UNIVERSIDAD RICARDO PALMA

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA INDUSTRIAL

MENCIÓN EN PLANEAMIENTO Y GESTIÓN EMPRESARIAL

DISEÑO Y APLICACIÓN DE UN PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) EN UN CENTRO DE DATOS PARA EMPRESAS FINANCIERAS BASADO EN LA NORMA ISO/IEC 22301

Tesis para optar el Grado de Maestro en Ingeniería Industrial con Mención en Planeamiento y Gestión Empresarial

AUTOR: Bach. Mario Jacinto Herrada Gutiérrez

ASESOR: Mg. Hugo Mateo López

Lima – Perú

2018

DEDICATORIA

A mis queridos padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo. Todo este trabajo ha sido posible gracias a ellos.

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a todos mis profesores de la Escuela de Posgrado por brindarme sus valiosos conocimientos y su bonita amistad. A si mismo mi gratitud al Dr. Joaquín Lombira Echevarría y al Mg. Ing. Hugo Julio Mateo López, por su acertada dirección en el desarrollo de esta Tesis, y quienes más allá de su trabajo supieron guiarme como un amigo.

RESUMEN

El presente trabajo de investigación tiene como objetivo diseñar e implementar un plan de recuperación ante desastres (DRP) la cual permitirá mantener la continuidad del negocio en un centro de datos para empresas financieras; para ello se utilizó los Marcos de Referencia de la Norma ISO/IEC 22301.

Utilizando la metodología mencionada se logró identificar los posibles riesgos, fortalecer la capacidad de respuesta y optimizar la restauración de la información, ellos ayudo a un mejoramiento permanente en los estándares de respuesta y continuidad.

Se puede afirmar que la metodología basadas en la norma ISO/IEC 22301 cuyo objeto es de estudio de este trabajo, es el artefacto inicial con el que toda empresa debería contar sin importar las iniciativas de negocio que tenga previsto lanzar, así mismo va a permitir que las organizaciones estén preparadas ante una interrupción de su negocio, por medio de la definición y documentación de procedimientos y estrategias de recuperación.

Palabras claves: ISO/IEC 22301, Plan de recuperación, posibles riesgos, capacidad de respuesta, restauración de la información.

ABSTRACT

The present research work aims to design and implement a disaster recovery plan (DRP) that allows to maintain the business continuity in a data center for financial companies; for this purpose, the Reference Frameworks of the ISO / IEC Standard 22301 were used.

Using the mentioned methodology, it was possible to identify the possible risks, to strengthen the capacity of response and to optimize the restoration of the information, they helped to a permanent improvement in the standards of response and continuity.

It can be said that the methodology based on ISO / IEC 22301, whose purpose is to study this work, is the initial artifact with which every company should count regardless of the business initiatives that it plans to launch (business architectures, process-oriented architecture, service-oriented architecture, automation and business process improvement), allows the organization to be prepared in the event of a business interruption, through the definition and documentation of recovery

Keywords: ISO/IEC 22301, Plan of recovery, possible risks, capacity of answer, restoration of the information.

ÍNDICE

CAPÍTULO I: PLANTEAMIENTO DEL ESTUDIO

1.1 Introducción

Mientras tengamos una continuidad en las operaciones y estas sean normales dentro del negocio, debemos considerar que siempre estará latente el riesgo y por consiguiente la probabilidad de que existan pérdidas potenciales o interrupciones no programadas asociadas a un evento de desastre, por lo que es de suma importancia elaborar un plan que sea viable y factible de recuperación, el cual nos permitirá asegurar la continuidad de las operaciones en la organización, a través de una planificación adecuada, una preparación, y la comunicación que serán los componentes claves, para lograr un exitoso plan de recuperación ante desastres (DRP).

A sí mismo en el caso de suscitarse un evento de desastre, es importante disponer de una estrategia de recuperación y que sea inmediata, el cual nos va a permitir el restablecimiento del negocio en menor tiempo, logrando así reducir o mitigar el impacto.

Por otro lado, el presente documento muestra los posibles tipos de contingencias, desastres, y los planes de acción para la recuperación de la información y la continuidad del negocio. Además, proporciona una directiva estratégica y una estructura común para todas las actividades. De la misma manera esta debe cumplir con los estándares corporativos y se deben adecuar a la norma ISO/IEC 22301.

Es por ello por lo que para mitigar las consecuencias que podría causar un evento de desastre, existen los planes de recuperación, los cuales consisten básicamente en acciones para recuperarse en se presente un desastre. Incluye la planeación de pasos y procesos para evitar riegos, mitigarlos o transferirlos a medios más seguros. Hoy en día un Plan de Recuperación ante Desastre es aplicable en todos los aspectos de un negocio.

1.2 Formulación del Problema y Justificación del Estudio

Problema General

¿Cómo mantener la continuidad del negocio ante un evento de desastres en un centro de datos para empresas financieras?

Problemas Específicos

- ¿Cómo identificar los posibles riesgos que pueden afectar adversamente la integridad en un centro de datos para empresas financieras?
- ¿Cómo fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras?
- ¿Cómo optimizar la restauración de la información en un centro de datos para empresas financieras?

Justificación del estudio

El propósito de desarrollar esta tesis estuvo en analizar la necesidad que surge en la empresa Financiera, para contar con un plan de contingencia que le permita reducir el impacto, los efectos de la perdida potencial de infraestructura y reducir al mínimo la pérdida de información y disponibilidad del servicio.

Para ello se diseñó e implemento un Plan de Recuperación ante Desastre basados en la normativa ISO 22301, el cual ayudo a disminuir la proclividad del negocio a interrupciones y reducir considerablemente los riesgos relacionados con la integridad, confidencialidad y disponibilidad del centro de datos.

Los principales beneficiados fueron la propia Empresa Financiera, los directivos y los trabajadores, ya que podían garantizar a sus clientes que las transacciones no sufrirían una pérdida de continuidad, y teniendo como visión posicionarse el mercado y ser líder en el rubro Financiero.

1.3 Antecedentes relacionados con el Tema

Farro (2015) realizó un trabajo de investigación que tuvo como objetivo elaboración de un plan de recuperación ante desastres para una empresa operadora satelital en el Perú y el diseño de una estación terrena satelital redundante para cualquier empresa de telecomunicaciones satelitales como alternativa de contingencia ante un posible desastre natural. La metodología que se usó para su desarrollo fue en base a los niveles de madurez y de riesgo, el cual permitió establecer el nivel de madurez actual de las operadoras satelitales y el nivel de riesgo de las amenazas latentes, utilizando a si una matriz de riesgo para determinar su severidad. Se halló que empresa no puede cubrir las necesidades básicas para reiniciar las operaciones desde un punto de vista de datos. El no contar con un plan de recuperación ante desastre previamente podría acarrear un gasto significativo para la recuperación de todos sus servicios básicos. Esta propuesta tuvo un plan de acción que consistió en analizar las amenazas de mayor probabilidad que puedan impactar seriamente las operaciones en el sector satelital, proponer actividades que ayuden a definir el plan de acción macro del programa de Recuperación ante Desastres y justificar la inversión de la implementación del Plan de Recuperación ante Desastre a diferencia con la no implementación de este.

García (2015) realizó una investigación donde menciono que la empresa plantea encontrar el grado de vulnerabilidad que posee la organización en materia de interrupción de servicios importantes para actuar en consecuencia, definir cuáles serán las medidas preventivas a tomar para reducir al mínimo posible la probabilidad de que ocurra un desastre y el impacto que pueda generar. Se diagnosticó que existen factores externos e internos que pueden alterar sus insumos, sus procesos y sus resultados. Es por ello por lo que se desarrolló una propuesta de Plan de Recuperación de Desastre con la recomendación e invitación al Instituto Politécnico Nacional particularmente a la Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas (UPIICSA), para implementar esa valiosa herramienta que le permitió regresar a la normalidad y proteger la valiosa información cuando una contingencia se llegue a presentar.

Ávila (2013) desarrolló un trabajo que tuvo como objetivo la elaboración de un directorio de procedimientos, planes de contingencia en caso de presentarse eventualidades, desastres, en el sistema integrado de manufacturas, dentro del departamento de ingeniería de la empresa Continental Tire Andina, basado en estándares y normas fijadas por la división de TI de Continental Tire Américas. Se observó que a pesar de que la empresa contaba con políticas y normas en cuanto al acceso del recurso tecnológico disponible, existe la necesidad de contar con métodos y planes efectivos que sean fácilmente aplicables y del conocimiento del personal ante la presencia de una contingencia o eventualidad mayor. La principal debilidad que se presenta al momento de brindar el soporte necesario para superar el percance es la falta de conocimiento personal (prioridad, tiempo, criticidad) y uso de un método ágil que los lleve a superar rápidamente los problemas, además de la falta de recursos y herramientas informáticas. Las propuestas de mejora que se plantearon fueron analizar los sistemas existentes dentro del departamento de ingeniería para definir requisitos previos, como el tipo de información, aplicaciones, infraestructura, entre otras, y especificar técnicamente los requisitos en base a los estándares y normas fijadas por Continental Tire Américas, necesarios para establecer, implantar e implementar un Plan de Recuperación ante Desastre dentro del departamento de ingeniería de la empresa Continental Tire Andina S.A.

Sáez (2015) elaboró un trabajo que tuvo como objetivo principal garantizar una respuesta frente a incidentes que pueden poner en riesgo la operación de la organización, brindando seguridad a los trabajadores, proteger los activos de la organización como procesos y tecnología, minimizando el tiempo de interrupción y asegurar la buena reputación de la organización. Se evidencio que las organizaciones Chilenas presentan serios problemas de continuidad de negocio y que a pesar de la complejidad de la geografía Chilena y la cantidad de amenaza que afectan a las distintas actividades económicas, no se encuentra literatura sobre el tema de BCP y la modesta información encontrada, se refiere al tema, como una herramienta para los sistemas de información, es por esto que surge la necesidad de que las empresas Chilenas se pongan a trabajar en lo que a continuidad de negocio se refiere cuanto antes, ya que en países desarrollados de Europa es prácticamente un estándar. La metodología que se usó fue en base a su análisis y alcance de sus resultados, esa investigación fue de carácter exploratoria ya que el objetivo fue examinar un tema o problema poco conocido del

cual se puedo inferir en la posibilidad de continuar su estudio para ser profundizado o crearse nuevas investigaciones a partir de la existente, en este caso es la creación de un nuevo Modelo de Plan de Continuidad de Negocio. Esta propuesta tuvo un plan de acción que consistió en analizar las metodologías existentes y estándares internacionales para su implementación de un Plan de Continuidad de Negocio y extraer sus principales fortalezas, identificar sus actividades necesarias para diseñar, implementar y mantener un Plan de Continuidad de Negocio (BCP) en Chile y finalmente analizar su cultura organizacional de las empresas chilenas, con la finalidad de detectar las características más importantes, para ser aprovechadas al momento de la implementación y gestión del BCP.

Mannella (2012) realizó un trabajo de investigación que tuvo como objetivo estructurar una guía que conduzca al uso adecuado de la computación en la nube como mecanismo de recuperación ante desastres tecnológicos para las Pymes de servicios en el Distrito Metropolitano de Lima (DMQ). La metodología que se uso fue el método científico basado en el conocimiento de lo exploratorio, Ya que se trató de tener una visión general aproximada de la realidad de las Pymes de Lima en cuanto a su conocimiento y uso de DRPs a través de mecanismos de computación en la nube, de los descriptivo, debido a que la preocupación primordial de ese diagnóstico radica en describir características fundamentales de los grupos homogéneos a ser evaluados, como lo son las Pymes de Servicios en Lima, en cuanto al tema de estudio, de uso de DRP y a la computación en la nube como el vehículo para llevar a cabo esto. Dado que la descripción hace uso de la fundamentación teórica y para ello fue necesario medir los resultados de esa investigación y finalmente lo explicativo, por cuanto buscará conocer las causas que determinaron las razones por las cuales en las Pymes de Lima no se tiene planes de recuperación ante desastres, y peor aún a través de modelos de computación en la nube, y qué efecto tiene esto en la estabilidad del negocio. Se observó que la Pymes no se encuentran preparadas para una recuperación ante desastre tecnológico, esto se debe al bajo grado de importancia otorgados por parte de los ejecutivos, debido al desconocimiento de mecanismos de recuperación ante desastres tecnológicos, provocando incluso perdidas económicas sustanciales y hasta de cartera de clientes. Las propuestas de mejora que se presentaron fueron fundamentar teóricamente el uso de la computación en la nube como mecanismo de recuperación ante desastres tecnológicos en las Pymes, efectuar el diagnóstico sobre la situación actual de las Pymes frente a la

implementación de un plan de recuperación ante desastres, elaborar una guía de implementación de recuperación ante desastres a través del uso de la computación en la nube enfocada a las Pymes y finalmente validar la guía implementada que resulte del su estudio mediante el criterio de expertos.

1.4 Objetivos Generales y Específicos

Objetivo General:

Diseñar e implementar un plan de recuperación ante desastres (DRP) basado en la Norma ISO/IEC 22301 que permita mantener la continuidad del negocio en un centro de datos para empresas financieras.

Objetivos Específicos:

- Diseñar y aplicar un método de análisis de vulnerabilidad que permita identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras.

- Diseñar y aplicar un método de pruebas de simulación que permita lograr fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras.

- Diseñar y aplicar un método de planes de respaldo que permita optimizar la restauración de la información en un centro de datos para empresas financieras.

1.5 Limitaciones Del Estudio

Si se decide implementar el DRP por el Departamento de Tecnología de Información, dependiendo de la alternativa de recuperación los limitantes serian:

- **Recursos Económicos:** El presupuesto que sea aprobado puede modificar las características de la alternativa seleccionada por parte del Departamento de Tecnología de Información. El proceso de implementación de la solución puede afectarse dependiendo que el presupuesto.
- **Recursos Tecnológicos:** Dependiendo de la alternativa seleccionada estamos sujetos a la disponibilidad de los equipos, servidores virtuales, equipos de activos de comunicación u otros implementos que se necesiten para la solución propuesta.

- **Recursos Humanos:** Es indispensable contar con el recurso humano capacitado para la implementación, control y seguimiento del DRP.

CAPÍTULO II: MARCO TEÓRICO

2.1 Bases Teóricas relacionadas con el Tema

Norma ISO/IEC 22301

De acuerdo con la norma ISO 22301 (2012) ésta es utilizada por organizaciones de todos los tamaños y tipos. Las organizaciones luego de implementar los estándares son capaces de obtener la certificación, lo cual permite a las empresas demostrar ante entidades reguladoras, clientes, posibles clientes y otras partes interesadas que mantienen sistemas de gestión basados en las buenas prácticas.

Hoy en día la norma es utilizada para obtener una certificación, y, por ende, incluye ciertos requisitos cortos y concisos que describen los elementos centrales de la gestión de la continuidad del negocio.

Por otro lado, esta norma provee un marco referencial en las organizaciones interesadas en la administración y gestión de la continuidad del negocio, que permite cumplir los requisitos reglamentarios y del cliente, así como los propios de las empresas.

A si mismo esta norma contiene ciertos requisitos que pueden ser auditados objetivamente, por lo tanto, pueden ser utilizado por una organización para asegurar que las partes interesadas usen un SGCN apropiadas en su lugar; y ha sido diseñada para lograr una mayor seguridad social (proporcionar protección de la sociedad, y responder a, incidentes, emergencias y desastres provocados por actos humanos intencionales, riesgos naturales y fallas técnicas).

Actualmente esta norma ISO 22301 a reemplazado a la norma británica BS 25999-2, estas dos normas son casi similares, sin embargo, la ISO/IEC 22301 es considerada como una versión mejorada de la BS 25999-2, y; a diferencia de la norma británica ha sido aceptada por institutos de normas nacionales a nivel

mundial.

Los objetivos de la norma ISO 22301 están enfocados en 4 pilares principales como se muestran a continuación:

- ✓ "Entender las necesidades que tiene la organización y los requisitos para establecer políticas y objetivos para la gestión de la continuidad de negocio;
- ✓ Implantar y operar controles y medidas para el manejo de la capacidad de una organización para la gestión de incidentes que causan interrupciones;
- ✓ Seguimiento y revisión del desempeño y la efectividad del SGCN;
- ✓ Mejora Continua basada en mediciones objetivas"

El modelo actual de la norma ISO 22301 exige cierta documentación obligatoria, que una empresa de acuerdo con su alcance y estructura debe desarrollar, esta documentación es la siguiente (Alexander, 2012):

- ✓ Lista de requisitos legales, normativos y de otra índole.
- ✓ Alcance del Plan de recuperación ante desastre.
- ✓ Política de la continuidad del negocio.
- ✓ Objetivos de la continuidad del negocio.
- ✓ Evidencia de competencias del personal.
- ✓ Registros de comunicación con las partes interesadas.
- ✓ Análisis del impacto en el negocio.
- ✓ Evaluación de riesgos, incluido un perfil del riesgo.
- ✓ Estructura de respuesta a incidentes.
- ✓ Planes de continuidad del negocio.
- ✓ Procedimientos de recuperación.
- ✓ Resultados de acciones preventivas.
- ✓ Resultados de supervisión y medición.
- ✓ Resultados de la auditoría interna.
- ✓ Resultados de acciones correctivas.

Cláusulas claves de ISO 22301

La norma ISO 22301 está organizada en base a las siguientes cláusulas principales:

- ✓ Cláusula 4: Contexto de la organización.
- ✓ Cláusula 5: Liderazgo.
- ✓ Cláusula 6: Planificación.
- ✓ Cláusula 7: Soporte.
- ✓ Cláusula 8: Operación.
- ✓ Cláusula 9: Evaluación del desempeño.
- ✓ Cláusula 10: Mejora.

Cada una de estas Cláusulas Principales se describe brevemente a continuación:

<u>Cláusula 4:</u> Contexto de la organización

Esta cláusula determina los requerimientos necesarios para establecer el propósito del SGCN, como debe aplicar temas internos y externos que son relevantes para el propósito de la organización y que afectan su habilidad de alcanzar los resultados esperados como:

- ✓ Actividades de la organización, sus funciones, servicios, productos, sociedades, cadenas de suministros, relaciones con las partes interesadas y el impacto potencial relacionado con un incidente que genere una interrupción.

- ✓ Vínculos entre la política de continuidad de negocio y los objetivos de la organización y otras políticas, incluyendo, la estrategia de gestión de riesgos globales.

- ✓ Leyes, regulaciones y otros requisitos aplicables, a los cuales la organización está suscrita.

- ✓ Identificar el alcance del SGCN, tomando en cuenta los objetivos estratégicos de la organización.

Cláusula 5: Liderazgo

Esta cláusula realiza un resumen de las exigencias a la alta gerencia de la organización, en relación con su rol en el SGCN, de manera que el sistema de gestión pueda funcionar eficazmente en sinergia con los objetivos de la empresa. Existen nuevos requerimientos para la alta gerencia, tales como:

- ✓ Asegurarse que el sistema de gestión de continuidad del negocio es compatible con la dirección estratégica de la organización.
- ✓ Integración de los requerimientos del Sistema de Continuidad del Negocio en los procesos del negocio.
- ✓ Comunicar la importancia de una eficaz gestión de la continuidad del negocio.

Cláusula 6: Planeación

Esta es una etapa crítica en la que se establecen objetivos estratégicos de continuidad del negocio, estos objetivos deben estar relacionados a la política de continuidad del negocio de la organización, y, deben ser medibles mediante las metas alcanzadas. Los objetivos de la continuidad de negocio deben:

- ✓ Estar alineados con la política de continuidad de negocio.
- ✓ Considerar el nivel mínimo de productos y servicios que es aceptable para que la organización alcance sus objetivos.
- ✓ Ser medibles, tomando en cuenta requisitos aplicables.
- ✓ Ser controlados y actualizados, según sea apropiado.

Cláusula 7: Soporte

Esta cláusula detalla el soporte requerido para establecer, implementar y mantener un Sistema de Gestión de Continuidad del Negocio eficaz, considerando todos los recursos necesarios, así como requerimientos para la gestión y registro de documentos.

El tema de comunicaciones es adicionado a la cláusula, constituyendo un punto importantísimo al gestionar cualquier alteración en la organización.

Cláusula 8: Operación

Después de la planificación del SGCN, la organización debe ponerlo en funcionamiento. Esta cláusula incluye:

- ✓ **Cláusula 8.1: La cláusula planificación operacional y control**

  Esta cláusula requiere que la organización asegure la existencia de procesos que hayan sido desarrollados para gestionar que los riesgos al SGCN estén correctamente implementados.

- ✓ **Cláusula 8.2: El Business Impact Analysis**

  Para la norma ISO 22301, esta cláusula introduce un nuevo término: "esquemas de tiempo priorizados", que define el orden y los tiempos para la recuperación de actividades críticas que soportan los productos y servicios claves.

Cláusula 9: Evaluación del desempeño

Permite realizar un seguimiento del sistema, y establecer revisiones periódicas para mejorar su operación, luego de implementado el sistema de gestión. Entre las principales actividades se tienen:

- ✓ Seguimiento de la medida en la cual la política, objetivos y metas de continuidad de negocio son cumplidos.

- ✓ Medición del desempeño de los procesos, procedimientos y funciones que protegen las actividades priorizadas.

- ✓ Seguimiento de la conformidad con esta norma y con los objetivos de la continuidad de negocio.

- ✓ Seguimiento histórico de evidencia de desempeño deficiente del SGCN.
- ✓ Realización de auditorías internas a intervalos planificados; y
- ✓ Evaluación de todo lo anterior en las revisiones por la dirección, a intervalos planificados.

