto no ocurre normalmente por tanto se puede establecer fecha para las actualizaciones de los componentes ya sea nombre de servidores, IP contactos, entre otros.

Teniendo en cuenta que todos estos cambios deben documentarse y colocarse en el control de cambios para llevar un control de todo lo realizado en el Plan De Recuperación Ante Desastres De Tecnología.

Estos procedimientos que están documentado en el Plan De Recuperación Ante Desastres De Tecnología se deben realizar directamente con el personal que interactúa con la aplicación en cuestión ya que es quien domina el funcionamiento de la misma.

Cada procedimiento lleva cantidad de pasos diferentes y se puede recuperar en ambientes diferentes de varias formas por tanto cualquier actualización o modificación es importante la documentación.

Puede ocurrir que una aplicación cambie de nombre o de estrategia dígame que su recuperación manual y la nueva forma de recuperación sea virtual esto también debe estar documentado en el plan.

**Quinto:** Revisión de proveedores.

Tal y como mencionamos arriba cada aplicación en el plan es necesario incluir los proveedores críticos partiendo del sistema principal o core principal de la organización, normalmente se colocan los proveedores de servicios de comunicación, base de datos, UPS, entre otros.

Esta parte es responsabilidad directa de Tecnología ya que ellos son los que conocen cuales son los proveedores importantes y necesarios a la hora de recuperación de los sistemas. A cada uno de los proveedores se le debe colocar número de contactos de oficina y celular.

Del mismo modo en el que se actualizan los datos de los contactos primario y alternos en el Plan De Recuperación Ante Desastres De Tecnología se deben colocar los nombres de los proveedores con sus respectivos contactos, sin embargo, también se debe tener presente la rotación y cambio proveedor.

Para este caso también existe el personal primario y alternativo para que los proveedores estén el personal que sea primario a la hora de solución de incidentes y alternativo en caso que no esté el primario.

Para las pruebas normalmente es necesario la presencia in site de alguno de los proveedores más críticos en caso que se requiera esta tarea es responsabilidad del área de tecnología, este a su vez debe obligatoriamente estar documentado en el Plan De Recuperación Ante Desastres De Tecnología.

Proveedores que tengan niveles de escalamiento para solución de inconvenientes se podría colocar todo como anexo al plan con todos los niveles de escalamiento para llamadas al personal con tiempo estimado de solución y de llamada entre supervisores dependiendo del incidente ocurrido, esto también es responsabilidad de tecnología saber cómo y cuándo se deber contactar al personal de un proveedor y tiempo estimado de solución de un incidente claro dependiendo del proveedor adicionalmente una estrategia para cada proveedor en caso que aplique.

**Sexto:** Revisión de anexos.

Normalmente algunas aplicaciones, proveedores tiene algún tema para comunicación para recuperación de aplicación, nivel de escalamiento en caso de incidentes, esta parte se incluye al final del documento como parte de anexos así una persona que no conozca de la materia pueda comunicarse con cualquier personal o proveedores de una aplicación o servicio de comunicación.

Este punto dependerá de que quiera agregar la organización en el Plan De Recuperación Ante Desastres De Tecnología.

El proceso para el modelo de revisión es cíclico por tanto asignamos a las diferentes áreas responsabilidades puntuales de cara a la mejora continua de este proceso de documentación, tener en cuenta que esto es un trabajo en equipo por diferentes áreas por tanto se debe seleccionar personal responsable y con compromiso con la organización.

**TI y RRHH** se debe informar los cambios de posiciones y desvinculación de los colaboradores, esta información debe fluir entre estas áreas, adicionalmente al equipo de riesgos para cuando se actualice el plan se tenga pendientes esta parte, del mismo modo incluir personal en caso que sea necesario.

**Riesgos y RRHH** crea concientización y Cultura con la finalidad de que las personas sepan la importancia y conozcan que en la organización existe un Plan De Recuperación Ante Desastres De Tecnología, a través de talleres, reuniones, actividades entre otros.