<u>Cláusula 10:</u> Mejora

Constituyen todas las acciones realizadas a lo largo de la organización, para aumentar la eficacia (cumplir objetivos) y la eficiencia (costo/beneficio óptimo) de los procesos y controles de seguridad, para brindar más beneficios a la organización y a sus partes interesadas, tal como se puede apreciar en la Figura N° 2.1

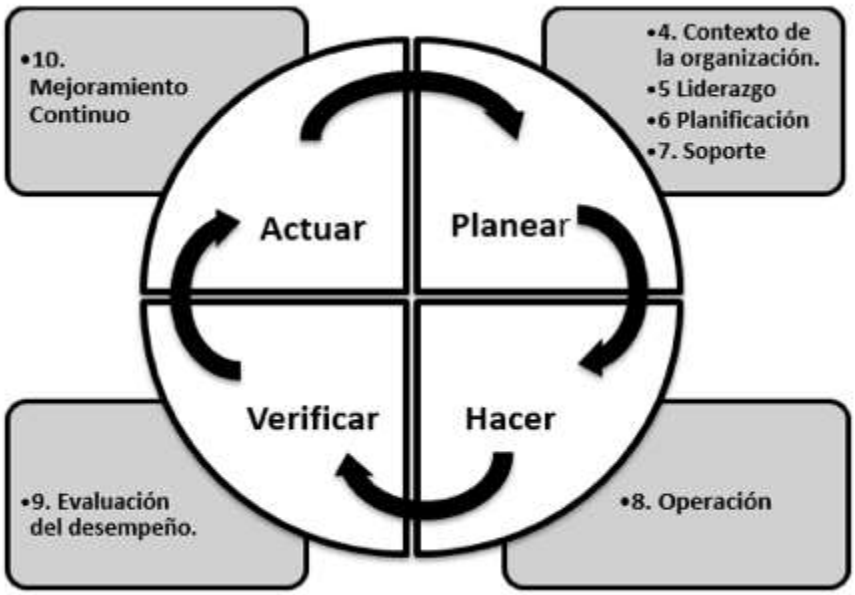

Figura 0.1: Ciclo DPCA y la ISO 22301

Fuente y elaboración: Norma ISO 22301,2012

Modelo de Gestión del Ciclo de Deming

Estas actividades tienden a mejorar la calidad son las catalizadoras para crear reacciones en cadena económicas, provoca reducción de costos, menos errores etc. Deming creía que, si no se realizaban esfuerzos para mejorar la calidad, este proceso nunca se iniciaría. La calidad tiene que seguir un ciclo donde se planea, se hace, se verifica y se actúa para seguir mejorando.

El ciclo de Deming o mejora continua es una guía para mejorar de forma continua y sistemática, básicamente está constituida por cuatro actividades: planificar, hacer, verificar y actuar PHVA o por sus siglas en inglés PDCA; plan, do, check and act, tal como se puede apreciar en la Figura N° 2.2

Figura 0.2: Ciclo de Deming

Fuente y elaboración: Norma ISO 22301,2012

Planificar:

En esta fase se preguntan cuáles son los objetivos que se quiere alcanzar. primero deberemos recopilar la información de la empresa para poder establecer la situación actual. La planificación aporta con soluciones posibles de las causas que producen los fallos o defectos.

Hacer:

Consiste en realizar o poner en marcha las soluciones que se planificaron para corregir los fallos. En esta fase se forma al personal encargado de poner en marcha el plan, para de esta manera poder ejecutar el plan experimentalmente y poder comprobar su eficiencia antes de hacerlo en todo el campo.

Verificar:

Es el momento de comprobar y controlar el avance y efectividad del plan de mejora, se medirán el cumplimiento de los objetivos y se observará los fallos existentes.

Actuar:

Aquí se documentará y se escribirá lo aprendido, se normalizará y formalizará los cambios que se adoptarán. Con los fallos aún existentes se realizará nuevamente el ciclo PHVA.

Desarrollo del Ciclo PHVA

Plan (planificar)

Aceptar que existen problemas

La información referente a los problemas puede provenir de diferentes fuentes. Para solucionar problemas, la administración debe participar en la aceptación e identificación de problemas.

Los problemas se describen en términos muy generales y aún no se han definido claramente los aspectos específicos del problema.

Formar equipos de mejora de la calidad

A este equipo se le debe encomendar la tarea de investigar, analizar y buscar una solución al problema en un plazo determinado. El equipo de resolución de problemas debe formarse con gente que tenga conocimiento del proceso o problema bajo estudio.

Definir con claridad los problemas

Una vez formado, el equipo de mejora de la calidad se dedica a definir con claridad el problema y su alcance.

Desarrollar mediciones del desempeño

Las mediciones pueden ser de naturaleza financiera, orientadas al cliente o relativas al funcionamiento interno de la organización. Las mediciones financieras se enfocan en determinar si los cambios hechos mejorarán el desempeño financiero de una organización. Las mediciones orientadas al cliente incluyen tiempos de respuesta, tiempos de entrega, funcionalidad del producto o servicio, precio, calidad u otros factores intangibles. Las mediciones relativas se enfocan en la mejora de procesos, productividad, capacidades y productividad de los empleados.

Analizar problemas

La información recopilada en esta etapa ayudará a determinar posibles soluciones. El análisis debe ser exhaustivo para poner al descubierto todas las complejidades implícitas u ocultas en el problema.

Determinar causas

Un diagrama de flujo da a los solucionadores de problemas una mayor comprensión de los procesos involucrados. La lluvia de ideas es una excelente técnica para empezar a determinar las causas.

Do (hacer)

Seleccionar e implementar una solución

Una vez que se identifica la causa, es el momento de proponer posibles soluciones. Esto inicia la sección Hacer del ciclo PDCA. Tan fuerte es el deseo de hacer algo que muchos solucionadores de problemas se ven tentados a reducir a prácticamente nada el tiempo destinado a planificar. Las mejores soluciones son aquellas que resuelven el problema real. Estas solo se encuentran después de identificar la causa raíz del problema.

La solución se debe evaluar contra cuatro criterios generales:

1. La solución se debe elegir con base en su potencial para evitar una recurrencia del problema.
2. La solución debe abordar la causa raíz del problema.
3. La solución debe ser rentable. La solución más cara no necesariamente es la mejor para los intereses de la empresa.
4. La solución debe tener la capacidad de implementarse en un tiempo razonable.

Para garantizar el éxito de la implementación de la solución es de vital importancia asignar deberes a individuos específicos y hacerlos responsables de llevar a cabo la tarea.

Check (verificar)

Evaluar solución

Para determinar si la solución ha funcionado, se deben aplicar las mediciones del desempeño creadas en el paso 4. Se debe utilizar gráficas de control, histogramas, etc. tanto antes como después. Si se utilizaron estos recursos durante el análisis inicial del problema, se puede generar una comparación directa para determinar cómo se está ejecutando la solución.

Act (actuar)

Asegurar la permanencia de la solución

Actuar, implica tomar la decisión de adoptar el cambio, abandonarlo o repetir el ciclo de resolución de problemas. Si se adopta el cambio, se deben realizar esfuerzos para asegurar que los nuevos métodos se han establecido. Es fácil pensar que el método "nuevo y mejorado" debe utilizarse, sin embargo, existe la tendencia de regresar a los viejos métodos, controles y procedimientos cuando se incrementa el estrés.

Mejora continua

Una revisión de operaciones pondrá al descubierto muchas oportunidades de mejora. Cualquier fuente de desperdicio, como las reclamaciones de garantía, horas extra, recortes, repetición de procesos, retrasos de la producción o áreas que necesiten más capacidad, son proyectos potenciales. Incluso las mejoras pequeñas pueden dar como resultado un impacto significativo en las utilidades de la organización.

Plan de Recuperación ante Desastre

Definición

Un plan de recuperación de desastres (DRP) se define como la manera en la cual una organización hace frente a posibles desastres, que puede llegar a imposibilitar parcial o totalmente la continuidad de las funciones o actividades de la organización.

Un plan de recuperación de desastres está constituido por las precauciones tomadas para que los efectos de un desastre se reduzcan al mínimo posible, para que la organización sea capaz de mantener o reanudar rápidamente funciones de misión crítica.

La planificación de desastres implica un análisis minucioso de los procesos de la organización, así como las necesidades de esta.

Los planes de recuperación de desastre tienen que acoplarse al grado de complejidad que poseen los sistemas y redes que funcionan en una institución y de esta forma, tratar de prevenir las cosas que puedan salir mal debido a la complejidad de los mimos.

Según Toigo (2002) entre quince a veinte años atrás, si existía una amenaza de incendio para los sistemas, un plan de recuperación de desastres podría consistir en apagar la computadora central y otros equipos antes de que el sistema de rociadores se encendiera, desmontar componentes, y posteriormente secar las placas de circuitos en el estacionamiento con un secador de pelo. Sin embargo, los actuales sistemas empresariales tienden a ser demasiado grandes y complicados para estos métodos sencillos y prácticos, y la interrupción del servicio o la pérdida de datos pueden tener consecuencias financieras graves, ya sea directamente o a través de la pérdida de confianza del cliente.

Los planes de recuperación de desastre óptimos varían sus resultados de organización a organización. La planificación de la recuperación de desastres puede ser desarrollada dentro de una organización o se puede desarrollar en el exterior de esta como una aplicación de software o un servicio. Ver Anexo 13

Objetivos de un DRP

Dentro de los objetivos con los cuales cuenta un plan de recuperación de desastres, uno de los más importantes, es el encontrar el grado de vulnerabilidad que posee la organización en materia de interrupción de servicios importantes para actuar en consecuencia, definir cuáles serán las medidas preventivas a tomar para reducir al mínimo posible la probabilidad de que ocurra un desastre y el impacto que pueda generar.

Un DRP identifica y analiza el posible costo en el servicio y la imagen pública entre otras consecuencias que generan las interrupciones, ya sean

breves o prolongadas en las actividades y cumplimiento de objetivos de la organización que se han visto impactadas por algún desastre.

También posee el objetivo de determinar cuáles son las necesidades al corto, al medio y al largo plazo, de la recuperación y cuáles serán los recursos necesarios para lograr la normalidad y condiciones para el óptimo desempeño de la organización.

A sí mismo un plan de recuperación de desastre identifica las posibles alternativas y cursos de acción que se pueden tomar, así como seleccionar los métodos más rentables y con mayor fiabilidad para suministrar la función de las operaciones de copia de seguridad y la restauración de un servicio a tiempo.

El DRP se encarga de desarrollar e implementar planes de contingencia que se ocupan de las necesidades inmediatas y de largo plazo para el centro de datos y otros servicios empresariales.

Como objetivo general es reducir al mínimo el tiempo de inactividad tecnológica, así como la perdida de datos e información de la organización mediante una recuperación bien planeada, ordenada y coherente después haber tenido el infortunio de ser impactados por una contingencia o desastre.

Según Rivas (2011) para cumplir con los objetivos del DRP de minimizar el tiempo de inactividad y la pérdida de datos al mínimo posible, es importante conocer los siguientes conceptos:

- ✓ **Objetivo de Tiempo de Recuperación (RTO, Recovery Time Objetive),** es el tiempo en el que el proceso de negocio debe estar restaurado después de un incidente grave, con el fin de evitar consecuencias inaceptables derivados de una ruptura en la continuidad del negocio.

Para reducir el RTO, se requiere que la Infraestructura (tecnológica, logística o física) esté disponible en el menor tiempo posible pasado el evento de interrupción.

- ✓ **Objetivo de Punto de Recuperación (RPO, Recovery Point Objetive),** es la edad de los archivos que se deben recuperar de almacenamiento de copia de seguridad para las operaciones tras un incidente grave. El RPO se expresa hacia atrás en el tiempo (es decir, en el pasado) desde el instante en que el incidente se produce, y puede ser especificado en segundos, minutos, horas o días, por lo tanto, es la cantidad máxima aceptable de pérdida de los datos medidos en el tiempo. Para reducir un RPO es necesario aumentar el sincronismo de réplica de datos. Ver Anexo 14

Estado del Arte del DRP

Según Slater (2012) la recuperación de desastres es el proceso mediante el cual se reanudan las actividades después de un evento disruptivo. El evento podría ser algo enorme, como un terremoto o los ataques terroristas contra el World Trade Center, o algo pequeño, como mal funcionamiento de software causado por un virus informático.

Los efectos del 11 de septiembre del 2001 demostraron que, aunque de alto impacto, eventos de baja probabilidad pueden ocurrir, la recuperación es posible. A pesar de que los edificios fueron destruidos y bloques de Manhattan se vieron afectadas, las empresas e instituciones con planes de continuidad bueno sobrevivido.

Las lecciones aprendidas incluyen:

- ✓ Los planes deben ser actualizados y probados con frecuencia;
- ✓ Todos los tipos de amenazas deben ser considerados;
- ✓ Las dependencias e interdependencias deben ser cuidadosamente analizadas;
- ✓ Personal clave puede no estar disponible;
- ✓ Telecomunicaciones son esenciales;
- ✓ Sitios alternativos de copia de seguridad que no debe estar situado cerca del sitio primario;
- ✓ Empleado apoyo (asesoramiento) es importante;
- ✓ Las copias de los planes deben ser almacenados en un lugar seguro fuera del sitio;
- ✓ Considerable perímetro de seguridad puede rodear el escenario de los incidentes relacionados con la seguridad nacional o del orden público y el personal puede impedir el regreso a los edificios;
- ✓ A pesar de las deficiencias, las continuidades de planes de negocio en lugar de pre 11 de septiembre fueron indispensables para el esfuerzo de continuidad,
- ✓ Aumento de la incertidumbre (después de una interrupción de alto impacto, como el terrorismo) puede prolongar el tiempo hasta que las operaciones se normalicen. (PSC, 2013)

La finalidad de conocer el origen del DRP es el aprender del pasado, de lo contrario se está condenado a cometer o vivir los mismos errores que surgieron después de los atentados terroristas del 11 de septiembre del 2001.

En el Global Disaster Recovery Índex publicado por Acronis (2011) se destaca que 6 mil funcionarios de tecnologías de la Información reportaron que los desastres naturales causaron sólo 4% de las

interrupciones de servicio, mientras incidentes en las instalaciones de los servidores (problemas eléctricos, fuegos y explosiones) representaron el 38%. Sin embargo, errores humanos, actualizaciones problemáticas y los virus encabezaron la lista con el 52%.

EL Vice Presidente de VMware Latinoamérica Mollón (2013) señala que la creciente dependencia a los datos en la era de la información, los ha convertido en el activo más valioso de una compañía y a medida que la infraestructura de las tecnologías de información aumenta de igual manera lo hace su complejidad, la importancia de la recuperación de desastres también crece.

Es interesante recalcar que un desastre natural no es la única causa ni la más común que causa interrupciones en los servicios y actividades de una organización. Contar con los debidos respaldos en la tecnología de información es vital para una institución Educativa Segura, por tal motivo se sostiene la importancia de la implementación de un plan de recuperación de desastres.

Ventajas de un DRP como parte de un proceso de contingencia

La correcta implementación de un DRP va a generar como resultado y a su vez ventaja el contar con el respaldo que brinda un plan de contingencia que delimita facultades y responsabilidades de los integrantes del equipo de recuperación de desastre, así como las personas que se encuentran en las instalaciones. Un DRP fundamenta una guía y genera una certeza considerable de que las personas, recursos e instalaciones críticas de las tecnologías de la información puedan seguir funcionales y disponibles en dado caso de que un desastre se presente.

Mediante la implementación y uso de un plan de recuperación de desastre se pueden obtener gran cantidad de beneficios, ya que cuando una contingencia se llega a presentar, esta puede ser de tal magnitud que

ponga en jaque a una institución sin embargo al contar con un DRP la organización puede responder en a la contingencia de una manera rápida y organizada.

Es importante señalar que los beneficios que un plan de recuperación de desastre puede brindar dependerán de las características específicas de cada organización como fue expuesto en la teoría de contingencias en el capítulo anterior, cada organización es única y la solución de una, no necesariamente será la solución para otra.
Según Barnes (2001) dentro de los beneficios que otorga la implementación de un plan de recuperación de desastre mencionados se pueden destacar los siguientes:

- ✓ Se protege la organización ya que se brinda atención de las instalaciones y recursos del centro de datos para asegurar la estabilidad de la organización. Se minimiza el riesgo de retrasos o contratiempos, asegurando que los recursos estén disponibles cuando se les necesita.

- ✓ Se incrementa la fiabilidad y certeza de los sistemas de uso cotidiano como de respaldo, trabajarán de manera adecuada y que permita de manera afectiva cumplir los objetivos organizacionales. Al minimizar la cantidad de decisiones que se deben de tomar cuando se presenta una contingencia, las cuales están forjadas bajo niveles altos de estrés y exigencia debido a las circunstancias y tiempo de respuesta que se posee para hacer frente a la situación.

- ✓ Un beneficio evidente de la implementación de un plan de recuperación de desastre es la seguridad que brinda a la institución y personas que laboran en ella. La sensación de seguridad y certeza que brindan las alternativas y cursos de acción ante un desastre incrementa la confianza desde el

interior de la organización, hasta todas las personas u otras organizaciones que están en contacto con la misma

Sin embargo, según Barnes (2001) otras ventajas que otorga una apropiada aplicación de Plan de Recuperación de Desastre son:

- ✓ La capacidad de proteger los sistemas críticos para la empresa.
- ✓ Reducción de pérdidas tras un incidente.
- ✓ Garantizar la fiabilidad de los sistemas de reserva.
- ✓ Proporcionar un estándar para probar el plan.
- ✓ La reducción de las posibles responsabilidades legales.

Mejora de la eficiencia general de la organización y la identificación de la relación de bienes y recursos humanos y Financieros para los servicios críticos.

Personal involucrado en la aplicación de un DRP en un proceso de contingencia

La aplicación exitosa de un plan de recuperación de desastre depende en gran medida del compromiso de todas las partes que integran una organización, un DRP no se puede lograr sin personal dedicado y con la responsabilidad de mantener los planes, la coordinación de los componentes y las pruebas.

El personal involucrado debe estar capacitado para desempeñar de manera eficiente las tareas que se le encomienden, de igual modo debe de asumir responsabilidades de recuperación y actualización periódica en el DRP.

Debido a la naturaleza misma del plan de recuperación de desastre que enfoca su atención en las tecnologías de información, el personal que

frecuentemente está involucrado en su desarrollo e implementación, proviene del departamento de Sistemas de Información y el equipo de soporte técnico, sin embargo, esto puede variar de organización a organización.

Según Wallace y Webber (2011) cualquiera que sea el departamento o área del cual provengan los integrantes del desarrollo e implementación del DRP es importante que tengan los siguientes conocimientos e información de la organización.

- ✓ Redes y Comunicaciones
- ✓ Gestión de Instalaciones
- ✓ Desarrollo y soporte técnico
- ✓ Administrador de bases de datos
- ✓ Administrador de sistemas
- ✓ Sistemas de seguridad de la información
- ✓ Operaciones
- ✓ Soporte de redes
- ✓ Implementación de redes

Todo el personal debe recibir formación en respuesta a las emergencias, a su nivel esperado de participación. Básicamente, hay tres grupos a los que la formación debe dirigirse, los empleados, directivos y personal de emergencia.

La formación general de los empleados debe asegurar que todos puedan reaccionar de forma automática a las advertencias de una emergencia posible o inminente. También deben ser entrenados en cualquier tarea que se espera que realicen durante una emergencia. Una parte importante de esta formación es el entendimiento básico del plan de recuperación de

desastre y cómo obtener información y orientación en caso de emergencia.

La formación general para los empleados debe incluir:

- ✓ Peligros en los medios de facilidad y vecinos.
- ✓ Las señales de advertencia y su significado, y qué respuesta se requiere que las señales.
- ✓ Responsabilidades definidas específicas de empleo que describen claramente la secuencia de acciones a realizar.
- ✓ Secuencia de las acciones a tomar en caso de emergencia, incluida la forma de informar sobre incidentes ya quienes.
- ✓ Identificación, localización y uso de los equipos de emergencia (extintores, ropa de protección, equipos de respiración tales como capuchas personales).
- ✓ Los procedimientos de apagado de emergencia.
- ✓ Procedimientos de evacuación y rutas, áreas de reunión, y los procedimientos de personal.

La involucración de la gerencia es de vital importancia para el desarrollo e implementación de un exitoso plan de recuperación de desastre, el liderazgo durante una emergencia es crucial para el éxito. Por lo tanto, es necesaria una capacitación más detallada para aquellos que tienen responsabilidades de liderazgo durante una emergencia. Además de la formación en sus deberes y responsabilidades para la respuesta de emergencia, según se define en el plan, deben comprender:

- ✓ La planificación de desastres, respuesta, recuperación, y de estructura de la comunidad.
- ✓ Las responsabilidades en el plan de recuperación de desastre.
- ✓ La ayuda y coordinación mutua entre el sector privado con los organismos gubernamentales.

- ✓ Habilidades de relaciones públicas, de liderazgo y de los medios necesarios para la gestión de desastres.
- ✓ Los intereses específicos de la institución empresas, tales como sustancias peligrosas.

El personal de respuesta a emergencias será aquel que tenga responsabilidades de respuesta específica en el DRP y deben ser entrenados en estos compromisos concretas, los requisitos del plan y sus procedimientos de apoyo. Esto puede requerir que analice la tarea de trabajo para determinar los objetivos específicos de rendimiento deseados.

Por otro lado, una vez determinados los objetivos de rendimiento, un programa de entrenamiento debe estar diseñado para cumplir dichos objetivos.

A sí mismo la capacitación debe asegurar que las funciones de emergencia se pueden realizar de manera adecuada. Las consideraciones generales para el personal de respuesta de capacitación incluyen:

- ✓ Amenazas y vulnerabilidades a las instalaciones de la empresa a causa de desastres.
- ✓ Los procedimientos de respuesta para eventos incluidos en el plan Comando, Control, y las líneas de autoridad.
- ✓ Equipo especial, donde se encuentra, y cómo usarlo
- ✓ Equipos y sistemas de controles (sistemas de riego, fuentes de alimentación y los servicios públicos, sistemas de parada).
- ✓ Generación de informes de estado.

Para Toigo (2002) la capacitación también puede incluir lo siguiente:

- ✓ Responsabilidad Definido para el entrenamiento.
- ✓ Determinación de los sujetos a la formación.
- ✓ El diseño de programas de formación (análisis de tareas de trabajo, los objetivos de rendimiento, los objetivos del programa y los métodos de entrenamiento).
- ✓ Instructores designados.
- ✓ La evaluación del programa, la calidad, y la revisión.

Según la CRM (2013) la Cruz Roja Internacional también plantea ciertos aspectos de seguridad útiles para la prevención y mitigación del desastre en las organizaciones, a continuación, un listado de las más importantes:

- ✓ Mantenga las listas de teléfonos de sus empleados y clientes clave con usted, y proporcionar copias a los miembros clave del personal
- ✓ Si tiene un sistema de correo de voz en su oficina, designar un número remoto en el que se puede grabar mensajes para los empleados. Proporcione el número de todos los empleados.
- ✓ Haga arreglos para la transferencia de llamadas programable para su línea de negocio principal. Si no se puede llegar a la oficina, puede llamar y reprogramar los teléfonos para que suenen en otro lugar.
- ✓ Instale luces de emergencia que se activan cuando se va la luz, son baratos y fáciles de conseguir en la construcción de los minoristas de alimentación.
- ✓ Haga una copia de seguridad de datos informáticos con frecuencia durante el día laboral. Mantenga una cinta de copia de seguridad fuera del sitio.
- ✓ Uso y sistemas de respaldo de la batería. Se agregará una protección para equipos sensibles y ayudar a prevenir un desplome de la computadora si se va la luz.

El recurso humano es y siempre será el aspecto más importante de una organización, en cualquier proyecto de una organización si se desea tener éxito y cumplir con los objetivos planteados se requiere de un personal involucrado, comprometido y responsable con las actividades y la responsabilidad que las mismas conllevan y un Plan de Recuperación no es la excepción.

Estructura de un Plan de Recuperación de Desastre

La estructura de un plan de recuperación de desastre no es única, ya que esta se debe de acoplar a las características específicas de cada organización donde se desarrolle e implemente, el mismo DRP en diferentes Instituciones puede generar resultados desiguales como la teoría de la contingencia lo planea.

Sin embargo, es posible llegar a contar con características similares que puedan brindar la columna vertebral para el desarrollo de un plan de recuperación de desastre.
Según Marianne, Pauline, Amy, Dean y David (2010, pág. 28) en su publicación, los 7 puntos que vienen a continuación resumen la estructura ideal de un plan de recuperación de desastres.

1. Elaboración de la declaración de políticas para el plan de contingencia. Contar con unas directivas formales proporciona la autoridad y orientación necesaria para elaborar un plan de contingencia efectivo.

2. Realización del análisis de impacto sobre el negocio. El análisis del impacto sobre el negocio ayuda a identificar y priorizar los sistemas y componentes críticos de tecnologías de Información.

3. Identificación de controles preventivos. Medidas que reducen los efectos de las disrupciones al sistema y pueden aumentar su disponibilidad y reducir los costos de contingencia del ciclo de vida.

4. Desarrollo de estrategias de recuperación. Tener una estrategia integral garantiza que el sistema se recuperará de manera rápida y efectiva después de una disrupción.

5. Desarrollo de un plan de contingencia. El plan de contingencia debería contener orientaciones y procedimientos detallados para la restauración del sistema dañado.

6. Prueba, formación y ejecución del plan. La prueba del plan identifica lagunas en la planificación, mientras que la formación prepara al personal de recuperación para la activación del plan; ambas actividades mejoran la eficacia del plan y la preparación general de la entidad.
7. Mantenimiento del plan. El plan debería ser un documento vivo que se actualiza regularmente para mantenerlo al día con mejoras al sistema.

En el mismo documento se plantean una secuencia estructurada de 18 actividades para un desempeño óptimo de un Plan de Recuperación de Desastre, que se enumeran a continuación:

1. El equipo de desarrollo del plan debería reunirse con el equipo interno de tecnología, el equipo de aplicación y los administradores de redes, y establecer el alcance de la acción, como, por ejemplo, elementos internos, activos externos, recursos de terceros y enlaces a oficinas/clientes/proveedores; debemos asegurarnos de informar a la dirección del departamento de Tecnología de

Información sobre dichas reuniones para que estén bien informados.

2. Recopilar todos los documentos relevantes de la infraestructura de redes, como los diagramas de las redes, la configuración de los equipos y bases de datos.

3. Obtener copias de los planes de recuperación de redes y de Tecnología de Información existentes; si no los hay, proceder con los siguientes pasos.

4. Identificar las amenazas contra la infraestructura de Tecnología de Información que la dirección considere más preocupantes: por ejemplo, incendios, errores humanos, apagones de energía, fallo de los sistemas.

5. Identificar aquello que la dirección considera que son las principales vulnerabilidades de la infraestructura: por ejemplo, inexistencia de sistemas de respaldo en caso de apagón eléctrico, copias de bases de datos obsoletas.

6. Examinar el historial previo de apagones y disrupciones, y cómo fueron gestionados por la empresa.

7. Identificar los activos Tecnología de Información que la dirección considera de importancia crítica. Por ejemplo: centro de llamadas, granjas de servidores, acceso a internet.

8. Determinar el tiempo máximo de apagón eléctrico que está dispuesta a aceptar la dirección en caso de indisponibilidad de los equipos Tecnología de Información.

9. Identificar los procedimientos operativos que se utilizan actualmente para responder a los apagones críticos.

10. Determinar cuándo se probaron estos procedimientos para validar si siguen siendo adecuados o no.
11. Identificar el/los equipo/s de respuesta de emergencia para todas las disrupciones de la infraestructura crítica de Tecnología de Información; determinar su nivel de conocimientos y preparación para manejar los sistemas críticos, especialmente en casos de emergencia.

12. Identificar las capacidades de respuesta de los proveedores en casos de emergencia; si se han utilizado alguna vez; si funcionaron correctamente; cuánto paga la compañía por estos servicios; el estado del contrato de servicio; la existencia del acuerdo de nivel de servicio y si se usa alguna vez.

13. Recopilar los resultados de todas las evaluaciones en un reporte de análisis de carencias que identifique lo que se está haciendo frente a lo que debería hacerse, con recomendaciones sobre cómo lograr el nivel requerido de preparación y las inversiones necesarias para ello.

14. Lograr que la dirección lea el reporte y acuerde tomar las acciones recomendadas.

15. Preparar un plan de recuperación de desastres que cubra los sistemas y las redes esenciales de Tecnología de Información.

16. Realizar pruebas de los planes y activos de recuperación de sistemas para validar su operatividad.

17. Actualizar la documentación del Plan de Recuperación de Desastre para que recoja los cambios efectuados.

18. Programar la próxima revisión de capacidades de recuperación de desastres Tecnología de Información.

Desarrollo del Plan de Recuperación de Desastre

Según Marianne, Pauline, Amy, Dean y David (2010) una vez definida la estructura y las actividades que desarrollar brindadas por el o Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos se requiere unificarlas y de esta forma desarrollar un Plan de Recuperación de Desastre.

El desarrollo de un DRP siempre debe de involucrar a la gerencia, de lo contrario es posible que no funcione o que los resultados no sean óptimos. La gerencia debe de estar encargada de la coordinación y asegurar la efectividad del DRP. Para que esto sea posible la gerencia es la encargada de brindar todos los recursos necesarios en el desarrollo e implementación. Por último, la gerencia debe de involucrar a todos los sectores o departamentos que integren a la institución en la definición del plan.

Una vez que se cuenta con el apoyo y dedicación de la gerencia se procederá a realizar un análisis de riesgo en el cual se creará una lista de posibles desastres naturales o causados por errores humanos, y clasificarlos según sus probabilidades. A partir de esta lista cada sector o departamento de la institución debe analizar el posible impacto y que consecuencias relacionadas podrían surgir a los desastres puntualizados en la lista. Para incrementar la efectividad del DRP se debe considerar una pérdida total del centro de datos y eventos con impactos de duración mayor una semana.

El siguiente paso es la asignación de prioridades, para ello se analizarán las operaciones y los procesos para determinar la máxima cantidad de tiempo que la institución puede sobrevivir sin ellos. Según la importancia

que tenga cada uno se les asignará un orden de prioridad a la recuperación.
Posteriormente se determinarán las estrategias y las alternativas más prácticas para proceder en caso de un desastre. Todos los aspectos de la organización son analizados, incluyendo hardware, software, comunicaciones, archivos, bases de datos, instalaciones, etc. Las alternativas a considerar varían según la función del equipo y pueden incluir duplicación de centros de datos, alquiler de equipos e instalaciones, contratos de almacenamiento y muchas más. Igualmente, se analiza los costos asociados.

Los datos y documentos que se debe proteger y respaldar pueden variar entre instituciones u organizaciones dependiendo sus características particulares, pero se pueden mencionar, inventarios, copias de seguridad de software y datos, cualquier otra lista importan y documentación de su personal.

Se recomienda realizar una prueba total de recuperación plan mínimo una vez al año, se debe especificar los procedimientos y la frecuencia con que se realizan las pruebas Estas pruebas tiene la finalidad de verificar la validez y funcionalidad del plan, determinar la compatibilidad de los procedimientos e instalaciones, identificar áreas que necesiten cambios, entrenar a los empleados y demostrar la habilidad de la organización de recuperarse de un desastre. Al término de las pruebas se debe realizar una retroalimentación con los resultaos obtenidos generando una actualización al plan.

Al finalizar las correcciones posteriores a la prueba del DRP, la gerencia debe tomar la decisión de su aprobación, recordando siempre que la gerencia es la encargada de establecer las políticas, los procedimientos, así como las responsabilidades y de la actualización permanente del plan.

Respaldo de la Información

Un plan de Recuperación de Desastre centra su atención en las Tecnologías de Información, y esto incluye la valiosa información con la que cada Institución cuenta, como lo son la investigación, las patentes, procesos de producción, el know-how e información personal de sus integrantes, por ello es importante saber qué tipo de información y como se debe de respaldar para evitar futuros problemas.

Según Insausti (2010) los siguientes tipos de información tendrán que respaldar para mitigar el riesgo en el caso de presentarse cualquier contingencia:

- ✓ Sistemas / Aplicaciones.
- ✓ Software Base.
- ✓ Datos PC ’s usuarios.
- ✓ Documentación de los sistemas.
- ✓ Parámetros y configuraciones.
- ✓ Usuarios y contraseñas.
- ✓ Configuración de hardware.
- ✓ Investigación y desarrollo.

Procedimientos

- ✓ Procedimientos de recuperación en caso de desastre
- ✓ Procedimientos operacionales
- ✓ Procedimientos administrativos
- ✓ Procedimientos de configuración
- ✓ Procedimientos de respaldo y recuperación de información

Para poder llevar a cabo un respaldo de la información que permita a una organización permanecer tranquila se requiere un respaldo de todo el Sistema, el cual permita la recuperación ante un daño total de la información. Es recomendado realizar respaldos generales de manera periódica, según las condiciones específicas de cada organización lo permitan.

El respaldo de todo el sistema se recomienda realizarlo con una periodicidad mensual y se deben genera dos copias, una de las cuales permanecerá dentro de las instalaciones y la otra debe ser custodiada en forma externa.

Existe un tipo de respaldo llamado Backup de Software Base, el cual permite recuperar la información de los diferentes productos de software base, instalados tales como: sistema operativo, base de datos, Aplicaciones etc. Para asegurar la eficacia de este tipo de respaldo, se realizará un respaldo cada que se instale un nuevo producto o cada que se actualice versión.

Es responsabilidad del administrador del sistema programar un respaldo antes y otro después de cualquier nueva instalación.

Según Insuasti (2010) el Software de las aplicaciones que se utilizan en la organización también debe de ser respaldado, para lo cual se maneja de acuerdo con los siguientes criterios:

- ✓ En ambiente de desarrollo dado la continuidad con que se crean y modifican programas, bases de datos, datos; los respaldos deben realizarse diariamente.

- ✓ En ambiente de producción, se deben asegurar respaldos semanales de la última versión en producción.

- ✓ Será responsabilidad del funcionario a cargo del desarrollo coordinar con los funcionarios responsables de la plataforma informática involucrada, los cambios drásticos en versiones y configuraciones de las aplicaciones en producción para realizar los diferentes respaldos antes y después del cambio.

Por otra parte, pero de manera paralela de datos que se genera en el accionar de una organización, también deben de ser respaldados y para ello se debe obedecer a los criterios descritos a continuación:

- ✓ De acuerdo con la operatividad de las aplicaciones y a la criticidad de los procesos e información, se deben programar respaldos o según requerimientos puntuales.
- ✓ Programar respaldos que permitan el respaldo de toda la base de datos ante el evento de una falla en el sistema.
- ✓ Programar respaldos que permitan respaldar tablas de referencias.

La configuración, es la forma específica en la cual se trabaja en las tecnologías de información, suele estar personalizada y por ende el personal se acostumbra a ella, si surge algún cambio puede afectar el funcionamiento o el desempeño de las personas, debido a esto, es importante realizar respaldos en la configuración y para ello se puede considerar los siguientes criterios:

- ✓ Se debe respaldar todo tipo de configuración que normalmente se pierden cuando se realizan reinstalaciones de software o recreaciones de base de datos, Sistema operativo
- ✓ Los respaldos deben incluir archivos de configuración de: Usuarios, Impresoras, Terminales, dispositivos, parámetros

del sistema, configuración a nivel de discos, parámetros de Base de Datos, etc.

- ✓ Los respaldos de configuraciones deben realizarse mensualmente.

Por último, es importante señalar que cada empleado o usuario es responsable de la información que resida en el PC asignado y será él el encargado de mantener copia de sus archivos más sensibles. Para lo cual también se recomienda que los respaldos sean realizados por lo menos una vez cada mes.

A continuación, se muestra un ejemplo de formato para la gestión de los respaldos de procesos, recuperación de la información crítica. Cabe señalar que este tipo de formato debe de diseñarse ante las características específicas de cada organización. Ver Anexo 15

Plan de Continuidad del Negocio

Objetivo

El plan de continuidad de negocio tiene como objetivo principal establecer la relación entre los diversos planes definidos previamente que permita la recuperación de los servicios críticos planteados dentro de los plazos determinados de acuerdo con las necesidades de la institución.

Alcance

A sí mismo el plan está limitado a los servicios críticos definidos en el alcance que pueden ser afectados por los escenarios de sismos, incendios y apagones.

Objetivos específicos

Como objetivos específicos del plan de continuidad del negocio serian:

- ✓ Establecer la relación, soporte e interacción entre los planes de continuidad realizados previamente.

- ✓ Guiar a los equipos de recuperación ante un desastre, mediante el establecimiento de procedimientos y responsabilidades de prevención, acción y restauración.

- ✓ Evitar confusiones, duplicidad de tareas y tiempos muertos en momentos de presión por la ocurrencia de un desastre.

Equipos de Recuperación

Los equipos que soportan el desarrollo de los planes de continuidad son:

- ✓ Equipo de comunicación de crisis
- ✓ Comité de operaciones en emergencias (COE)
- ✓ Equipo de recuperación de TI
- ✓ Equipo de gestión logística

Instrucciones para el uso del Plan de Continuidad

- ✓ **Invocar el plan**

  El plan entra en vigor cuando ocurre una incidencia ocasionada por sismos, incendios o apagones que afecte las operaciones normales de la institución hasta que se declare el desastre el fin de un desastre.

- ✓ **Declarar el desastre**

  El equipo de comunicación de crisis declara el estado de desastre de acuerdo con los criterios definidos en el plan de gestión de crisis.

- ✓ **Notificar**

  De acuerdo con lo establecido en el plan de gestión de crisis, deben determinar cuándo un incidente se declarar crisis para determinar la activación del plan y las acciones de contingencias pertinentes.

  Además, el comité de operaciones de emergencias, equipo de gestión logística y el equipo de recuperación de TI deben realizar los diagnósticos sobre sus recursos de acuerdo con los lineamientos de cada uno de sus planes que serán notificados al equipo de gestión de crisis.

- ✓ **Comunicar a medios de comunicación**

  El equipo de gestión de crisis determinará, de acuerdo con el nivel de desastre, la información que se debe brindar a los diferentes medios de comunicación, la cual será únicamente a través del comunicador externo del INMP.

- ✓ **Uso de planes**

  Se desarrollan los siguientes planes de continuidad, tal como se aprecia en la Tabla N° 2.1:

Tabla 0:1: Planes de Continuidad incluidos en el SGCN

CÓDIGO	DESCRIPCIÓN
PGC	Plan de Gestión de Crisis
PRE	Plan de Respuesta a Emergencias
PRD	Plan de Recuperación de Desastres
PGL	Plan de Continuidad de Gestión Logística

Fuente y elaboración propia.

Los planes de continuidad desarrollados a lo largo del proyecto interactúan entre sí ante un escenario de sismo, incendios o apagones.

- ✓ **Fase 1: Prevención**

  Son las actividades preventivas que se realizan en la operatividad normal de la empresa con el objetivo de mantener a la entidad bajo un entorno preparado y seguro.

- ✓ **Fase 2: Ocurrencia del desastre**

  Esta fase establece la ejecución de los planes de continuidad debido a la ocurrencia de un desastre ocasionado por sismos, incendios o apagones. Debido al rubro de la institución, cuyo objetivo es brindar servicios de salud a las personas, éstas representan la prioridad de protección para el INMP, tal como se puede apreciar en la Tabla N° 2.2

Tabla 0:2: Actividades ante la ocurrencia de un desastre

COMPONENTE O RECURSO	DESCRIPCIÓN	PGC	PRE	PRD	PGL
Personas	El Comité de Operaciones de Emergencia activa el plan según la magnitud del incidente y lo dispuesto en el Plan de Respuesta a Emergencias, e inicia los pasos para la activación de alarmas, evacuación de las personas		x		

Fuente y elaboración propia.

- ✓ **Fase 3: Evaluación Inicial**

  Esta fase establece la interacción entre los planes inmediatamente después de la ocurrencia de un desastre y la evaluación inicial de

la situación, brindando la información necesaria para toma de decisiones frente a la activación de los planes.

- ✓ **Fase 4: Activación de Planes de Contingencia**

  Esta fase establece la interacción en la activación de planes de continuidad.

  Además, cabe recalcar que paralelamente a las actividades realizadas para mantener la operatividad de la entidad de salid dispuestas en los planes de continuidad el equipo de gestión de crisis se encarga de proteger la información y reputación de la institución frente a los entes externos brindando solo la información necesaria.

Monitoreo

Debido a la criticidad de los servicios del INMP y al ser una entidad estatal, se debe realizar revisiones periódicas, una vez iniciada la activación de los planes de contingencias, sobre el estado de acciones realizadas, uso de recursos e insumos y personal.

2.2 Definición de términos básicos

- ✓ **Amenaza**: Es un fenómeno, sustancia, actividad humana o condición peligrosa que puede ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales. (CIIFEN, 2016, pág. 53).

- ✓ **Bussiness Continuity Planning (BCP):** "Capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades comerciales en un nivel aceptable previamente definido" (Sáez, 2015, pág.5).

- ✓ **Desastre**: “Efecto de un suceso súbito e inesperado que altera la prestación de bienes y servicios de una comunidad en un momento determinado, debido a la exposición desmedida al riesgo” (Pretell, 2014, pág. 3).

- ✓ **Disaster Recovery Planning (DRP): C**onstituye una parte del plan de continuidad de negocio en aquellas compañías que dispongan de infraestructura tecnológica para soportar sus operaciones y, de forma análoga al plan de continuidad de negocio, consta de todas las prácticas necesarias que, en caso de desastre, permiten recuperar en el menor tiempo posible el entorno tecnológico (sistemas, aplicaciones e infraestructuras) que soporta las actividades de una organización. (Sáez, 2015, pág.95).

- ✓ **Disponibilidad**: “En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados” (Instituto Nacional de Tecnologías Educativas, 2012, pág. 28).

- ✓ **Evaluación de Impacto**: “La evaluación de impacto tiene por objeto determinar si el programa produjo los efectos deseados en las personas, hogares o instituciones y si esos efectos son atribuibles a la intervención del programa” (Bello, 2009, pág. 5).

- ✓ **Plan de Contingencia**: “El plan de contingencia es el componente del plan para emergencias, que contiene los procedimientos para la pronta respuesta en caso de presentarse un evento específico” (Bonilla & Carbajal, 2013, pág. 16).

- ✓ **Recuperación de Información**: “Se puede definir como el problema de la selección de información desde un mecanismo de almacenamiento en respuestas a consultas realizadas por un usuario” (Castillo, 2010, pág. 34).

- ✓ **Riesgo**: “Se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad” (CIIFEN, 2016, pág. 49).

- ✓ **Vulnerabilidad**: “son las características y las circunstancias de una comunidad, sistema o bien que los hacen susceptibles a los efectos dañinos de una amenaza” (CIIFEN, 2016, pág. 55).

2.3 Hipótesis

Hipótesis General

Mediante el diseño e implementación de un plan de recuperación basado en la norma ISO/IEC 22301 se logrará mantener la continuidad del negocio para un centro de datos para empresas financieras.

Hipótesis Específicas

- Mediante el diseño e implementación de un análisis de vulnerabilidad se logrará identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras.

- Mediante el diseño e implementación de pruebas de simulaciones se logrará fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras.

- Mediante el diseño e implementación de planes de respaldo se logrará optimizar la restauración de la información en un centro de datos para empresas financieras.