**Riesgos, TI y Procesos** se debe crear un proceso para la divulgación del plan entre las áreas de TI para que conozcan formato que está incluido y que no, cuales son las aplicaciones que deben darle prioridad a la hora de brindar un servicio, etc.

Con ayuda del departamento de procesos crea un flujo de aprobación para la publicación de este documento en intranet o algún servidor interno que cada

personal que lo necesito tenga la última versión del documento y pueda manejarlo, esto sería solo como lectura.

Riesgos y TI se encargan de programar pruebas en el año de las aplicaciones críticas probando las estrategias de recuperación, procedimientos, personal crítico entre otros.

Para estas pruebas se eligen las aplicaciones que realizar la prueba día y hora de la misma con la finalidad de no afectar a la operatividad de la organización.

Como parte de la mejora continua se realiza indicadores de desempeño de la prueba para cada etapa de la misma se robustecen los indicadores adicionalmente se documentan las lecciones aprendidas como parte de aprendizajes y oportunidades de mejoras de las aplicaciones procedimientos o procesos de la prueba.

Es importante tener en cuenta que los aprendizajes, lecciones aprendidas u oportunidades de mejoras se le debe dar el debido seguimiento con la finalidad de aplicar mejora continua y que estas situaciones no vuelvan a ocurrir o también se podría minimizar el riesgo.

Riesgo que se puede convertir en un incidente, cuando se realizan prueba se debe documentar las lecciones aprendidas es de vital importancia darle el debido seguimiento para que las situaciones no se vuelvan a repetir.

Al mismo tiempo cuando ocurre un incidente que afecte la operatividad el banco y se necesite activar o no el Plan De Recuperación Ante Desastres De Tecnología es necesario documentar todos lo por menores oportunidades de mejoras tareas realizadas correctamente, así como también los aprendizajes que pueden servir para mejorar el funcionamiento en el plan como para la recuperación de los sistemas en las diferentes estrategias de recuperación.

### **3.1 Impacto de en las entidades financieras**

El Plan De Recuperación Ante Desastre De Tecnología tiene un impacto muy fuerte en las entidades financieras ya que a través del tiempo las organizaciones y el mundo gira a través de la parte digital y muchas estrategias dependen totalmente de la tecnología, por esta razón se debe tener más y más conocimiento y buen funcionamiento del Plan De Recuperación Ante Desastres De Tecnología en las organizaciones.

El impacto que pueda tener una organización en caso de no tener este documento actualizado o disponible puede ser costoso, pero más allá de lo financiero están diferentes impactos que también afectan a las organizaciones que si se podría medir son más fuerte que el financiero seria el impacto reputación, este es más complicado de cara a clientes ya que por el uso de las redes la información fluye muy rápido, cualquier información sale a luz de una vez.

Adicionalmente está el impacto legal que un cliente puede realizar una demanda dependiendo que la situación o incidente que ocurre en la organización esto ya pasa por un proceso diferente por parte del departamento legal y demás.

Y por último el impacto cliente que también está incluido en los demás impactos sin embargo se debe analizar qué impacto o a cuantos clientes impacto el incidente ocurrido.

Estos son los impactos que pueden tener las organizaciones en caso de no tener este plan actualizado, aclarar también que existen otros planes, otras estrategias que también pueden incurrir en afectar la organización a nivel de los impactos antes mencionados.

Dentro de la importancia que tiene un Plan De Recuperación Ante Desastres De Tecnología en las organizaciones se ve alineado también al buen desempeño que tiene los servidores y aplicaciones que poseen las aplicaciones.

No todas las organizaciones tienen las mismas aplicaciones las mismas, las mismas estrategias de recuperación, así como también las aplicaciones que puedan trabajar en alta disponibilidad.

Existen muchas razones ya sea por costo la empresa sea pequeña o simplemente no tenga otra estrategia de recuperación, que no debería de ser así dentro del Plan De Recuperación Ante Desastres De Tecnología en las organizaciones se debe colocar todo y en caso que no lo tenga trabajar para la mejora de estos.

Dentro del Plan De Recuperación Ante Desastres De Tecnología existe un término que es agenda o árbol de llamadas que sería la lista de contactos de los colaboradores crítico de ese plan que sería como el orden de llamadas para en caso de incidentes contactar, así como también a los proveedores. En este último caso no es necesario tener un orden sino colocar los más crítico o relevantes para las aplicaciones.

Los Back up o copia de seguridad son también elementos importantes para la documentación del Plan De Recuperación Ante Desastres De Tecnología en las organizaciones ya que con esto sabemos que tiempo se puede colocar para la recuperación de las aplicaciones críticas y así determinas correctamente el RTO y RPO de cada aplicación.

Partiendo del conocimiento de este es mucho más fácil conocer que tiempo podemos recuperar las aplicaciones sin embargo siempre es bueno colocar un tiempo de holgura por cualquier incidente que pueda ocurrir.

En resumen, este y los otros planes se deben actualizar, mejorar a través del tiempo y de las pruebas ya que el impacto ocasionado a las organizaciones puede ser de diferentes maneras y en caso positivo si todo esta correcto la organización pierde el mínimo de tiempo a nivel operativo o de recuperación y por ende perdería poco a nivel financiero y de clientes.

### **3.2 Requisitos para realizar una Plan de Recuperación ante Desastres de TI.**

Los requisitos para realizar un Plan De Recuperación Ante Desastres De Tecnología parte Análisis de Impacto al Negocio BIA, donde se establece todos los procesos del negocio y todas las aplicaciones que interactúa con el negocio.

En las diferentes organizaciones tiene su forma para documentar el plan sin embargo de acuerdo a la Norma ISO 22301 existen elemento imprescindible para la realización de documentación del Plan De Recuperación Ante Desastres De Tecnología.

Los requisitos de acuerdo a la norma ISO 22301 que debe tener son:

- Estrategias de recuperación.
- Aplicaciones críticas.
- Procedimientos de las aplicaciones críticas de acuerdo a sus respectivas estrategias de recuperación.
- Proveedores críticos.
- Estrategias de personal.
- Personal Crítico (Primario y Alterno).
- Aprobación por las diferentes partes.

Estos serían los requisitos más importantes que debe tener el plan, dentro de lo mismo debe tener la información más actualizada con la finalidad que cuando se realice pruebas de contingencia todo este correcto a nivel de procedimiento y aplicaciones.



En caso que se requiera algún otro requisito importante dependiendo de la organización se puede incluir estos mencionados anteriormente están alineados con la norma ISO 22301, ya depende de la organización cuales agregar al Plan De Recuperación Ante Desastres De Tecnología.

### **3.3 Beneficios que tienen las entidades financieras de tener un Plan de Recuperación ante Desastres de TI alineado a las buenas prácticas.**

Básicamente el Plan De Recuperación Ante Desastres De Tecnología debe estar alineado tanto a las buenas prácticas como a la estrategia del negocio eso es obligatorio, ya que en este plan no se documenta elementos que no sean crítico para la organización.

Los beneficios que tiene una organización que tenga una correcta y buena documentación del Plan De Recuperación Ante Desastres De Tecnología, fundamentalmente es la continuidad operativa del negocio, que en caso de cualquier incidente se pueda mantener la continuidad del servicio, teniendo en cuenta el tiempo y la estrategia de recuperación.

Las organizaciones que tienen este plan correcto protegen el negocio de incidentes grandes en los servicios o procesos que son digitales a través de estrategias planes de contingencia, respaldos y demás.

Se reducen los riesgos a nivel general en la organización por la falta de alguna aplicación o servicios que afecta a los clientes u operatividad del negocio.

Acceso garantizado a las aplicaciones en todo momento partiendo de las aplicaciones críticas como parámetros en la recuperación de los sistemas.

Servicios disponibles para los clientes las 24 horas, así como también a los proveedores, colaboradores entre otros.

Tener la capacidad de una recuperación con éxito para las pruebas de contingencia, así como también los incidentes reales, poder minimizar los errores para la toma de decisión en caso de ser necesario.