2.4 Relación entre Variables

A continuación, se presenta la matriz de relación entre las hipótesis y las variables, los mismos que se pueden visualizar en la Tabla N° 2.3 y posteriormente se adjunta la matriz de relación entre variables dependientes y definición conceptual tal como se aprecia en la Tabla N° 2.4

Tabla 0:3: Relación entre Hipótesis y Variables

HIPÓTESIS	VARIABLES	INDICADORES
Mediante el diseño e implementación de un plan de recuperación basado en la norma ISO/EIC 22301 se logrará mantener la continuidad del negocio para un centro de datos para empresas financieras.		
Mediante el diseño e implementación de un análisis de vulnerabilidad se logrará identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras.	Variable Independiente: Análisis de vulnerabilidad	Si se implementa / No se implementa
	Variable Dependiente: Posibles riesgos	Número total de posibles riegos
Mediante el diseño e implementación de pruebas de simulaciones se logrará fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras.	Variable Independiente: Pruebas de simulaciones	Si se implementa / No se implementa
	Variable Dependiente: Capacidad de respuesta	Tiempo total en la capacidad de respuesta.
Mediante el diseño e implementación de planes de respaldo se logrará optimizar la restauración de la información en un centro de datos para empresas financieras.	Variable Independiente: Planes de respaldo	Si se implementa / No se implementa
	Variable Dependiente: Restauración de la información	Tiempo total en la restauración de la información.

Fuente y elaboración propia.

Tabla 0:4: Matriz de Operacionalización

VARIABLE	INDICADOR	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL
Posibles riesgos	Número total de posibles riesgos (Bimestral)	Los riesgos son futuros eventos inciertos, los cuales pueden influir en el cumplimiento de los objetivos de la organización, incluyendo sus objetivos estratégicos, operacionales, Financieros y de cumplimiento. Fuente: (Espiñeira, Sheldon y Asociados, 2008, pág. 4). ¿Qué es un riesgo y cómo identificarlo? https://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/boletin-advisory-edicion-12-2008.pdf	Se obtendrán los datos mediante toma de muestras en intervalos de tiempo. Para ello se basará en el estándar ISO/IEC 22301 que facilitan el proceso de desarrollo de un plan de recuperación ante desastres.
Capacidad de respuesta	Tiempo total en la capacidad de respuesta. (Bimestral)	Definida como un esfuerzo mediante el cual se da respuesta oportuna a una situación de emergencia o evento adverso donde la capacidad de respuesta en lo local es superada ante la magnitud del evento, o donde es pertinente la asunción y el ejercicio de responsabilidades multidisciplinarias. Fuente: (Restrepo Gonzales r., 2011, pág. 3). Taller EDAN Salud para el fortalecimiento del componente de Gestión del Riesgo frene a Desastre META-2011. https://es.slideshare.net/giramvndo/equipos-de-respuesta-inmediata-en-salud-ante-desastres	Se obtendrán los datos mediante toma de muestras en intervalos de tiempo. Para ello se basará en el estándar ISO/IEC 22301 que facilitan el proceso de desarrollo de un plan de recuperación ante desastres.
Restauración de la información	Tiempo total en la restauración de la información. (Bimestral)	Los respaldos tienen el objetivo de hacer frente a cualquier perdida de información y poder mantener la continuidad del negocio, por lo que, si contamos con una correcta planificación de copias de seguridad, lo único que nos falta para que la organización pueda seguir funcionando es restaurar la información y volver a la situación previa al desastre. Fuente: (Castro Liceaga R., 2010, pág. 23). Respaldo de la Información, Recuperación y Optimización. http://slideplayer.es/slide/5429021/	Se obtendrán los datos mediante toma de muestras en intervalos de tiempo. Para ello se basará en el estándar ISO/IEC 22301 que facilitan el proceso de desarrollo de un plan de recuperación ante desastres.

Fuente y elaboración propio

CAPITULO IV : METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Tipo y nivel de Investigación

Según Sánchez y Reyes (2009) esta investigación es de tipo aplicado porque se analizó diversas teorías, las cuales se utilizaron para el entendimiento de una realidad práctica, también es tecnológico porque busco la validez de la aplicación de determinadas técnicas en la realidad del estudio y también ayudo a demostrar la validez de la eficacia en los resultados deseados y finalmente es cuantitativo por que dio resultados numéricos.

3.2 Diseño de Investigación.

Según Hernández, Fernández y Baptista (2010) el diseño de la investigación es experimental, en su variante cuasi experimental, porque es un estudio de intervención.

Según Sánchez y Reyes (2009) el diseño es de series de tiempo como se muestra en la siguiente Tabla N° 3.1

Dónde:

Tabla 0:1: Diseño de Serie de Tiempos

NOMBRE	ESQUEMA
Series de tiempo	O_1 O_2 O_3 X O_4 O_5 O_6

Fuente y elaboración propia.

O: Observación o resultado de la variable dependiente

X: Aplicación de la variable independiente

3.3 Población y muestra

La población está constituida por todo el universo de empleados que laboran permanentemente en la empresa financiera de la ciudad de Lima.
Con respecto a la muestra tomada, estuvo constituida por el número total de posibles riesgos, tiempo total en la capacidad de respuesta y tiempo total en la restauración de la información ante un evento de desastre durante los periodos 2014 – 2015 (pre test) y 2016 – 2017 (post test).

3.4 Técnicas e Instrumentos

Esta investigación se pasó en diversos instrumentos que permitieron recopilar información sobre el problema. Estos son algunas de las técnicas que se utilizó:

- ✓ Observación directa: se llevó a cabo en cada uno de los puestos que desempeñan las unidades de observación. La descripción de los datos recabados en la hoja de observación, sirvieron para el diagnóstico de la situación del actual sistema, en concordancia a los objetivos fijados, tal y como se ha venido planteando a lo largo de esta investigación.
- ✓ Observación estructurada: Esta se realizó con la ayuda de elementos técnicos apropiados, tales como: fichas, cuadros, tablas, etc.
- ✓ Entrevista: Se realizó con el fin de tener una conversación con una dinámica de preguntas y respuestas abiertas, en las cuales se socializo una temática determinada relacionada con la problemática a estudiar; esta técnica permitió conocer el punto de vista de diferentes partes involucradas en la discusión.
- ✓ Trabajo de gabinete: Esta etapa incluyo la tabulación de los datos, que se mostró de la siguiente forma (el análisis y la interpretación se incluyeron en las conclusiones y en la teoría, es decir haciendo referencia al marco teórico).

3.5 Recolección de datos

Se tomaron muestras aleatorias de datos de las poblaciones establecidas en el punto 3.3 en determinados periodos de tiempo para el estudio pre-test de datos y conocer que tanto cambian los mismos (variabilidad), conocer como están distribuidos los datos y que relación existen entre ellos, mediante la utilización de la herramienta de la Estadística Descriptiva.

Del mismo modo, para la recopilación de datos para el estudio post-test, según el diseño cuasi-experimental desarrollado; se empleó el análisis inferencial con la prueba Wilcoxon para datos NO paramétricos con pruebas de hipótesis, realizando estimaciones y demostrando causalidad.

3.6 Análisis de datos

A continuación, se presenta la Tabla N° 3.2, Análisis de datos utilizados en la presente investigación.

Tabla 0:2: Análisis de Datos

VARIABLES	INDICADORES	ESCALA DE MEDICIÓN	ESTADÍSTICOS DESCRIPTIVOS	ANÁLISIS INFERENCIAL
Posibles riesgos	Número total de posibles riesgos	Escala de proporción	✓ Media ✓ Desviación estándar ✓ Cuartiles ✓ Mediana ✓ Moda ✓ Asimetría ✓ Curtosis ✓ Prueba de normalidad	Prueba NO paramétrica Wilcoxon
Capacidad de respuesta	Tiempo total en la capacidad de respuesta.	Escala de proporción	✓ Media ✓ Desviación estándar ✓ Cuartiles ✓ Mediana ✓ Moda ✓ Asimetría ✓ Curtosis ✓ Prueba de normalidad	Prueba NO paramétrica Wilcoxon
Restauración de la información	Tiempo total en la restauración de la información.	Escala de proporción	✓ Media ✓ Desviación estándar ✓ Cuartiles ✓ Mediana ✓ Moda ✓ Asimetría ✓ Curtosis ✓ Prueba de normalidad	Prueba NO paramétrica Wilcoxon

Fuente y elaboración propia.

3.7 Matriz de consistencia

A continuación, se presenta la Matriz de Consistencia que se puede visualizar en la Tabla N° 3.3

Tabla 0:3: Matriz de Consistencia

PROBLEMAS GENERAL	OBJETIVOS GENERAL	HIPÓTESIS GENERAL	V.I.	INDICADORES VI	V.D.	INDICADORES VD
¿Cómo mantener la continuidad del negocio ante un evento de desastres en un centro de datos para empresas financieras?	Diseñar e implementar un Plan de Recuperación ante Desastres (DRP) basado en la Norma ISO/IEC 22301 que permita mantener la continuidad del negocio en un centro de datos para empresas financieras.	Mediante el diseño e implementación de un plan de recuperación basado en la norma ISO/EIC 22301 se logrará mantener la continuidad del negocio para un centro de datos para empresas financieras.				
PROBLEMA ESPECIFICO	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECIFICO**				
¿Cómo identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras?	Diseñar y aplicar un método de análisis de vulnerabilidad que permita identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras.	Mediante el diseño e implementación de un análisis de vulnerabilidad se logrará identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras.	Análisis de vulnerabilidad	SI/NO	Posibles Riesgos	Número total de posibles riesgos
¿Cómo se logrará fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras?	Diseñar y aplicar un método de pruebas de simulación que permita lograr fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras.	Mediante el diseño e implementación de pruebas de simulaciones se logrará fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras.	Pruebas de simulaciones	SI/NO	Capacidad de respuesta	Tiempo total en la capacidad de respuesta.
¿Cómo optimizar la restauración de la información en un centro de datos para empresas financieras?	Diseñar y aplicar un método de planes de respaldo que permita optimizar la restauración de la información en un centro de datos para empresas financieras.	Mediante el diseño e implementación de planes de respaldo se logrará optimizar la restauración de la información en un centro de datos para empresas financieras.	Planes de respaldo	SI/NO	Restauración de la información	Tiempo total en la restauración de la información.

Fuente y elaboración propia.

CAPÍTULO IV: RESULTADOS Y ANÁLISIS DE RESULTADOS

4.1 Generalidades

La norma internacional ISO 22301 basada en el "Plan – Do – Check - Act" (PDCA) nos va a permitir planificar, establecer, implementar, operar, funcionamiento, monitoreo, revisión, mantenimiento y mejorar continua, la cual tendrá como finalidad identificar los posibles riesgos que puedan afectar adversamente la integridad de la información, fortalecer la capacidad de respuesta ante un evento de desastre y optimizar la restauración de la información desde tres enfoques:

- ✓ Al reducir el número de posibles riesgos aumentaremos nuestra capacidad física, técnica, personal y organizativa, reduciendo así nuestras vulnerabilidades que están expuestas a las amenazas que enfrentamos.

- ✓ Al reducir el tiempo en la capacidad de respuesta disminuimos la perdida de la información evitando un impacto considerable en la continuidad del negocio y para ello es necesario realizar pruebas de simulación.

- ✓ Al reducir el tiempo en la restauración de la información disminuimos la perdida de continuidad en el negocio y para ello es necesario contar con planes de respaldo cuyo objetivo traer consigo la información a la brevedad permitiendo al negocio volver a funcionar.

Para tal motivo, se han aplicado herramientas propias de estrategia de la ISO 22301 en las distintas etapas de la metodología PDCA (PDCA): Planear, hacer, verificar y actuar. Estas herramientas están enfocada a la mejora continua concernientes a la estabilidad que determina el estado de los procesos que son materia de estudio mediante la utilización de cartas de control para variables y

atributos, así como también estudio de capacidad y el uso de herramientas de calidad como análisis de Pareto, hojas de verificación, diagramas de flujo, entre otras, que la estrategia de la ISO 22301 emplea dentro de su metodología PDCA.

Se empleara el software MINITAB para las cartas de control y análisis de capacidad en la situación pre-test como parte de la medición en el diagnóstico y también en la situación post-test con nuevas mediciones y controles de los procesos para la visualización de los cambios con las mejoras que resultaron de la aplicación del presente trabajo de tesis; el MS Visio se utilizó para los diagramas de flujo que permiten visualizar las actividades que comprenden los procesos sobre todo aquellas actividades que van a ser intervenidas y por último el MS Excel para el registro de toma de datos, Pareto y otros.

La aplicación de las diferentes herramientas de la ISO 22301 no solo han sido parte del estudio que la presente tesis persigue (estudio pre-test, test y post-test), sino también dichas herramientas han sido implementadas como parte de las actividades de mejora que propone la tesis y que permitieron lograr incrementar el desempeño de los procesos mencionados con la consecuente obtención de beneficios en productividad y calidad con efectos positivos económicos.

4.2 Aplicación del Modelo

La aplicación del modelo de gestión se realiza en base a experiencias reales ocurridas en el Banco Financiero y el esquema del nuevo modelo diseñado, como resultado de la integración de la norma ISO 22301, dicha información se registra en los formularios creados en el presente plan.

Los formularios contienen toda la información del modelo aplicado al caso de estudio paso a paso, en éstos se puede evidenciar la ejecución de cada una de las Fases, incluyendo la descripción de su contenido, de manera que la implementación para quienes adopten el modelo sea ágil, adaptable y de fácil comprensión.

4.3 Análisis de vulnerabilidad

Con la implementación de la metodología PDCA basada en la norma ISO 22301 para la empresa financiera, se logró identificar los posibles riesgos, de tal forma que se logró alcanzar a reducir el número total de posibles riesgos que prácticamente eran amenaza potencial para el negocio.

A continuación, se describe a detalle su desarrollo de la siguiente manera:

Planificar

- ✓ **Procedimiento para identificación de requisitos y partes interesadas**

El objetivo de este documento tendrá como finalidad definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos y de otra índole relacionados con la implementación del análisis de vulnerabilidad, como también las responsabilidades para su cumplimiento.

Los usuarios involucrados en este documento serán todos los empleados del área de infraestructura tecnológica del banco financiero.

A sí mismo el oficial de seguridad de TI será el responsable de identificar todas las personas que puedan verse afectadas por la gestión en la implementación del análisis de vulnerabilidad y a todos los requisitos legales, normativos, contractuales y de otra índole que correspondan.

El oficial de seguridad de TI del banco financiero será quien definirá el responsable del cumplimiento de cada requisito individual y que partes interesadas serán notificadas cuando se produzca una modificación.

También el oficial de seguridad de TI del banco financiero deberá enumerar todos los requisitos, partes interesadas y personas responsables en la "Lista de requisitos legales, normativos, contractuales y de otra índole" y debe ser publicada en una carpeta con acceso público a los involucrados para su conocimiento

Por otra parte, el empleado del área de infraestructura tecnológica del banco financiero deberá notificar al oficial de seguridad si detecta o encuentra algún nuevo requisito legal, normativo, contractual o de otra índole que pueda ser importante para la gestión de implementar el análisis de vulnerabilidad.

El oficial de seguridad será la persona responsable de revisar la lista de requisitos legales, normativos, contractuales y de otra índole al menos cada seis meses y de actualizarla cuando sea necesario. El oficial de seguridad notificara a todas las partes interesadas cuando realice una actualización, tal como se puede apreciar en la Tabla N° 4.1

El oficial de seguridad será el propietario y responsable de este documento, que deberá verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Tabla 0:1: Lista de requisitos legales, normativos, contractuales y de otras índoles

Requisito	Documento que impone el requisito	Persona responsable del cumplimiento	Partes Interesadas
Procedimiento para reducir el número total de riesgos	Normas de la SBS para control de instituciones financieras.	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Acuerdos y niveles de servicios internos y externos.	Plan estratégico vigente en la organización	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Procedimiento de seguridad de la información	Políticas y reglamentos de seguridad de la información y	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Plan de recuperación para el área de TI	Plan estratégico de TI vigente en la organización	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Continuidad de los servicios de TI	Plan estratégico operativo anual 2017	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados

Fuente y elaboración propia.

- ✓ **Políticas para definir el alcances y objetivos de la implementación del análisis de vulnerabilidad**

El análisis de vulnerabilidad tendrá como política definir el objetivo, alcance y reglas básicas para su estudio.

A si mismo esta política se aplicará en toda la implementación del análisis de vulnerabilidad del banco financiero.

Por otro lado, los usuarios de estos documentos serán todos los empleados del área de infraestructura tecnológica del banco financiero como también todos los proveedores y socios que cumplen alguna función o forman parte de la implementación del análisis de vulnerabilidad.

El objetivo de la implementación del análisis de vulnerabilidad será identificar potenciales amenazas de riesgo que puedan afectar adversamente el centro de datos de la entidad financiera y los impactos que esas amenazas podrían tener sobre las operaciones del negocio; también servirán para proporcionar un marco de referencia para construir resiliencia organizacional con capacidad de una respuesta efectiva.

A si mismo con la implementación del análisis de vulnerabilidad, el banco financiero cumplirá sus objetivos estratégicos y comerciales como son:

- Brindar un mejor servicio bancario de calidad a los clientes finales.
- Mantener la disponibilidad de los servicios tecnológicos y de negocio en todo momento.
- Continuar siendo una empresa financiera de alta rentabilidad.

La gestión para la implementación del análisis de vulnerabilidad se llevará a cabo conforme a los requisitos enumerados en la lista de requisitos legales,

normativos, contractuales y de otra índole, y dentro del marco referencial definido por los siguientes documentos:

- Plan estratégico vigente de la organización
- Políticas y reglamentos de seguridad de la información vigente en la organización
- Plan estratégico operativo anual 2017

El gerente de producción y servicios de TI será el responsable de definir los objetivos para la implementación del análisis de vulnerabilidad y el método para medir el cumplimiento de estos. El gerente de producción y servicios de TI tiene la responsabilidad de revisar esos objetivos al menos una vez cada seis meses.

Con respecto al alcance del estudio, el análisis de vulnerabilidad se implementará única y exclusivamente en el centro de datos del banco financiero, con especial atención sobre las actividades identificadas durante el análisis de impactos en el negocio.

✓ **Plan de capacitación y concienciación**

Con el objetivo de preparar al personal para que pueda ejecutar sus tareas cumpliendo una función en la gestión de la implementación del análisis de vulnerabilidad, se deberá llevar a cabo la siguiente capacitación, tal como se puede apreciar en la Tabla N° 4.2

Tabla 0:2: Plan de capacitación y concienciación para el análisis de vulnerabilidad

Cargo o nombre	Conocimientos necesarios para el estudio del análisis de vulnerabilidad	Que capacitaciones es necesaria
Gerente de producción y servicios de TI	✓ Procesos del negocio ✓ Políticas organizacionales ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación ✓ Políticas de seguridad informática	✓ Plan de recuperación ante desastre ✓ Gobierno de TI ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo.
Sub gerente de procesamiento e infraestructura Sub gerente de servicios tecnológicos Sub gerente de control tecnológico	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación ✓ Políticas de seguridad informática	✓ Plan de recuperación ante desastre ✓ Gobierno de TI ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo.
Jefe de comunicaciones	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo avanzado de sistemas y equipos informáticos. ✓ Manejo avanzado de redes. ✓ Configuración de equipos de red.	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Herramientas de monitoreo. ✓ Configuración avanzada de equipos de networking.
Jefe de servidores	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo y configuración avanzada de servidores y bases de datos	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Configuración avanzada de bases de datos y servidores. ✓ Administración y mantenimiento de bases de datos.
Jefe de centro de computo	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo y configuración avanzada de equipos Core, Backups y procesamiento	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Configuración avanzada de equipos Core. ✓ Administración y mantenimiento de equipos Core.
Jefe de soporte técnico	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo avanzado de sistemas operativos y equipos informáticos. ✓ Manejo avanzado de aplicativos.	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Instalación de software y mantenimiento de sistemas informáticos. ✓ Manejo de herramientas de gestión.

Fuente y elaboración propia.

Para que los empleados del área de infraestructura de TI comprendan la importancia de implementar un análisis de vulnerabilidad, se deberá aplicar los siguientes métodos de concienciación: boletín informativo, articulo en internet, reuniones conjuntas, mensajes de correo electrónico y grabaciones en video informativo, tal como se puede apreciar en la Taba N° 4.3

Tabla 0:3: Capacitación programada para el análisis de vulnerabilidad

Método de conciencia ción	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio agosto	Agosto	Setiembre	Octubre	Noviembre	diciembre
Boletín informativo	X			X			X			X		
Artículo en internet		X		X		X		X		X		X
Reuniones conjuntas		X		X		X		X		X		X
Mensajes electrónicos	X	X	X	X	X	X	X	X	X	X	X	X
Grabaciones en video informativo			X				X				X	

Fuente y elaboración propia.

Hacer

- ✓ **<u>Metodología para el análisis del impacto en el Centro de Datos</u>**

El objetivo de este documento será definir la metodología y el proceso para evaluar el impacto provocado por una interrupción en las actividades del centro de datos del banco financiero y determinar prioridades.

Este análisis de impacto en el centro de datos será aplicado en todo el alcance de la implementación del análisis de vulnerabilidad; es decir, a todas las actividades que se vean afectadas y amenazadas por posibles riesgos en el centro de datos de la entidad del banco financiero.

Los usuarios de este documento son todos los empleados del área de infraestructura tecnológica del banco financiero que participaran en la implementación del análisis de vulnerabilidad.

- **Organización**

  El análisis de impacto en el centro de datos se realizará una vez finalizada la evaluación de los posibles riesgos para que la información sobre los recursos necesarios pueda ser utilizada a partir de dicha evaluación.

  A sí mismo el manejo de estos documentos confidenciales producidos de acuerdo con esta metodología se realizará en conformidad con las políticas de seguridad de la información y confidencialidad del banco financiero.

- **Identificación de actividades**

  El coordinador TI de la implementación del análisis de vulnerabilidad será la persona responsable de identificar todas aquellas actividades críticas que tengan un impacto significativo en el Core del negocio, y a si mismo deberá designar el personal responsable para cada actividad.

- **Impactos del incidente disruptivo en el centro de datos**

  El impacto que tendrá un incidente disruptivo sobre una actividad en el centro de datos de la entidad financiera será evaluado a través de la siguiente Tabla N°4.4 según clasificación:

Tabla 0:4: Clasificación de impactos en el centro de datos de la empresa financiera

Consecuencia Insignificante	1	La duración del incidente disruptivo no afecta significativamente las operaciones del centro de datos como, por ejemplo: Cables sin ordenar que causen confusión
Consecuencia aceptable	2	La duración del incidente disruptivo provoca daños sobre las operaciones del centro de dato, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas, Por ejemplo: Falla de acceso a la información
Consecuencia Critica	3	La duración del incidente disruptivo provoca daños sobre las operaciones del centro de datos, y ese daño no es aceptable por su magnitud y circunstancias específicas, por ejemplo: Fuga de Líquidos
Consecuencia Catastrófica	4	La duración del incidente disruptivo provoca grandes daños sobre el centro de datos, las obligaciones laborales o el prestigio de la organización, que le harán perder la mayor parte de su capital y/o tendrán que cancelar sus operaciones en forma permanente, por ejemplo: Perdida de Climatización

Fuente y elaboración propia.

- **Presentación de los resultados**

  La información será recabada mediante los cuestionarios elaborados sobre el análisis del impacto en el centro de datos y será enviada al coordinador de TI, que tiene la responsabilidad de reunir y documentarla a través de la estrategia de la implementación del análisis de vulnerabilidad.

- **Revisión periódica de análisis del impacto en el negocio**

  El coordinador TI de la implementación del análisis de vulnerabilidad deberá realizar una revisión de los cuestionarios sobre el análisis del impacto en el centro de datos. Esta revisión se realizará al menos tres veces por año, o con mayor frecuencia en caso de cambios organizacionales significativos.

- ✓ **Estrategia para la implementación del análisis de vulnerabilidad**

El objetivo de este documento tiene como finalidad definir como el banco financiero garantizará que se cumpla todas las condiciones para reanudar las actividades en el centro de datos ante la presencia de posibles riesgos que podrían ocasionar un desastre u otro incidente disruptivo en el centro de datos.

Los usuarios de este documento serán todos los miembros de la alta dirección y personal involucrado en la implementación del análisis de vulnerabilidad.

A si mismo esta estrategia estará redactada en base a los resultados del análisis del impacto en el centro de datos, y la gestión de los posibles riesgos.

- **Análisis del impacto en el centro de datos**

Para analizar el impacto que tendrá el centro de datos ante la presencia de posibles riesgos se establecerá una lista de actividades, las cuales serán las que respaldan la provisión de las operaciones y el servicio del centro de datos para el Core del negocio del banco financiero.

Estas actividades se encuentran listadas (no necesariamente en orden de ejecución), de manera que se determine el número total de posibles riesgos que atentan la continuidad del negocio y el retorno a la normalidad de sus actividades en el centro de datos del banco financiero, tal como se puede apreciar en la Tabla N° 4.6

Tabla 0:5: Actividades que respaldan la provisión de los servicios

Nombre de la actividad
Verificar el correcto funcionamiento de los equipos de Comunicaciones
Realizar monitoreo constante de los equipos de Comunicaciones
Verificar alarmas y conexiones físicas de los equipos de Comunicaciones
Ejecutar acciones preventivas y correctivas de los equipos de Comunicaciones
Verificar el correcto funcionamiento de los servidores, base de datos de aplicaciones de Core Bancario, Negocios, Administrativos y Tecnológicos
Realizar el monitoreo constante del aplicativo de Core Bancario
Ejecutar acciones preventivas y correctivas de los servidores de aplicativos de Core Bancario y Negocios
Limpieza externa de los equipos de Comunicaciones
Realizar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones
Realizar acciones preventivas y correctivas para los aplicativos de Core Bancario y Negocios
Realizar acciones preventivas y correctivas para los sistemas y aplicativos Administrativos, Financieros y Tecnológicos

Fuente y elaboración propia.

- **Gestión de los posibles riesgos**

  Para gestionar los posibles riesgos se procedió a evaluar aquellos riesgos que puedan generar un impacto significativo afectando a si la vulnerabilidad en el centro de datos y para ello se procederá a detallar en la siguiente “Matriz de evaluación de riesgos”.

  Así mismo estos posibles riesgos que podrían producir un incidente disruptivo, es decir, una interrupción en el centro de datos identificada durante la evaluación de riesgos se debería también a lo siguiente:

- El personal de TI posee varias actividades que consumen todo su tiempo
- Ausencia de personal de TI en las capacitaciones
- El personal con acceso a los sistemas del banco financiero no ha sido debidamente capacitado en el uso y manejo responsable de estas aplicaciones.
- Las políticas organizacionales demasiado burocráticas, las aprobaciones de procesos toman demasiado tiempo
- No existe la disponibilidad de los sistemas y equipos para realizar pruebas, mantenimientos
- No cuentan con medidas preventivas para minimizar las posibles consecuencias de tales incidentes (estas acciones también se detallan en el documento "Tratamiento de riesgos.
- No cuenta con un Plan de respuesta a los incidentes la forma adecuada para responder a cada uno de los incidentes.

✓ **Plan de la implementación de análisis de vulnerabilidad**

El objetivo de este plan de implementación de análisis de vulnerabilidad será definir de forma precisa cómo el banco financiero gestionará los incidentes generados por posibles riesgos y cómo recuperará sus actividades el centro de datos dentro de plazos establecidos. A si mismo este plan deberá mantener en un nivel aceptable el daño producido por un incidente disruptivo.

Este plan se aplicará a todas las actividades críticas y que estén expuesta a posibles riesgos, y cuyo alcance será el de la implementación del análisis de vulnerabilidad en el centro de datos.

A si mismo los usuarios de este documento serán todos los empleados del área de infraestructura tecnológica del banco financiero, tanto internos como

externos, que cumplan una función o estén involucrados en la implementación del análisis de vulnerabilidad.

- **Contenido del plan de implementación de análisis de vulnerabilidad**

Nuestro plan de implementar un análisis de vulnerabilidad estará formado por dos grandes secciones:

➢ <u>El plan de respuesta a los incidentes:</u>

El objetivo de este plan será asegurar la protección de la información y de la seguridad en el centro de datos de la entidad financiera ante el caso de un desastre o de otro incidente, como también contener el incidente. A si mismo se lograra reducir al mínimo el número total de posibles riesgos en el centro de datos de la empresa financiera.

Este plan se aplicará a todos los incidentes de severidad alta y que amenazan con interrumpir cualquier actividad crítica dentro del centro de datos, por un período mayor al objetivo de tiempo de recuperación de cada actividad individual, tal como se puede apreciar en la Tabla N° 4.7

Tabla 0:6: Los usuarios de este documento son los empleados de TI del banco financiero.

Cargo	Función y responsabilidad
Empleados del Área de Infraestructura Tecnológica	Establecer los criterios de evaluación de la condición critica
Empleados del Área de Infraestructura Tecnológica	Definir por cada evaluación de criterio las consecuencias de falla y sus calificaciones
Empleados del Área de Infraestructura Tecnológica	Recabar los expedientes de la evaluación de la condición del equipo o la frecuencia de las fallas genéricas
Empleados del Área de Infraestructura Tecnológica	Determinar las frecuencias de las fallas y sus grados
Empleados del Área de Infraestructura Tecnológica	Definir una tabla de rangos para la condición critica
Empleados del Área de Infraestructura Tecnológica	Definir las reglas de los rangos para la condición critica
Empleados del Área de Infraestructura Tecnológica	Seleccionar el sistema o equipo de evaluación
Empleados del Área de Infraestructura Tecnológica	Efectuar el análisis

Empleados del Área de Infraestructura Tecnológica	Jerarquizar los sistemas/equipos por condición critica
Empleados del Área de Infraestructura Tecnológica	Jerarquizar los sistemas/equipos por riesgo

Fuente y elaboración propia.

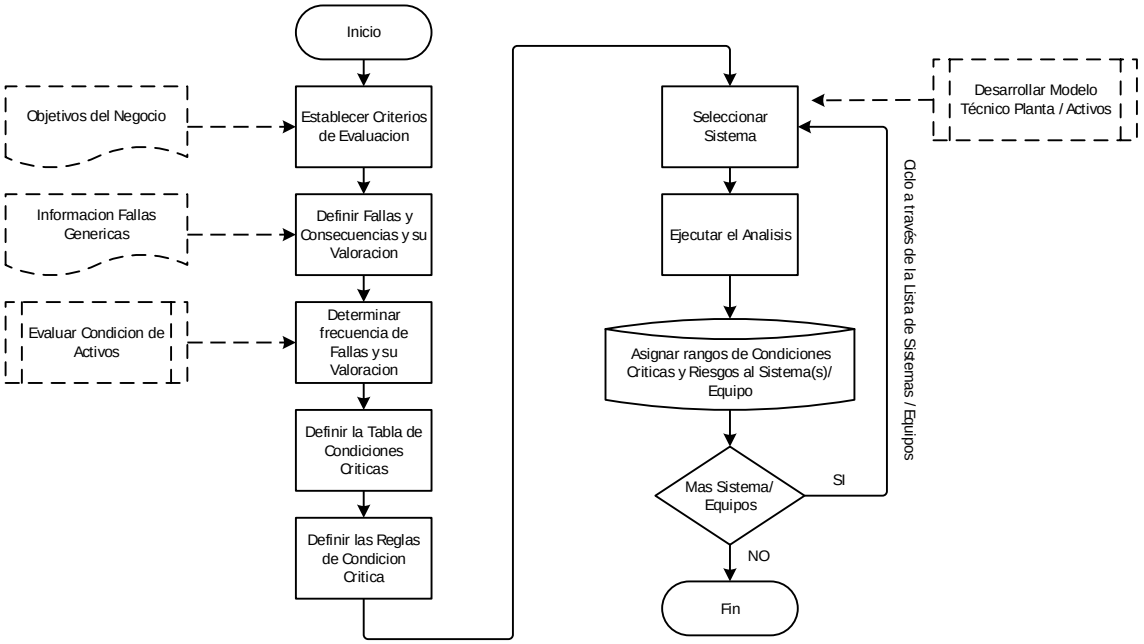

Figura 0.1: Plan de Respuesta a los Incidentes mediante el Análisis de Vulnerabilidad

Fuente y elaboración propia.

Procedimiento para incidentes disruptivos en el centro de datos

Todos los empleados del área de infraestructura tecnológica tendrán la obligación de reportar cualquier incidente generado por posibles riesgos, así mismo estarán obligados a informarlo de la siguiente manera:

- Todos los incidentes generados por posibles riesgos y que estén relacionados con tecnología de la información y de la comunicación dentro del centro de datos será informado vía telefónicamente al jefe de Mesa de Servicios o Área de Infraestructura Tecnológica.

A si mismo cualquier otro evento o vulnerabilidad que atente contra el centro de datos y que todavía no se hubiera convertido en un incidente disruptivo debe ser informado de la misma forma y a la brevedad.

Gestión de incidentes disruptivos en el centro de datos

La persona que recibe la información sobre el incidente deberá evaluar si el incidente, o potencial incidente, es real o falso, y si es real, activara inmediatamente este plan respetando los siguientes pasos:

- Comenzar a controlar y erradicar el incidente de acuerdo con lo detallado en las siguientes secciones del presente documento, ver Tabla N° 4.8

- Informar a todos los empleados del área de infraestructura de TI sobre la ocurrencia del incidente dentro del centro de datos.

- Notificar a jefe de seguridad y salud ocupacional, que debe evaluar si es necesario alertar a alguna de las partes interesadas.

- Controla el estado del incidente y, si es necesario, informa a los demás empleados involucrados, acerca del progreso en la gestión del incidente.

En caso de que la persona no pueda controlar y/o erradicar el incidente, deberá informarlo al gerente de crisis. La información que se envía al gerente de crisis debe incluir la naturaleza y alcance del incidente disruptivo, como también su potencial impacto.

La persona responsable de erradicar el incidente deberá registrar en el registro de incidentes todas las acciones tomadas.

Gerente de crisis

El Gerente de crisis deberá supervisar el progreso en la gestión del incidente y el período de interrupción de las actividades individuales mediante el plan de implementación de análisis de vulnerabilidad y deberá evaluar el tiempo necesario para solucionar el incidente dentro del centro de datos.

En el caso de que el tiempo necesario para solucionar el incidente es mayor que el objetivo de tiempo de recuperación de una actividad particular, se deberá activar el plan de recuperación para la actividad interrumpida, tal como se puede apreciar en la Tabla N° 4.8. En ese caso, el gerente de crisis deberá notificárselo a todos los gerentes de recuperación, quienes activarán sus planes de recuperación.

- El plan de recuperación de actividades en el centro de datos:

El objetivo de este plan de recuperación será definir de forma precisa cómo el banco financiero recuperará las actividades del centro de datos dentro de plazos establecidos ante la presencia de posibles riesgos que puedan ocasionar un desastre significativamente o un incidente disruptivo de severidad alta. A si mismo este plan deberá garantizar la culminación de esta actividad dentro del objetivo de tiempo de recuperación establecido, tal como se puede apreciar en la Tabla N° 4.8

A si mismo este plan propuesto incluirá todos los recursos y procesos necesarios para la recuperación de esta actividad.

Para llevar a cabo este plan es necesario contar con un gabinete de crisis quienes serán los responsables de gestionar, coordinar, controlar y el cumplimiento de la recuperación de las actividades en el centro de datos de la entidad financiera.

Tabla 0:7: Pasos de recuperación para la continuidad de las operaciones

PROCEDIMIENTOS DE RECUPERACIÓN	GABINETE DE CRISIS
1. Reunión del equipo en la ubicación alternativa	
1.1 Verificar si todos los miembros del equipo se encuentran presentes	Auxiliar de recuperación
1.2 Informar a los miembros del equipo del incidente disruptivo ocurrido	Gerente de recuperación
1.3 Dar directrices puntuales necesarias a los miembros del equipo	Coordinador de recuperación
2. Verificación y recuperación de la infraestructura	
2.1 Verificar si se cuenta con la infraestructura necesaria para iniciar la recuperación de la actividad	Supervisor de recuperación
2.2 Levantar un informe de la infraestructura disponible y de la infraestructura faltante necesaria	Supervisor de recuperación
2.3 Instalación de muebles básicos necesarios para iniciar la recuperación	Auxiliar de recuperación
3. Verificación y recuperación de los equipos y vínculos de TIC	
3.1 Verificar si se cuenta con los equipos y vínculos necesarios para iniciar la recuperación de la actividad	Operador de recuperación
3.2 Levantar un informe sobre los equipos faltantes (si los hubiera) y de cuál es la capacidad operativa con los equipos actuales	Operador de recuperación
3.3 Poner operativos los equipos necesarios para iniciar la recuperación de la actividad	Supervisor de recuperación
4. Verificación y recuperación de aplicaciones	
4.1 Verificar si se cuenta con las aplicaciones y los instaladores de estas para iniciar la recuperación de la actividad	Operador de recuperación
4.2 Poner en marcha las aplicaciones necesarias para la recuperación de la actividad	Supervisor de recuperación
4.3 Levantar un informe sobre el funcionamiento de las aplicaciones puestas en marcha y la carga de trabajo que pueden soportar	Supervisor de recuperación
5. Verificación y recuperación de datos y documentos	
5.1 Verificar si se cuenta con los datos y documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación
5.2 Poner a disposición de las personas correspondientes a los datos y los documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación

Fuente y elaboración propia.

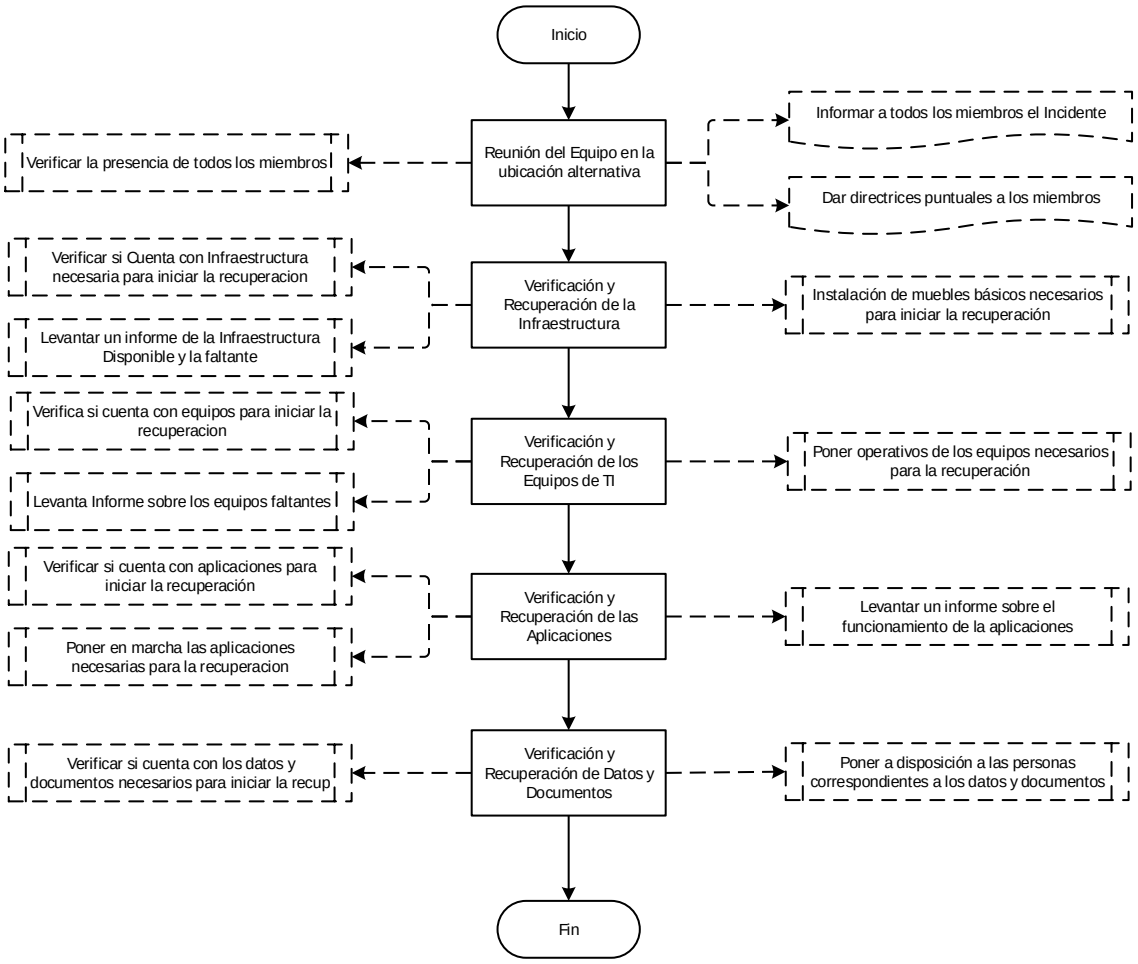

Figura 0.2: Plan de Recuperación de actividades en el Centro de Datos

Fuente y elaboración propia.

Verificar

- ✓ **Plan de prueba y verificación**

El objetivo de este plan es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los arreglos para la gestión de la implementación del análisis de vulnerabilidad, como también para establecer las acciones correctivas necesarias.

Este plan se aplica a todos los elementos que se encuentran dentro del alcance de la implementación del análisis de vulnerabilidad, incluyendo los arreglos con los

proveedores y socios.

Los usuarios de este documento son todos los empleados del área de la infraestructura de TI que cumplen una función en la implementación del análisis de vulnerabilidad.

- **Implementación de pruebas y verificaciones**

La prueba y verificación para la implementación del análisis de vulnerabilidad en el centro de datos del banco financiero será de la siguiente manera:

- ✓ Plazo: se efectuará durante 3 días luego de la implementación del análisis de vulnerabilidad.

- ✓ A si mismo será el gerente de producción y servicios de TI la persona responsable de la coordinación e implementación de la prueba y verificación.

- ✓ A continuación, mencionaremos los objetivos de esta prueba y su verificación:

    - o Se verificará si los planes y recursos son precisos para implementar el análisis de vulnerabilidad.

    - o Se verificará si los empleados del área de infraestructura de TI son responsables de la implementación del análisis de vulnerabilidad están familiarizados con los detalles del plan.
    - o Se verificar la implementación de todos los pasos especificados en los planes.

    - o Se verificará el cumplimento con todas las obligaciones dentro de los plazos predefinidos.

- Se deberá activar procedimientos alternativos en caso de que sea necesario.

- Se deberá asegurar todos los recursos necesarios (incluyendo la recuperación de datos).

- Se deberá lograr la armonización del plan de análisis de vulnerabilidad de otras actividades.

- Se deberá generar comentarios o sugerencias para mejorar el plan.

✓ Para el alcance de la prueba y verificación: Se validará el correcto funcionamiento de los servicios en el centro de datos con respecto a:

- Comunicaciones
- Aplicativos de Core Bancario y Negocios
- Aplicativos Financieros, Administrativos y Tecnológicos

✓ Para la operatividad de los servicios y actividades incluyen también a los proveedores del banco financiero como:

- Level3
- Claro
- IBM
- LENOVO
- Bloomberg
- Cosapi Data
- Electrodata, etc.

- ✓ Método de prueba y verificación:

  - El chequeo de escritorio: este chequeo será aplicado en los planes con técnicas de auditoría, validación y verificación; realizado por el autor del plan y un moderador.
  - El repaso de los planes: este chequeo será aplicado en los planes a través de interacción de equipos; realizada por los principales participantes del plan y por el moderador, cuya interacción se verifica en una reunión conjunta.

  - La simulación: esta verificación se aplicará en todos los planes relacionados con recursos de información reales; realizado por todos los empleados necesarios, proveedores y por el moderador.

  - La prueba funcional: se procederá a reubican las actividades en la ubicación alternativa bajo un ejercicio controlado (anunciado); participan todos los empleados del área de infraestructura de TI necesarios, proveedores, el moderador y observadores.

  - La prueba completa: se trasladan todas las actividades desde la ubicación original a la alternativa (anunciado o no); participan todos los empleados del área de infraestructura de TI necesarios, proveedores, el moderador, observadores y auditores.

- **Revisión de resultados**

El gerente de producción y servicio TI deberá controlar los resultados de las pruebas y deberá preparar un Informe de prueba y verificación.