Todo esto también tiene un impacto en la parte financiera por tanto otro de los beneficios que tienen las entidades financieras de tener un Plan De Recuperación Ante Desastres De Tecnología es ahorro en las perdidas ya que también en caso que se afecte algún equipo se debe hacer una inversión en el o los mismos equipos que se afecten.

Que tenemos también como beneficio la administración de las aplicaciones más críticas de la organización en un documento en el cual se puede publicar en intranet (Red Interna) para el uso público de las personas que requieran esta información.

Quienes tendrían acceso serían las personas que requieran hacer una implementación en la cual la misma interactúe con alguna de las aplicaciones críticas por ejemplo alguna implementación digital y se necesite saber la estrategia de recuperación de cualquier aplicación crítica que este documentado en el Plan De Recuperación Ante Desastres De Tecnología.

Como parte de auditoría externa e interna que se realice a la organización ya que las auditorías requieren esta información como insumo para la revisión o auditorías que se realizan periódicamente a las áreas, esta documentación se le solicita al área de Riesgos estos como responsables de tener en custodia este documento.

Al mismo tiempo el área de Tecnología en caso que requieran esta información tiene el documento como una copia y no puede actualizar el mismo sin la autorización del área de Riesgo, esto con la finalidad de tener control y que Tecnología no sea juez y parte en la elaboración y documentación del Plan De Recuperación Ante Desastres De Tecnología, sino que estas dos partes en la documentación del mismo.

Por esta razón a principio de año se programan todas las veces que se actualizara el Plan De Recuperación Ante Desastres De Tecnología, el mismo debe ser revisado a totalidad en conjunto con el área de Riesgo, Tecnología y Seguridad,

y validar que todo este correcto al mismo tiempo programamos pruebas del plan para confirmar que todo lo escrito sea lo real.

Es responsabilidad de las áreas que se encargan de documentar esta información la veracidad de la misma por esto las personas deben saber el compromiso que tienen y la importancia que es la documentación del Plan De Recuperación Ante Desastres De Tecnología.

## **CONCLUSIONES**

## CONCLUSIONES

Cuando las organizaciones van tomando fuerza creciendo a nivel estructural financiero van demandando más tecnología y se debe tomar las pautas necesarias para la protección y salvaguardar la información, este que es la parte vital para una organización o entidad financiera.

En el Plan De Recuperación Ante Desastres De Tecnología se documentan las estrategias de recuperación los procedimientos aplicaciones críticas y demás todo esto con la finalidad de la continuidad operativa o continuidad en el servicio y por ende una pérdida financiera.

Al realizar esta investigación nos dimos cuenta que el nivel de las organizaciones de cara al Plan De Recuperación Ante Desastres De Tecnología está alto sin embargo se debe mejorar el conocimiento en las áreas para concientización sobre la importancia del plan.

La elaboración de la entrevista que realizamos a las diferentes organizaciones nos permitió tener indicadores de cómo está el conocimiento del plan, así como el uso del mismo a través de pruebas de contingencia, adicionalmente las pruebas realizadas periódicamente que tanto los colaboradores conocen y saben la importancia de la misma.

Los elementos que son fundamentales para la realización del plan de recuperación antes desastres teniendo en cuenta que las diferentes organizaciones tienen sus políticas para la documentación y divulgación del plan, así como también los niveles de aprobación.

Consideramos muy importante y necesario el uso del Plan De Recuperación Ante Desastres De Tecnología para mantener la continuidad operativa de la organización ante cualquier incidente natural físico o digital, esto va de la mano con la buena documentación del plan, así como también la correcta actualización del mismo.

La importancia de un Plan De Recuperación Ante Desastres De Tecnología va más allá que los sistemas ya que también se puede incluir recuperación de

personas, estrategias cruzadas entre departamentos críticos de la organización, indicar cuáles serían como el plan de contingencia para un departamento físico este también es de la importancia que tiene este plan.

Este componente de las estrategias de personal y departamental es bien importante y se pudiera incluir en el plan dependiendo si la organización o las áreas pertinentes aprueban esta iniciativa.