Este informe deberá incluir las acciones correctivas correspondientes, como también otras recomendaciones de mejora, tal como se puede apreciar en la Tabla N° 4.9

Tabla 0:8: Registros guardados de la revisión de resultados.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Informe de prueba y verificación (en formato electrónico)	Ordenador del Gerente de producción y Servicios TI	Gerente de producción y servicios TI	Solamente el Gerente de producción y Servicios TI puede editar la lista	3 años

Fuente y elaboración propia.

✓ Plan de mantenimiento y revisión en el centro de datos

Para mantener la exactitud y utilidad de todos los elementos de esta implementación del análisis de vulnerabilidad, será necesario revisar y actualizar de acuerdo con las siguientes frecuencias, tal como se puede apreciar en la Tabla N° 4.10

Tabla 0:9: Plan de mantenimiento y revisión en el centro de datos

Elemento del estudio de análisis de vulnerabilidad	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Actualización de software, IOS de equipos de Comunicaciones		X						X				
Limpieza de equipos de Comunicaciones				X						X		
Actualización de software, SO de equipos de Servidores, bases de datos	X						X					
Limpieza de equipos de Servidores, bases de datos			X						X			

Fuente y elaboración propia.

✓ Procedimiento para auditoria interna en el centro de datos

El objetivo de este procedimiento será describir todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Este procedimiento será aplicado a todas las actividades realizadas dentro de la implementación del análisis de vulnerabilidad.

Los usuarios de este documento son los miembros de la alta gerencia del banco financiero y los auditores internos.

- **Objetivo de la auditoría interna en el centro de datos**

  El objetivo de la auditoría interna en el centro de datos será determinar si los procedimientos, controles, procesos, acuerdos y demás actividades en la implementación del análisis de vulnerabilidad concuerdan con las normas ISO 22301, con las regulaciones correspondientes y con la documentación interna de la organización; como también verificar si son implementados y sostenidos y si cumplen requisitos de políticas y establecen objetivos.

- **Planificación de la auditoría interna en el centro de datos**

  Sera el gerente de producción y servicios TI quien aprobara el programa anual de auditorías internas.

  A sí mismo el deberá realizar una o más auditorías internas en el transcurso de un año, asegurando una cobertura acumulativa de todo el alcance en la implementación del análisis de vulnerabilidad. Las auditorías internas son planificadas en base a la evaluación de riesgos, como también por los resultados de auditorías anteriores. Generalmente son realizadas antes de la revisión por parte de la gerencia.

  El programa anual de auditoría interna debe incluir la siguiente información sobre cada auditoría interna individual:

  - El momento de la auditoría: La fecha será establecida previa coordinación y disponibilidad con el área de infraestructura de TI
  - Alcance de la auditoría: Área de Infraestructura TI
  - Criterio de auditoría: Normas ISO 22301.
  - Métodos de la auditoría: Revisión de documentación, entrevistas con empleados del área de infraestructura de TI, revisión de registros, de sistemas informáticos, etc.

- Quién realizará la auditoría: Auditor interno del banco financiero.

A si mismo se deberá llevar un registro de las auditorías realizadas en el Programa anual de auditoría interna.

- **Designación de auditores internos en el centro de datos**

El gerente de riesgos será la persona quien designe a los auditores internos.

Un auditor interno puede ser alguien de la organización o una persona externa a la misma. Los criterios para la designación de los auditores se explican a continuación:

- Que conozca las normas ISO/IEC 22301.
- Que esté familiarizado sobre técnicas de auditoría sobre sistemas de gestión.
- Que sepa cómo funcionan las tecnologías de la información y de la comunicación como para estar familiarizado con el objetivo de los sistemas individuales y también con los impactos sobre procedimientos de seguridad.

También se deberá seleccionar a los auditores internos de tal forma que garanticen la objetividad e imparcialidad; es decir, de evitar el conflicto de intereses, ya que los auditores no pueden auditar su propio trabajo.

Y finalmente se recomienda que los auditores internos realicen un curso para auditores internos según la norma ISO/IEC 22301.

Actuar

- ✓ **Procedimiento para acciones correctivas y preventivas en el centro de datos**

El objetivo de este procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de acciones correctivas y preventivas.

Este procedimiento se aplica a todas las actividades concernientes a la implementación del análisis de vulnerabilidad.

Los usuarios de este documento son todos los empleados del área de infraestructura de TI del banco financiero.

- ✓ **Acciones Correctivas**

  - No conformidad

    Para el caso del estudio las no-conformidad será todo incumplimiento de los requerimientos de las normas, documentación interna, reglamentos, obligaciones contractuales y de otra clase dentro de la implementación del análisis de vulnerabilidad. A si mismo las no-conformidades podrán ser identificadas durante una auditoría interna o externa, en base a resultados de la revisión por parte de la dirección, luego de incidentes, durante el transcurso normal de las operaciones de negocios o en cualquier otra situación.

    Un empleado del área de infraestructura de TI que detecta una no conformidad deberá tomar acciones inmediatamente para controlarla, contenerla y corregirla y para contener sus consecuencias. Si un empleado no es responsable de esa no conformidad debe transmitir la información sobre ella a la persona responsable que pueda corregirla.

  - Acciones correctivas

    La persona responsable deberá evaluar la necesidad de eliminar el origen de la no-conformidad y evitar su recurrencia tomando acciones correctivas.

Una acción correctiva deberá ser iniciada por cualquier empleado del área de infraestructura de TI, cuando sea pertinente, por cualquier cliente, proveedor o socio de la organización. Una acción correctiva podrá demandar cambios sobre cualquier documento, proceso o acuerdo dentro del marco de la implementación del análisis de vulnerabilidad.

- Implementación de acciones correctivas

  Los pasos para la implementación de una acción correctiva se dan a conocer de la siguiente forma tal como se puede apreciar en la Tabla N° 4.11

Tabla 0:10: Pasos para la implementación de una acción correctiva en el centro de datos

Pasos	Persona responsable de la Implementación
1. Revisión de la no-conformidad	Cualquiera con una función en la implementación del análisis de vulnerabilidad
2. Determinación de la causa de la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
3. Identificar si la no-conformidad ya existía	Persona responsable del área donde se ha identificado la no-conformidad
4. Evaluación de la necesidad de tomar acciones para eliminar la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
5. Determinación de las acciones necesarias para eliminar las causas de la no-conformidad y para asegurar que no se produzca nuevamente	Persona responsable del área donde se ha identificado la no-conformidad
6. Implementación de las acciones planificadas	Persona a cargo de la implementación, designada por la persona responsable
7. Revisión para determinar si la acción tomada logró eliminar las causas de la no-conformidad	Subgerente de producción y servicios TI
8. Informar a todas las personas involucradas que se ha implementado la acción correctiva	Persona a cargo de la implementación, designada por la persona responsable

Fuente y elaboración propia.

✓ Acciones Preventivas

El objetivo de la acción preventiva será evitar los efectos no deseados, es decir actividades que estén orientadas a ser eliminadas por ser causa de potenciales de no-conformidades evitando así su ocurrencia.

- Implementación de acciones preventivas

  Las acciones preventivas serán identificadas durante la evaluación de riesgos y el análisis del impacto en el centro de datos generalmente es detallado en el plan de tratamiento del riesgo.

  Las acciones preventivas que no sean atendidas en los documentos mencionados se implementaran de la misma forma que la detallada para las acciones correctivas.

✓ **Gestión de documentos**

El propietario de este documento será el subgerente de producción y servicios TI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, será necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas y preventivas iniciadas

- Cantidad de acciones correctivas y preventivas incompletas

- Cantidad de acciones correctivas y preventivas tomadas sin haber sido registradas en un formulario designado.

4.4 Pruebas de Simulaciones

Con la implementación de la metodología PDCA basada en la norma ISO 22301 para la empresa financiera, se logró fortalecer la capacidad de respuesta, de tal forma que se logró alcanzar a reducir el tiempo total de respuesta que prácticamente eran una amenaza para la continuidad de las operaciones en el centro de datos del banco financiero.

A continuación, se describe a detalle su desarrollo de la siguiente manera:

Planificar

- ✓ **Procedimiento para identificación de requisitos y partes interesadas**

  El objetivo de este documento tendrá como finalidad definir el proceso para identificar las partes involucradas, de los requisitos legales, normativos y de otra índole relacionados con la implementación de pruebas de simulación, como también las responsabilidades para su cumplimiento.

  Los Empleados involucrados en este documento serán los operadores del centro de datos del área de infraestructura tecnológica del banco financiero.

  A sí mismo el oficial de seguridad del área de infraestructura de TI será la persona responsable en identificar a todos los empleados que puedan verse de algún modo afectadas por la gestión en la implementación de las pruebas de simulación y a todos los requisitos legales, normativos, contractuales y de otra índole que correspondan.

  De tal forma el oficial de seguridad de TI será quien definirá al responsable para el cumplimiento de cada requisito individual y que partes interesadas serán notificadas cuando se produzca una modificación.

  También el oficial de seguridad de TI deberá enumerar todos los requisitos, partes interesadas y personas responsables en la "Lista de requisitos legales, normativos, contractuales y de otra índole" y deberá ser publicada en una carpeta con acceso público a los involucrados para su conocimiento

Por otra parte, los operadores del centro de datos del banco financiero deberán notificar al oficial de seguridad de TI si detecta o encuentra algún nuevo requisito legal, normativo, contractual o de otra índole que pueda ser importante para la gestión de implementar las pruebas de simulación.

El oficial de seguridad de TI será la persona responsable de revisar la lista de requisitos legales, normativos, contractuales y de otra índole al menos cada seis meses y de actualizarla cuando sea necesario. El oficial de seguridad TI notificara a todas las partes interesadas cuando realice una actualización, tal como se puede apreciar en la Tabla N° 4.12

El oficial de seguridad TI será el propietario y responsable de este documento, que deberá verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Tabla 0:11: Lista de requisitos legales, normativos, contractuales y de otras índoles

Requisito	Documento que impone el requisito	Persona responsable del cumplimiento	Partes Interesadas
Procedimiento para reducir el tiempo total de respuesta	Normas de la SBS para control de instituciones financieras.	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Acuerdos y niveles de servicios internos y externos.	Plan estratégico vigente en la organización	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Procedimiento de seguridad de la información	Políticas y reglamentos de seguridad de la información y	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Plan de recuperación para el área de TI	Plan estratégico de TI vigente en la organización	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados
Continuidad de los servicios de TI	Plan estratégico operativo anual 2017	Todos los empleados del área de infraestructura de TI del banco financiero	Alta gerencia, órganos de control y regulación, socios, empleados

Fuente y elaboración propia.

- ✓ **Establecer Políticas para definir el alcances y objetivos de la implementación de las pruebas de simulación**

  Las pruebas de simulación tendrán como política definir el objetivo, alcance y reglas básicas para su estudio.

  A si mismo esta política se aplicará en toda la implementación de las pruebas de simulación del banco financiero.

  Por otro lado, los usuarios de estos documentos serán todos los empleados del área de infraestructura tecnológica del banco financiero como también todos los proveedores y socios que cumplen alguna función o forman parte de la implementación de las pruebas de simulación.

  El objetivo de la implementación de las pruebas de simulación será identificar las causas que dan origen a una débil capacidad de respuesta que puedan afectar adversamente el centro de datos de la entidad financiera y los impactos de esas demoras podrían tener sobre las operaciones del negocio; también servirán para proporcionar un marco de referencia para construir resiliencia organizacional con capacidad de una respuesta efectiva.

  A si mismo con la implementación de la prueba de simulación, el banco financiero cumplirá sus objetivos estratégicos y comerciales como son:

  - Brindar un mejor servicio bancario de calidad a los clientes finales.
  - Mantener la disponibilidad de los servicios tecnológicos y de negocio en todo momento.
  - Continuar siendo una empresa financiera de alta rentabilidad.

La gestión para la implementación de las pruebas de simulación se llevará a cabo conforme a los requisitos enumerados en la lista de requisitos legales, normativos, contractuales y de otra índole, y dentro del marco referencial definido por los siguientes documentos:

- Plan estratégico vigente de la organización
- Políticas y reglamentos de seguridad de la información vigente en la organización
- Plan estratégico operativo anual 2017

El gerente de producción y servicios de TI será el responsable de definir los objetivos para la implementación de las pruebas de simulación y el método para medir el cumplimiento de estos. El gerente de producción y servicios de TI tiene la responsabilidad de revisar esos objetivos al menos una vez cada seis meses.

Con respecto al alcance del estudio, las pruebas de simulación se implementarán única y exclusivamente en el centro de datos del banco financiero, con especial atención sobre las actividades identificadas durante el análisis de impactos en el negocio.

- ✓ **Plan de capacitación y concienciación**

Con el objetivo de preparar al personal para que pueda ejecutar sus tareas cumpliendo una función en la gestión de la implementación de las pruebas de simulación, se deberá llevar a cabo la siguiente capacitación, tal como se puede apreciar en la Tabla N° 4.13

Tabla 0:12: Plan de capacitación y concienciación para la prueba de simulación

Cargo o nombre	Conocimientos necesarios para el estudio del análisis de vulnerabilidad	Que capacitaciones es necesaria
Gerente de producción y servicios de TI	✓ Procesos del negocio ✓ Políticas organizacionales ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación ✓ Políticas de seguridad informática	✓ Plan de recuperación ante desastre ✓ Gobierno de TI ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo.
Sub gerente de procesamiento e infraestructura Sub gerente de servicios tecnológicos Sub gerente de control tecnológico	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación ✓ Políticas de seguridad informática	✓ Plan de recuperación ante desastre ✓ Gobierno de TI ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo.
Jefe de comunicaciones	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo avanzado de sistemas y equipos informáticos. ✓ Manejo avanzado de redes. ✓ Configuración de equipos de red.	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Herramientas de monitoreo. ✓ Configuración avanzada de equipos de networking.
Jefe de servidores	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo y configuración avanzada de servidores y bases de datos	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Configuración avanzada de bases de datos y servidores. ✓ Administración y mantenimiento de bases de datos.
Jefe de centro de computo	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo y configuración avanzada de equipos Core, Backups y procesamiento	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Configuración avanzada de equipos Core. ✓ Administración y mantenimiento de equipos Core.
Jefe de soporte técnico	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo avanzado de sistemas operativos y equipos informáticos. ✓ Manejo avanzado de aplicativos.	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Instalación de software y mantenimiento de sistemas informáticos. ✓ Manejo de herramientas de gestión.

Fuente y elaboración propia.

Para que el personal comprenda la importancia de implementar pruebas de simulación, se deberá aplicar los siguientes métodos de concienciación: boletín informativo, articulo en internet, reuniones conjuntas, mensajes de correo electrónico y grabaciones en video informativo, tal como se puede apreciar en la Taba N° 4.14

Tabla 0:13: La implementación de capacitación programada para la prueba de simulación.

Método de concienciación	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio agosto	Agosto	Setiembre	Octubre	Noviembre	diciembre
Boletín informativo	X		X		X		X		X		X	
Artículo en internet		X		X		X		X		X		X
Reuniones conjuntas	X		X		X		X		X		X	
Mensajes electrónicos	X	X	X	X	X	X	X	X	X	X	X	X
Grabaciones en video informativo	X				X				X			X

Fuente y elaboración propia.

Hacer

- ✓ **<u>Metodología para el análisis del impacto en el Centro de Datos</u>**

El objetivo de este documento será definir la metodología y el proceso para evaluar los impactos de la interrupción de las actividades en el centro de datos del banco financiero y determinar prioridades.

Este análisis de impacto en el centro de datos será aplicado en todo el alcance de la implementación de las pruebas de simulación; es decir, a todas las actividades y operaciones que se vean afectadas y amenazadas por eventos inesperados en el centro de datos de la entidad del banco financiero.

Los usuarios de este documento serán los operadores y analista del área de infraestructura tecnológica del banco financiero que participaran en la implementación de las pruebas de simulación.

- **Organización**

  Antes de evaluar el análisis del impacto que se ha generado en el centro de datos primero debemos realizar una evaluación de los riesgos mediante la implementación de las pruebas de simulación| para que la información sobre los recursos necesarios pueda ser utilizada a partir de dicha evaluación.

  A sí mismo el manejo de estos documentos confidenciales producidos de acuerdo con esta metodología se realizará en conformidad con las políticas de seguridad de la información y confidencialidad del banco financiero.

- **Identificación de actividades**

  El coordinador TI de la implementación de las pruebas de simulación será la persona responsable de identificar todas aquellas actividades críticas que tengan un impacto significativo en el Core del negocio, y a si mismo tendrá la labor de designa a las personas responsables para cada actividad.

- **Impactos del incidente disruptivo en el centro de datos**

  El impacto que tendrá un incidente disruptivo sobre una actividad en el centro de datos de la entidad financiera será evaluado a través de la siguiente Tabla N°4.15 según clasificación:

Tabla 0:14: Clasificación de impactos en el centro de datos de la empresa financiera

Consecuencia Insignificante	1	La duración del incidente disruptivo no afecta significativamente las finanzas, las obligaciones legales o el prestigio de la organización.
Consecuencia aceptable	2	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia Critica	3	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o el prestigio de la organización, y ese daño no es aceptable por su magnitud y circunstancias específicas.
Consecuencia Catastrófica	4	La duración del incidente disruptivo provoca grandes daños sobre las finanzas, las obligaciones legales o el prestigio de la organización, que le harán perder la mayor parte de su capital y/o tendrán que cancelar sus operaciones en forma permanente.

Fuente y elaboración propia.

- **Presentación de los resultados**

  La información será recabada mediante los cuestionarios elaborados sobre el análisis del impacto que tendrá el centro de datos y será enviada al coordinador de TI, que tiene la responsabilidad de reunir y documentarla a través de la estrategia de la implementación de las pruebas de simulación.

- **Revisión periódica de análisis del impacto en el negocio**

  El coordinador TI de la implementación del análisis de vulnerabilidad deberá realizar una revisión de los cuestionarios sobre el análisis del impacto en el centro de datos. La revisión se realizará al menos una vez por año, o con mayor frecuencia en caso de cambios organizacionales significativos.

- ✓ **Estrategia para la implementación de las pruebas de simulación**

El objetivo de este documento tiene como finalidad definir como el centro de datos del banco financiero garantizará que se cumpla todas las condiciones para reanudar las actividades y operaciones ante una falta de una capacidad de respuesta la cual podría ocasionar una pérdida significativa en el Core del negocio.

Los usuarios de este documento serán todos los miembros de la alta dirección y personal involucrado en la implementación de las pruebas de simulación.

A si mismo esta estrategia estará redactada en base a los resultados del análisis del impacto en el centro de datos y de la evaluación, y tratamiento de riesgo.

- **Análisis del impacto en el centro de datos**

Para analizar el impacto que tendrá el centro de datos ante un evento de desastre se establecerá una lista de actividades, las cuales serán las que respaldan la provisión de las operaciones y el servicio del centro de datos para el Core del negocio del banco financiero.

Estas actividades se encuentran listadas (no necesariamente en orden de ejecución), de manera que se minimice el tiempo total en la capacidad de respuesta que atenta la continuidad del negocio y el retorno a la normalidad de sus actividades y servicios en el centro de datos del banco financiero, tal como se puede apreciar en la Tabla N° 4.17

Tabla 0:15: Actividades que respaldan la provisión de los servicios

Nombre de la actividad
Estudiar el efecto de cambios internos y externos de los sistemas, al hacer alteraciones en el modelo del sistema y observando los efectos de esas alteraciones en el comportamiento del sistema del centro de datos.
Observar detalladamente que los sistemas que se está simulando puede conducir a un mejor entendimiento del sistema y por consiguiente a sugerir estrategias que mejoren la operación y eficiencia del sistema del centro de datos.
Comprender mejor la operación del sistema, a detectar las variables más importantes que interactúan en los sistemas y a entender mejor las interrelaciones entre estas variables del centro de datos.
Experimentar nuevas situaciones, sobre las cuales tiene poca o ninguna información. A través de estas pruebas de simulación se logrará anticipar mejor a posibles resultados no previstos en el centro de datos.
Anticipar los de cuellos de botellas u otro problema que puede surgir en el comportamiento de los sistemas al incorporar nuevos elementos en el centro de datos.
En una simulación cada variable podrá sostenerse constantemente excepto algunas cuya influencia está siendo estudiada. Como resultado el posible efecto de descontrol de las variables en el comportamiento del sistema necesita no ser tomados en cuenta. Como frecuentemente debe ser hecho cuando el experimento está desarrollado sobre un sistema real.

Fuente y elaboración propia.

- **Gestión de la capacidad de respuesta**

  Para gestionar la capacidad de respuesta se procederá a evaluar aquellas actividades críticas que puedan verse afectados su vulnerabilidad en el centro de datos y para ello se procederá a detallar en la siguiente "Matriz de evaluación de riesgos". Una débil capacidad en respuesta podría producir perdida de continuidad en las operaciones del Core del negocio, es decir, ante una interrupción no atendida a la brevedad en el centro de datos se debería a causa de lo siguiente:

  - La falta de participación en la reducción efectiva del riesgo de desastre.
  - La falta de compromiso de la alta gerencia en la implementación de las pruebas de simulación.
  - La falta de integración de los riesgos de desastre en las actividades de desarrollo.
  - La ausencia de estrategias fundamentales para fortalecer la capacidad

de respuesta ante evento de desastres.

- La falta de centralización de responsabilidades las cuales nos permitiría la reducir el tiempo total en la capacidad de respuesta.
- La falta de alianzas estratégicas con los proveedores ya que estas serían una herramienta para reducir el tiempo de respuesta.

✓ **Plan de implementación de pruebas de simulación**

El objetivo de este plan de implementación de pruebas de simulación será definir de forma precisa cómo el banco financiero gestionará los incidentes en caso de un desastre o de otro incidente disruptivo y cómo recuperará sus actividades en el centro de datos dentro de una capacidad de respuesta efectiva. A si mismo este plan deberá mantener en un nivel aceptable el daño producido por un incidente disruptivo.

Este plan se aplicará a todas las actividades críticas y que estén expuesta a una falta de capacidad de respuesta, y cuyo alcance será el de la implementación de las pruebas de simulación en el centro de datos.

A si mismo los usuarios de este documento son todos los empleados del área de infraestructura tecnológica del banco financiero, tanto internos como externos, que cumplan una función o estén involucrados en la implementación de las pruebas de simulación.

- **Contenido del plan de implementación de pruebas de simulación**

Este plan de implementación de las pruebas de simulación estará formado por dos grandes secciones:

- El plan de respuesta a los incidentes:

El objetivo de este plan será asegurar la protección de la información y de la seguridad en el centro de datos de la entidad financiera ante el caso de un desastre o de otro incidente, como también contener el incidente. A si mismo se lograra reducir al mínimo el tiempo total en la capacidad de respuesta sobre el centro de datos de la empresa financiera.

Este plan se aplicará a todos los incidentes de severidad alta que amenazan con interrumpir cualquier actividad crítica dentro del centro de datos, por un período mayor al objetivo de tiempo de recuperación de cada actividad individual, tal como se puede apreciar en la Tabla N° 4.18

Tabla 0:16: Los usuarios de este documento son los empleados de TI del banco financiero.

Cargo	Autorizaciones y responsabilidades
Empleados del Área de Infraestructura Tecnológica	Formular el problema: En este paso debe quedar perfectamente establecido el objeto de la simulación.
Empleados del Área de Infraestructura Tecnológica	Definir el sistema: El sistema a simular debe estar perfectamente definido
Empleados del Área de Infraestructura Tecnológica	Formular el modelo: Esta etapa es un arte y será discutida más adelante
Empleados del Área de Infraestructura Tecnológica	Coleccionar datos: La naturaleza y cantidad de datos necesarios están determinadas por la formulación del problema y del modelo
Empleados del Área de Infraestructura Tecnológica	Implementar el modelo en la computadora: El modelo es implementado utilizando algún lenguaje de computación.
Empleados del Área de Infraestructura Tecnológica	Verificar: En esta etapa se comprueba que no se hayan cometidos errores durante la implementación del modelo
Empleados del Área de Infraestructura Tecnológica	Validar: En esta etapa se comprueba la exactitud del modelo desarrollado.
Empleados del Área de Infraestructura Tecnológica	Diseñar experimentos: En esta etapa se decide las características de los experimentos a realizar: el tiempo de arranque, el tiempo de simulación y el número de simulaciones.
Empleados del Área de Infraestructura Tecnológica	Experimentar: En esta etapa se realizan las simulaciones de acuerdo el diseño previo.
Empleados del Área de Infraestructura Tecnológica	Interpretar: Se analiza la sensibilidad del modelo con respecto a los parámetros que tienen asociados la mayor incertidumbre.
Empleados del Área de Infraestructura Tecnológica	Implementar: Conviene acompañar al cliente en la etapa de implementación para evitar el mal manejo del simulador o el mal empleo de los resultados de este.
Empleados del Área de Infraestructura Tecnológica	Documentar: Incluye la elaboración de la documentación técnica y manuales de uso.

Fuente y elaboración propia.

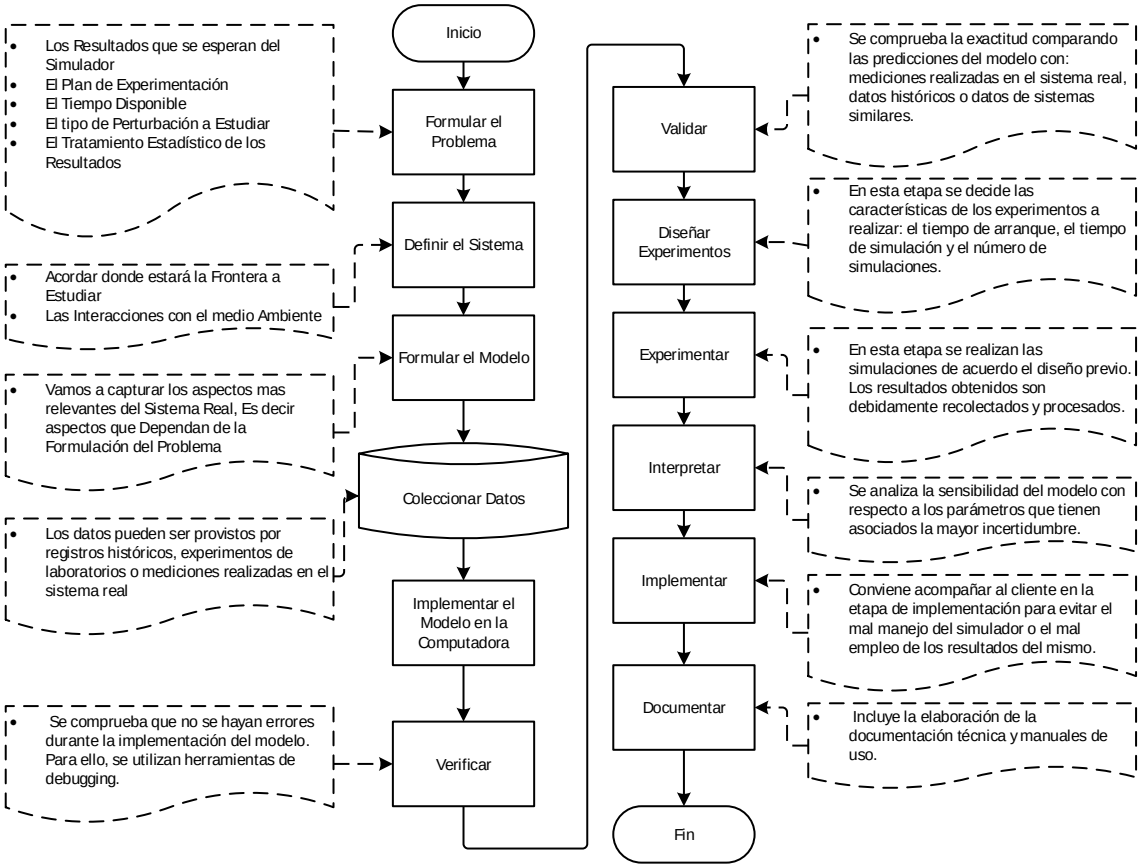

Figura 0.3: Plan de Respuesta a los Incidentes mediante pruebas de simulación

Fuente y elaboración propia.

Procedimiento para incidentes disruptivos en el centro de datos

Todos los empleados del área de infraestructura tecnológica tendrán la obligación de reportar cualquier incidente, así mismo estarán obligados a informar cualquier incidente disruptivo de la siguiente manera:

- Todos los incidentes relacionados con tecnología de la información y de la comunicación dentro del centro de datos será informado telefónicamente al jefe de Mesa de Servicios o Área de Infraestructura Tecnológica.

A si mismo cualquier otro evento o vulnerabilidad que atente contra el centro de datos y que todavía no se hubiera convertido en un incidente

disruptivo debe ser informado de la misma forma y a la brevedad.

Gestión de incidentes disruptivos en el centro de datos

La persona que recibe la información sobre el incidente deberá evaluar si el incidente, o potencial incidente, es real o falso, y si es real, activara inmediatamente este plan respetando los siguientes pasos:

- Comenzar a controlar y erradicar el incidente de acuerdo con lo detallado en las siguientes secciones del presente documento, ver Tabla N° 4.19

- Informar a todas las personas responsables sobre la ocurrencia del incidente dentro de su área de responsabilidad.

- Notificar a jefe de seguridad y salud ocupacional, que debe evaluar si es necesario alertar a alguna de las partes interesadas.

- Controla el estado del incidente y, si es necesario, informa a los demás empleados involucrados, acerca del progreso en la gestión del incidente.

En caso de que la persona no pueda controlar y/o erradicar el incidente, deberá informarlo al gerente de crisis. La información que se envía al gerente de crisis debe incluir la naturaleza y alcance del incidente disruptivo, como también su potencial impacto.

La persona responsable de erradicar el incidente deberá registrar en el registro de incidentes todas las acciones tomadas.

Gerente de crisis

El Gerente de crisis deberá supervisar el progreso en la gestión del incidente y el período de interrupción de las actividades individuales mediante el plan de implementación de las pruebas de simulación y deberá evaluar el tiempo estimado para solucionar el incidente dentro del centro de datos.

En el caso de que el tiempo necesario para solucionar el incidente es mayor que el objetivo de tiempo de recuperación de una actividad particular, se deberá activar el plan de recuperación para la actividad interrumpida, tal como se puede apreciar en la Tabla N° 4.19. En ese caso, el gerente de crisis deberá notificárselo a todos los gerentes de recuperación, quienes activarán sus planes de recuperación.

- El plan de recuperación de actividades en el centro de datos:

  El objetivo de este plan de recuperación será definir de forma precisa cómo el banco financiero recuperará sus actividades dentro de plazos establecidos ante el caso de un desastre o de un incidente disruptivo. A si mismo este plan de recuperación deberá garantizar la culminación de esta actividad dentro del objetivo de tiempo y capacidad de recuperación establecido, tal como se puede apreciar en la Tabla N° 4.19

  Este plan propuesto incluye todos los recursos y procesos necesarios para la recuperación de esta actividad.

  Para llevar a cabo este plan de recuperación es necesario contar con un gabinete de crisis quienes serán los responsables de gestionar, coordinar, controlar y el cumplimiento de la recuperación de las actividades en el centro de datos de la entidad financiera.

Tabla 0:17: Pasos de recuperación para la disponibilidad de los servicios

PROCEDIMIENTOS DE RECUPERACIÓN	GABINETE DE CRISIS
1. Reunión del equipo en la ubicación alternativa	
1.1 Verificar si todos los miembros del equipo se encuentran presentes	Auxiliar de recuperación
1.2 Informar a los miembros del equipo del incidente disruptivo ocurrido	Gerente de recuperación
1.3 Dar directrices puntuales necesarias a los miembros del equipo	Coordinador de recuperación
2. Verificación y recuperación de la infraestructura	
2.1 Verificar si se cuenta con la infraestructura necesaria para iniciar la recuperación de la actividad	Supervisor de recuperación
2.2 Levantar un informe de la infraestructura disponible y de la infraestructura faltante necesaria	Supervisor de recuperación
2.3 Instalación de muebles básicos necesarios para iniciar la recuperación	Auxiliar de recuperación
3. Verificación y recuperación de los equipos y vínculos de TIC	
3.1 Verificar si se cuenta con los equipos y vínculos necesarios para iniciar la recuperación de la actividad	Operador de recuperación
3.2 Levantar un informe sobre los equipos faltantes (si los hubiera) y de cuál es la capacidad operativa con los equipos actuales	Operador de recuperación
3.3 Poner operativos los equipos necesarios para iniciar la recuperación de la actividad	Supervisor de recuperación
4. Verificación y recuperación de aplicaciones	
4.1 Verificar si se cuenta con las aplicaciones y los instaladores de estas para iniciar la recuperación de la actividad	Operador de recuperación
4.2 Poner en marcha las aplicaciones necesarias para la recuperación de la actividad	Supervisor de recuperación
4.3 Levantar un informe sobre el funcionamiento de las aplicaciones puestas en marcha y la carga de trabajo que pueden soportar	Supervisor de recuperación
5. Verificación y recuperación de datos y documentos	
5.1 Verificar si se cuenta con los datos y documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación
5.2 Poner a disposición de las personas correspondientes los datos y los documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación

Fuente y elaboración propia.

Verificar

- ✓ **Plan de prueba y verificación**

El objetivo de este plan es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los arreglos para la gestión de la implementación de las pruebas de simulación, como también para establecer las acciones correctivas necesarias.

Este plan se aplica a todos los elementos que se encuentran dentro del alcance de la implementación de las pruebas de simulación, incluyendo los arreglos con los proveedores y socios.

Los usuarios de este documento son todos los empleados del área de la infraestructura de TI que cumplen una función en la implementación de las pruebas de simulación.

- **Implementación de pruebas y verificaciones**

La prueba y verificación para la implementación de las pruebas de simulación en el centro de datos del banco financiero será de la siguiente manera:

- ✓ Plazo: se efectuará durante 3 días luego de la implementación de las pruebas de simulación.

- ✓ A si mismo será el gerente de producción y servicios de TI la persona responsable de la coordinación e implementación de la prueba y verificación.

- ✓ A continuación, mencionaremos los objetivos de esta prueba y su verificación:

- Se verificará si los planes y recursos son precisos para implementar las pruebas de simulación.

- Se verificará si los empleados del área de infraestructura de TI son responsables de la implementación de las pruebas de simulación están familiarizados con los detalles del plan.

- Se verificará la implementación de todos los pasos especificados en los planes.

- Se verificará el cumplimento con todas las obligaciones dentro de los plazos predefinidos.

- Se deberá activar procedimientos alternativos en caso de que sea necesario.

- Se deberá asegurar todos los recursos necesarios (incluyendo la recuperación de datos).

- Se deberá lograr la armonización del plan de pruebas de simulación de otras actividades.

- Se deberá generar comentarios o sugerencias para mejorar el plan.

✓ Para el alcance de la prueba y verificación: Se validará el correcto funcionamiento de los servicios en el centro de datos con respecto a:

- Comunicaciones
- Aplicativos de Core Bancario y Negocios
- Aplicativos Financieros, Administrativos y Tecnológicos

✓ Para la operatividad de los servicios y actividades incluyen también a los proveedores del banco financiero como:

- Level3
- Claro
- Luz del sur
- IBM
- SONDA
- Bloomberg
- Electrodata, etc.

✓ Método de prueba y verificación:

- El chequeo de escritorio: este chequeo será aplicado en los planes con técnicas de auditoría, validación y verificación; realizado por el autor del plan y un moderador.

- El repaso de los planes: este chequeo será aplicado en los planes a través de interacción de equipos; realizada por los principales participantes del plan y por el moderador, cuya interacción se verifica en una reunión conjunta.

- La simulación: esta verificación se aplicará en todos los planes relacionados con recursos de información reales; realizado por todos los empleados necesarios, proveedores y por el moderador.

- La prueba funcional: se procederá a reubican las actividades en la ubicación alternativa bajo un ejercicio controlado (anunciado); participan todos los empleados del área de infraestructura de TI necesarios, proveedores, el moderador y observadores.

- La prueba completa: se trasladan todas las actividades desde la ubicación original a la alternativa (anunciado o no); participan todos los empleados del área de infraestructura de TI necesarios, proveedores, el moderador, observadores y auditores.

- **Revisión de resultados**

El gerente de producción y servicio TI deberá controlar los resultados de las pruebas y deberá preparar un Informe de prueba y verificación.

Este informe deberá incluir las acciones correctivas correspondientes, como también otras recomendaciones de mejora, tal como se puede apreciar en la Tabla N° 4.20

Tabla 0:18: Registros guardados de la revisión de resultados.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Informe de prueba y verificación (en formato electrónico)	Ordenador del Gerente de producción y Servicios TI	Gerente de producción y servicios TI	Solamente el Gerente de producción y Servicios TI puede editar la lista	3 años

Fuente y elaboración propia.

✓ **<u>Plan de mantenimiento y revisión en el centro de datos</u>**

Para mantener la exactitud y utilidad de todos los elementos de esta implementación de las pruebas de simulación, será necesario revisar y actualizar de acuerdo con las siguientes frecuencias, tal como se puede apreciar en la Tabla N° 4.21

Tabla 0:19: Plan de mantenimiento y revisión en el centro de datos

Elemento del estudio de pruebas de simulación	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Estudiar el efecto de cambios internos y externos de los sistemas		X						X				
Detectar las variables más importantes que interactúan en los sistemas				X						X		
Experimentar nuevas situaciones, sobre las cuales tiene poca o ninguna información.	X						X					
Anticipar los de cuellos de botellas u otro problema que puede surgir en el comportamiento de los sistemas al incorporar nuevos elementos en el centro de datos.			X						X			

Fuente y elaboración propia.

- ✓ **Procedimiento para auditoria interna en el centro de datos**

El objetivo de este procedimiento será describir todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Este procedimiento será aplicado a todas las actividades realizadas dentro de la implementación de las pruebas de simulación.

Los usuarios de este documento son los miembros de la alta gerencia del banco financiero y los auditores internos.

- **Objetivo de la auditoría interna en el centro de datos**

  El objetivo de la auditoría interna en el centro de datos será determinar si los procedimientos, controles, procesos, acuerdos y demás actividades en la implementación de las pruebas de simulación concuerdan con las normas ISO 22301, con las regulaciones correspondientes y con la documentación interna de la organización; como también verificar si son implementados y sostenidos y si cumplen requisitos de políticas y establecen objetivos.

- **Planificación de la auditoría interna en el centro de datos**

  Sera el gerente de producción y servicios TI quien aprobara el programa anual de auditorías internas.

  A sí mismo el deberá realizar una o más auditorías internas en el transcurso de un año, asegurando una cobertura acumulativa de todo el alcance en la implementación de las pruebas de simulación. Las auditorías internas son planificadas en base a la evaluación de riesgos, como también por los resultados de auditorías anteriores. Generalmente son realizadas antes de la revisión por parte de la gerencia.

El programa anual de auditoría interna debe incluir la siguiente información sobre cada auditoría interna individual:

- El momento de la auditoría: La fecha será establecida previa coordinación y disponibilidad con el área de infraestructura de TI
- Alcance de la auditoría: Área de Infraestructura TI
- Criterio de auditoría: Normas ISO 22301.
- Métodos de la auditoría: Revisión de documentación, entrevistas con empleados del área de infraestructura de TI, revisión de registros, de sistemas informáticos, etc.
- Quién realizará la auditoría: Auditor interno del banco financiero.

A si mismo se deberá llevar un registro de las auditorías realizadas en el Programa anual de auditoría interna.

- **<u>Designación de auditores internos en el centro de datos</u>**

  El gerente de riesgos será la persona quien designe a los auditores internos.

  Un auditor interno puede ser alguien de la organización o una persona externa a la misma. Los criterios para la designación de los auditores se explican a continuación:

  - Que conozca las normas ISO/IEC 22301.
  - Que esté familiarizado sobre técnicas de auditoría sobre sistemas de gestión.
  - Que sepa cómo funcionan las tecnologías de la información y de la comunicación como para estar familiarizado con el objetivo de los sistemas individuales y también con los impactos sobre procedimientos de seguridad.

También se deberá seleccionar a los auditores internos de tal forma que garanticen la objetividad e imparcialidad; es decir, de evitar el conflicto de intereses, ya que los auditores no pueden auditar su propio trabajo.

Y finalmente se recomienda que los auditores internos realicen un curso para auditores internos según la norma ISO/IEC 22301.

Actuar

- ✓ **Procedimiento para acciones correctivas y preventivas en el centro de datos**

El objetivo de este procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de acciones correctivas y preventivas.

Este procedimiento se aplica a todas las actividades concernientes a la implementación de las pruebas de simulación.

Los usuarios de este documento son todos los empleados del área de infraestructura de TI del banco financiero.

- ✓ **Acciones Correctivas**

  - No conformidad

    Para el caso del estudio las no-conformidad será todo incumplimiento de los requerimientos de las normas, documentación interna, reglamentos, obligaciones contractuales y de otra clase dentro de la implementación de las pruebas de simulación. A si mismo las no-conformidades podrán ser identificadas durante una auditoría interna o externa, en base a resultados de la revisión por parte de la dirección, luego de incidentes, durante el transcurso normal de las operaciones de negocios o en cualquier otra situación.

Un empleado del área de infraestructura de TI que detecta una no conformidad deberá tomar acciones inmediatamente para controlarla, contenerla y corregirla y para contener sus consecuencias. Si un empleado no es responsable de esa no conformidad debe transmitir la información sobre ella a la persona responsable que pueda corregirla.

- Acciones correctivas

  La persona responsable deberá evaluar la necesidad de eliminar el origen de la no-conformidad y evitar su recurrencia tomando acciones correctivas.

  Una acción correctiva deberá ser iniciada por cualquier empleado del área de infraestructura de TI, cuando sea pertinente, por cualquier cliente, proveedor o socio de la organización. Una acción correctiva podrá demandar cambios sobre cualquier documento, proceso o acuerdo dentro del marco de la implementación de las pruebas de simulación.

- Implementación de acciones correctivas

  Los pasos para la implementación de una acción correctiva se dan a conocer de la siguiente forma tal como se puede apreciar en la Tabla N° 4.22

Tabla 0:20: Pasos para la implementación de una acción correctiva en el centro de datos

Pasos	Persona responsable de la Implementación
1. Revisión de la no-conformidad	Cualquiera con una función en la implementación del análisis de vulnerabilidad
2. Determinación de la causa de la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
3. Identificar si la no-conformidad ya existía	Persona responsable del área donde se ha identificado la no-conformidad
4. Evaluación de la necesidad de tomar acciones para eliminar la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
5. Determinación de las acciones necesarias para eliminar las causas de la no-conformidad y para asegurar que no se produzca nuevamente	Persona responsable del área donde se ha identificado la no-conformidad

6. Implementación de las acciones planificadas	Persona a cargo de la implementación, designada por la persona responsable
7. Revisión para determinar si la acción tomada logró eliminar las causas de la no-conformidad	Subgerente de producción y servicios TI
8. Informar a todas las personas involucradas que se ha implementado la acción correctiva	Persona a cargo de la implementación, designada por la persona responsable

Fuente y elaboración propia.

- ✓ **Acciones Preventivas**

El objetivo de la acción preventiva será evitar los efectos no deseados, es decir actividades que estén orientadas a ser eliminadas por ser causa de potenciales de no-conformidades evitando así su ocurrencia.

- Implementación de acciones preventivas

  Las acciones preventivas serán identificadas durante la evaluación de riesgos y el análisis del impacto en el centro de datos generalmente es detallado en el plan de tratamiento del riesgo.

  Las acciones preventivas que no sean atendidas en los documentos mencionados se implementaran de la misma forma que la detallada para las acciones correctivas.