Los resultados que pudimos recopilar en las entrevistas pudimos observar que los diferentes planes en las organizaciones son muy parecidos porque están alineados a la norma ISO 22301, sin embargo, luego hay algunos que agregan o incluyen otro componentes o elementos que son importante para su organización y es válido también.

Con esta propuesta de un modelo de revisión de un Plan De Recuperación Ante Desastres De Tecnología buscamos implementarla en las organizaciones con la finalidad que otras también puedan utilizarla ya que la misma está alineada a la norma ISO 22301 y tiene todos los elementos a considerar para la realización de un Plan De Recuperación Ante Desastres De Tecnología. Cabe destacar como hemos mencionado anteriormente que algunas organizaciones agregan o quitan algunos elementos, pero al final se colocaron lo más importante.

Este elevado nivel de madurez que encontramos en la entrevista realizada no indica que muchas organizaciones financieras están haciendo lo correcto con el uso de los planes de contingencia por tanto esta propuesta del modelo de revisión puede ayudar a la mejora continua del Plan De Recuperación Ante Desastres De Tecnología.

## BIBLIOGRAFIA

Atalait, J. (2011), ¿Qué debe tener un Plan de Recuperación de Desastres? Recuperado de <https://www.atalait.com/blog/que-debe-tener-un-plan-de-recuperacion-de-desastres>

Amaya, J, (2012), ¿Qué es y por qué hacer un Análisis de Riesgos? Recuperado de <https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/>

Alfaro, D, (2018) La importancia de implementar un plan de recuperación ante desastres Recuperado de <https://www.itsitio.com/us/la-importancia-implementa-plan-recuperacion-desastres/>

Benarroch, M., (2016), BIA – Análisis De Impacto De Negocios, Recuperado de <https://aloglobal.com/ciberseguridad-consultorias-especializadas/bia-analisis-de-impacto-de-negocios/>

Beal, V, (2007), ¿Qué es un Plan de Recuperación ante Desastres de Tecnología Recuperado de <https://www.webopedia.com/TERM/D/DRP.html>

Bustos, S, (2017), ¿Beneficios de implementar un DRP) Disaster Recovery Plan) en las organizaciones Recuperado de <https://www.grupoalbe.com/beneficios-de-implementar-un-drp-disaster-recovery-plan-en-las-organizaciones-pymes/>

Casillas, M., (2018), ¿Qué Es Un DRP?, Recuperado de <https://inbest.solutions/que-es-un-drp/>

Cobser (2003-2016) Análisis de Impacto en el Negocio, [www.cobser.es](http://www.cobser.es), recuperado de <https://cobser.es/analisis-de-impacto-en-el-negocio/>

Kirvan, P., (2015), Guía para planear la recuperación de desastres (DR) de TI, Recuperado de <https://searchdatacenter.techtarget.com/es/tutoriales/Guia-para-planear-la-recuperacion-de-desastres-DR-de-TI>

Muñoz, D., (2003), Proceso Crítico de Negocio, Recuperado de [http://www.surlatina.cl/contenidos/archivos\\_articulos/11-procesoscriticosdenegocios.pdf](http://www.surlatina.cl/contenidos/archivos_articulos/11-procesoscriticosdenegocios.pdf)

Martinez, J., (2009), ANÁLISIS DE IMPACTO. Herramienta imprescindible para una buena política de continuidad del negocio, <http://www.iee.es>, recuperado de <http://www.iee.es/pages/bases/articulos/segu011.html>

Rodriguez, M., (2012), ¿Qué Es Un DRP?, Recuperado de <https://www.inbest.cloud/comunidad/que-es-un-drp>

Software Green House (2018) RPO y RTO recuperado de <https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo>

Vicente, B., (2015). Análisis evaluación para el diseño de un plan de recuperación ante desastres (DRP) aplicación en un centro de dato para Empresas municipales basado en la norma ISO/IEC 24762:2008. (Tesis de Grado). Universidad Politécnica Salesiana Ecuador