- ✓ **Gestión de documentos**

El propietario de este documento será el subgerente de producción y servicios TI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, será necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas y preventivas iniciadas

- Cantidad de acciones correctivas y preventivas incompletas

- Cantidad de acciones correctivas y preventivas tomadas sin haber sido registradas en un formulario designado.

4.5 Planes de Respaldo

Con la implementación de la metodología PDCA basada en la norma ISO 22301 para la empresa financiera, se logró optimizar la restauración de la información, de tal forma que se logró alcanzar a reducir el tiempo total en la restauración de la información que prácticamente eran una amenaza para la continuidad de las operaciones en el banco financiero.

A continuación, se describe a detalle su desarrollo de la siguiente manera:

Planificar

- ✓ **Procedimiento para identificación de requisitos y partes interesadas**

  El objetivo de este documento tendrá como finalidad definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos y de otra índole relacionados con la implementación del plan de respaldo, como también las personas responsables para su cumplimiento.

  Por otro lado, los usuarios involucrados en este documento serán todos los empleados del área de infraestructura tecnológica del banco financiero.

  A sí mismo el oficial de seguridad de TI será el responsable de identificar todas las personas que puedan verse afectadas por la gestión en la implementación del plan de respaldo y a todos los requisitos legales, normativos, contractuales y de otra índole que correspondan.

  El oficial de seguridad de TI del banco financiero será quien definirá el responsable del cumplimiento de cada requisito individual y que partes interesadas serán notificadas cuando se produzca una modificación.

También el oficial de seguridad de TI del banco financiero deberá enumerar todos los requisitos, partes interesadas y personas responsables en la "Lista de requisitos legales, normativos, contractuales y de otra índole" y debe ser publicada en una carpeta con acceso público a los involucrados para su conocimiento

Por otra parte, el empleado del área de infraestructura tecnológica del banco financiero deberá notificar al oficial de seguridad de TI si detecta o encuentra algún nuevo requisito legal, normativo, contractual o de otra índole que pueda ser importante para la gestión de implementar los planes de respaldo.

El oficial de seguridad de TI será la persona responsable de revisar la lista de requisitos legales, normativos, contractuales y de otra índole al menos cada seis meses y de actualizarla cuando sea necesario. El oficial de seguridad TI notificara a todas las partes interesadas cuando realice una actualización, tal como se puede apreciar en la Tabla N° 4.23

El oficial de seguridad TI será el propietario y responsable de este documento, que deberá verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Tabla 0:21: Lista de requisitos legales, normativos, contractuales y de otras índoles

Requisito	Documento que impone el requisito	Persona responsable del cumplimiento	Plazos	Partes Interesadas
Procedimiento para reducir el tiempo total de restauración de la información.	Normas de la SBS para control de instituciones financieras.	Todos los empleados del área de infraestructura de TI del banco	Continuo	Alta gerencia, órganos de control y regulación, socios, empleados
Acuerdos y niveles de servicios internos y externos.	Plan estratégico vigente en la organización	Todos los empleados del área de infraestructura de	Continuo	Alta gerencia, órganos de control y regulación, socios,

Procedimiento de seguridad de la información	Políticas y reglamentos de seguridad de la información y	Todos los empleados del área de infraestructura de	3 años	Alta gerencia, órganos de control y regulación, socios,
Plan de recuperación para el área de TI	Plan estratégico de TI vigente en la organización	Todos los empleados del área de infraestructura de	3 años	Alta gerencia, órganos de control y regulación, socios,
Continuidad de los servicios de TI	Plan estratégico operativo anual 2017	Todos los empleados del área de infraestructura de	1 año	Alta gerencia, órganos de control y regulación, socios,

Fuente y elaboración propia.

- ✓ **Políticas, alcances y objetivos de la implementación del plan de respaldo**

El plan de respaldo tendrá como política definir el objetivo, alcance y reglas básicas para su estudio.

A si mismo esta política se aplicará en todo el plan de respaldo del banco financiero.

Por otro lado, los usuarios de estos documentos serán todos los empleados del área de infraestructura tecnológica del banco financiero como también todos los proveedores y socios que cumplen alguna función o forman parte de la implementación del plan de respaldo.

El objetivo de la implementación del plan de respaldo será identificar las causas que dan origen a una mala restauración de la información que puedan afectar adversamente el centro de datos de la entidad financiera y los impactos de esas demoras que podrían tener sobre las operaciones o actividades del Core del negocio; también servirán para proporcionar un marco de referencia para construir resiliencia organizacional con capacidad de una respuesta efectiva.

A si mismo con la implementación del plan de respaldo, el banco financiero cumplirá sus objetivos estratégicos y comerciales como son:

- Brindar un mejor servicio bancario de calidad a los clientes finales.

- Mantener la disponibilidad de los servicios tecnológicos y de negocio en todo momento.
- Continuar siendo una empresa financiera de alta rentabilidad.

La gestión para la implementación del plan de respaldo se llevará a cabo conforme a los requisitos enumerados en la lista de requisitos legales, normativos, contractuales y de otra índole, y dentro del marco referencial definido por los siguientes documentos:

- Plan estratégico vigente de la organización
- Políticas y reglamentos de seguridad de la información vigente en la organización
- Plan estratégico operativo anual 2017

El gerente de producción y servicios de TI será el responsable de definir los objetivos para la implementación del plan de respaldo y el método para medir el cumplimiento de estos. El gerente de producción y servicios de TI tiene la responsabilidad de revisar esos objetivos al menos una vez cada seis meses.

Con respecto al alcance del estudio, el plan de respaldo se implementará única y exclusivamente en el centro de datos del banco financiero, con especial atención sobre las actividades identificadas durante el análisis de impactos en el negocio.

- ✓ **Plan de capacitación y concienciación**

Con el objetivo de preparar al personal para que pueda ejecutar sus tareas cumpliendo una función en la gestión de la implementación del plan de respaldo, se deberá llevar a cabo la siguiente capacitación, tal como se puede apreciar en la Tabla N° 4.24

Tabla 0:22: Plan de capacitación y concienciación para el plan de respaldo

Cargo o nombre	Conocimientos necesarios para las pruebas de simulación	Que capacitaciones es necesaria
Gerente de producción y servicios de TI	✓ Procesos del negocio ✓ Políticas organizacionales ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación ✓ Políticas de seguridad informática	✓ Plan de recuperación ante desastre ✓ Gobierno de TI ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo.
Sub gerente de procesamiento e infraestructura Sub gerente de servicios tecnológicos Sub gerente de control tecnológico	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación ✓ Políticas de seguridad informática	✓ Plan de recuperación ante desastre ✓ Gobierno de TI ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo.
Jefe de comunicaciones	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo avanzado de sistemas y equipos informáticos. ✓ Manejo avanzado de redes. ✓ Configuración de equipos de red.	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Herramientas de monitoreo. ✓ Configuración avanzada de equipos de networking.
Jefe de servidores	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo y configuración avanzada de servidores y bases de datos	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Configuración avanzada de bases de datos y servidores. ✓ Administración y mantenimiento de bases de datos.
Jefe de centro de computo	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo y configuración avanzada de equipos Core, Backups y procesamiento	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Configuración avanzada de equipos Core. ✓ Administración y mantenimiento de equipos Core.
Jefe de soporte técnico	✓ Procesos del negocio ✓ Normas de control y regulación ✓ Manejo de gestión de recuperación. ✓ Manejo avanzado de sistemas operativos y equipos informáticos. ✓ Manejo avanzado de aplicativos.	✓ Plan de recuperación ante desastre ✓ Regulación y normas de la SBS ✓ Técnicas de trabajo en equipo y liderazgo. ✓ Instalación de software y mantenimiento de sistemas informáticos. ✓ Manejo de herramientas de gestión.

Fuente y elaboración propia.

Para que los empleados del área de infraestructura de TI comprendan la importancia de implementar estos planes de respaldo, se deberá aplicar los siguientes métodos de concienciación: boletín informativo, articulo en internet, reuniones conjuntas, mensajes de correo electrónico y grabaciones en video informativo, tal como se puede apreciar en la Taba N° 4.25

Tabla 0:23: Capacitación programada para el plan de respaldo

Método de conciencia ción	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio agosto	Agosto	Setiembre	Octubre	Noviembre	diciembre
Boletín informativo	X		X		X		X		X		X	
Artículo en internet		X		X		X		X		X		X
Reuniones conjuntas	X		X		X		X		X		X	
Mensajes electrónicos	X	X	X	X	X	X	X	X	X	X	X	X
Grabaciones en video informativo	X				X				X			X

Fuente y elaboración propia.

Hacer

- ✓ **<u>Metodología para el análisis del impacto en el Centro de Datos</u>**

El objetivo de este documento será definir la metodología y el proceso para evaluar el impacto provocado generado por una mala restauración de información en las actividades del centro de datos del banco financiero y determinar prioridades.

Este análisis de impacto en el centro de datos será aplicado en todo el alcance de la implementación del plan de respaldo; es decir, a todas las actividades que se vean afectadas y amenazadas por una mala restauración de la información en el centro de datos de la entidad del banco financiero.

Los usuarios de este documento son todos los empleados del área de infraestructura tecnológica del banco financiero que participaran en la implementación del plan de respaldo.

- **Organización**

  El análisis de impacto en el centro de datos se realizará una vez finalizada la evaluación de una mala restauración de la información ante un evento inesperado para que información sobre los recursos necesarios pueda ser utilizada a partir de dicha evaluación.

  A sí mismo el manejo de estos documentos confidenciales producidos de acuerdo con esta metodología se realizará en conformidad con las políticas de seguridad de la información y confidencialidad del banco financiero.

- **Identificación de actividades**

  El coordinador TI de la implementación del plan de respaldo será la persona responsable de identificar todas las actividades críticas que tengan un impacto significativo en el Core del negocio, y a si mismo deberá designar el personal responsable para cada actividad.

- **Impactos del incidente disruptivo en el centro de datos**

  El impacto que tendrá el incidente disruptivo sobre una actividad en el centro de datos de la entidad financiera será evaluado a través de la siguiente Tabla N°4.26 según clasificación:

Tabla 0:24: Clasificación de impactos en el centro de datos de la empresa financiera

Consecuencia Insignificante	1	La duración del incidente disruptivo no afecta significativamente las finanzas, las obligaciones legales o el prestigio de la organización.
Consecuencia aceptable	2	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia Critica	3	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o el prestigio de la organización, y ese daño no es aceptable por su magnitud y circunstancias específicas.
Consecuencia Catastrófica	4	La duración del incidente disruptivo provoca grandes daños sobre las finanzas, las obligaciones legales o el prestigio de la organización, que le harán perder la mayor parte de su capital y/o tendrán que cancelar sus operaciones en forma permanente.

Fuente y elaboración propia.

- **Presentación de los resultados**

  La información será recabada mediante los cuestionarios elaborados sobre el análisis del impacto que tendrá el centro de datos y será enviada al coordinador de TI, que tiene la responsabilidad de reunir y documentarla a través de la estrategia de la implementación del plan de respaldo.

- **Revisión periódica de análisis del impacto en el negocio**

  El coordinador TI de la implementación del plan de respaldo deberá realizar una revisión de los cuestionarios sobre el análisis del impacto en el centro de datos. Esta revisión se realizará al menos una vez por año, o con mayor frecuencia en caso de cambios organizacionales significativos.

✓ **Estrategia para la implementación del plan de respaldo**

Este documento tiene como objetivo definir como el banco financiero garantizará que se cumpla todas las condiciones para reanudar las operaciones y actividades en el centro de datos ante la presencia de una mala

restauración de información que podrían tener un impacto muy significativo en el Core del negocio de la entidad financiera.

A si mismo este documento se aplicará a todo el alcance de la implantación del plan de respaldo, según se define en la política de la implementación de los planes de respaldo.

Los usuarios de este documento serán todos los miembros de la alta dirección y personal involucrado en la implementación del plan de respaldo.

A si mismo esta estrategia estará redactada en base a los resultados del análisis del impacto en el centro de datos y de la evaluación, y tratamiento de riesgo.

- **Análisis del impacto en el centro de datos**

Para analizar el impacto que tendrá el centro de datos ante una mala restauración de información se establecerá una lista de actividades, las cuales serán las que respaldan la provisión de las operaciones y el servicio del centro de datos para el Core del negocio del banco financiero.

Estas actividades se encuentran listadas (no necesariamente en orden de ejecución), de manera que se minimice el tiempo total en la capacidad de respuesta que atenta la continuidad del negocio y el retorno a la normalidad de sus actividades en el centro de datos del banco financiero, tal como se puede apreciar en la Tabla N° 4.28

Tabla 0:25: Actividades que respaldan la provisión de servicios

Nombre de la actividad
¿A qué medio enviará la copia de seguridad (cinta o disco)?
¿Realizará copias de seguridad manualmente o las programará para que se realicen automáticamente?
Si se automatizan las copias de seguridad, ¿de qué forma comprobará que se han realizado correctamente?
¿De qué forma comprobará que las copias de seguridad se pueden usar?
¿Durante cuánto tiempo guardará las copias de seguridad antes de volver a usar el medio?
Supongamos que se produce un error, ¿cuánto tiempo tardará la restauración a partir de la copia de seguridad más reciente? ¿Es aceptable ese tiempo de inactividad?
¿Dónde almacenará las copias de seguridad? ¿Tendrán las personas adecuadas acceso a esas copias?
Si el administrador del sistema responsable no está disponible, ¿hay alguien más que sepa las contraseñas y procedimientos adecuados para realizar las copias de seguridad y restaurar el sistema si fuera necesario?

Fuente y elaboración propia.

- **Gestión de la restauración de la información**

  Para gestionar el plan de respaldo se procederá a evaluar aquellas actividades críticas que puedan verse afectados su vulnerabilidad en el centro de datos y para ello se procederá a detallar en la siguiente "Matriz de evaluación de riesgos". Una mala restauración de la información podría producir perdida en la continuidad de las operaciones en Core del negocio, es decir, una interrupción no atendida a la brevedad en el centro de datos se debería a causa de lo siguiente:

  - La falta de un inventario completo de todos los activos digitales de la organización, ya que de esa manera no podemos valorar adecuadamente la complejidad y los riesgos presentes en el entorno de TI.

  - La falta de identificación de amenazas internas y externas que pueden afectar el Core del negocio.

  - La falta de clasificación de los sistemas de información según la

criticidad de sus funciones para la continuidad de la actividad de la empresa.

- No se tiene definido los objetivos de recuperación, es decir una entidad financiera suele albergar información cambiante y, y por lo tanto los objetivos de recuperación tienden a ser más exigentes.

- La falta de una técnica y herramienta de gestión en recuperación de información

- No tener definido los roles de los involucrados y las responsabilidades que cada uno de ellos asume.

- No considerar los puntos de vista de todos los stakeholders durante la planificación, y lo que es más importante, deben estar de acuerdo con los SLAs y las prioridades establecidas por el equipo de TI.

- No tener documentada el plan estratégico de recuperación, ya que esto permitirá que se garantice la conservación de protocolos que se hayan definido, y facilitar una buena comunicación interna.

- La ausencia de pruebas de simulación para restaurar información crítica, ya que esto permitirá determinar la compatibilidad de los procedimientos, identificar áreas que requieren algún tipo de cambio y, por su puesto, entrenar a los empleados.

- No tener actualizados los planes de respaldo de información, ya que esto debe darse cuando exista cambios sustanciales en la propia organización, los cuales terminan afectando al RTO y RPO de la misma.

- ✓ **Plan de implementación para la restauración de la información**

El objetivo de este plan de respaldo que se implementará será definir de forma precisa cómo el banco financiero gestionará los incidentes en caso de un desastre o de otro incidente disruptivo y cómo recuperará sus actividades en el centro de datos dentro de plazos establecidos. A si mismo este plan deberá mantener en un nivel aceptable el daño producido por un incidente disruptivo.

Este plan se aplicará a todas las actividades críticas y que estén expuesta a una mala restauración de información, y cuyo alcance será el de la implementar un plan de respaldo en el centro de datos.

A si mismo los usuarios de este documento son todos los empleados del área de infraestructura tecnológica del banco financiero, tanto internos como externos, que cumplan una función en la implementación del plan de respaldo.

- **Contenido del plan de respaldo a implementar**

Este plan respaldo a implementar estará formado por dos grandes secciones:

- ➢ El plan de respuesta a los incidentes:

El objetivo de este plan será asegurar de manera óptima una restauración de la información para la continuidad de las operaciones en el centro de datos ante el caso de un desastre o de otro incidente, como también contener el incidente. A si mismo lograremos reducir al mínimo el tiempo total que nos tomaría restaurar la información y no tener algún impacto en el Core del negocio de la empresa financiera.

Este plan se aplicará a todos los incidentes de severidad alta que amenazan con interrumpir cualquier actividad crítica dentro del centro de datos por un período mayor al objetivo de tiempo de recuperación de cada actividad individual, tal como se puede apreciar en la Tabla N° 4.29

Tabla 0:26: Los usuarios de este documento son los empleados de TI

Cargo	Autorizaciones y responsabilidades
Empleados del Área de Infraestructura Tecnológica	Creación, Evaluación e Implementación de un Plan de Recuperación de Desastres: Un sitio de respaldo es vital, sin embargo, es inútil sin un plan de respaldo.
Empleados del Área de Infraestructura Tecnológica	Sitios de respaldo: frío, templado y caliente: Uno de los aspectos más importantes del plan de respaldo es tener una ubicación desde la cual este puede ser ejecutado.
Empleados del Área de Infraestructura Tecnológica	Disponibilidad del Hardware y Software: Su plan de respaldo debe incluir métodos para conseguir el hardware y software necesarios para las operaciones en el sitio de respaldo.
Empleados del Área de Infraestructura Tecnológica	Disponibilidad de los respaldos: Cuando se declara un desastre, es necesario notificarlo a sus instalaciones de almacenamiento fuera de sitio por dos razones: ✓ Para enviar los últimos respaldos al sitio de respaldo ✓ Para coordinar entregas de respaldos regulares al sitio de respaldo
Empleados del Área de Infraestructura Tecnológica	Conectividad de red al sitio de respaldo: Un centro de datos no es de mucha ayuda si se encuentra desconectado del resto de la organización que está sirviendo.
Empleados del Área de Infraestructura Tecnológica	Personal del sitio de respaldo: El problema sobre conseguir el personal para su sitio de respaldo es multidimensional.
Empleados del Área de Infraestructura Tecnológica	Regreso a la normalidad: Eventualmente todas las operaciones y actividades retoman su continuidad.

Fuente y elaboración propia.

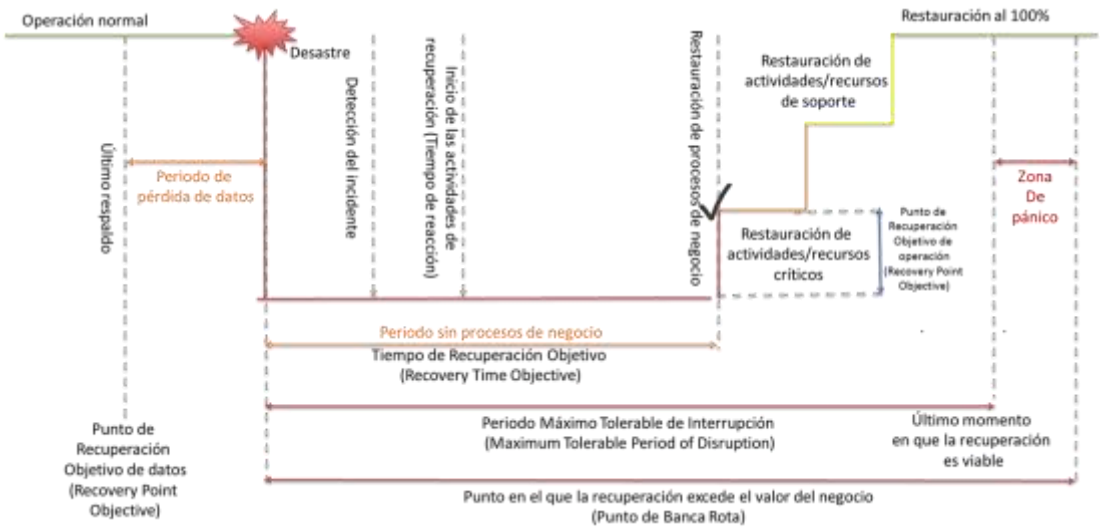

Figura 0.4: Plan de Respaldo y Recuperación ante incidentes Mediante el RPO y RTO

Fuente y elaboración propia.

Ejemplo: se muestra una fórmula sencilla con el costo de la pérdida de datos o falla crítica en una red empresarial.

1. Si los ingresos anuales son de aproximadamente US$1 millón por año y es un modelo 24×7, 7 días a la semana, 52 semanas al año, dividiendo el negocio de $1 millón de dólares por las 8760 horas, le dará la siguiente pérdida de ingresos por hora:

Figura 0.5: Costo por la Perdida de datos – Modelo 1

Fuente y elaboración propia.

2. Si sus ingresos anuales son de aproximadamente US$1 millón por año y la empresa es una de las que opera de 8:00AM a 5:00PM, 5 días a la semana, 52 semanas al año, dividiendo el negocio de $1 millón de dólares por las 2.080 horas, le proporcionará la siguiente pérdida de ingresos por hora:

Figura 0.6: Costo por la Perdida de Datos – Modelo 2

Fuente y elaboración propia.

Procedimiento para incidentes disruptivos en el centro de datos

Todos los empleados del área de infraestructura tecnológica tendrán la obligación de reportar cualquier incidente, así mismo estarán obligados a informar cualquier incidente disruptivo de la siguiente manera:

- Todos los incidentes relacionados con tecnología de la información y de la comunicación dentro del centro de datos será informado telefónicamente al jefe de Mesa de Servicios o Área de Infraestructura Tecnológica.

A si mismo cualquier otro evento o vulnerabilidad que atente contra el centro de datos y que todavía no se hubiera convertido en un incidente disruptivo debe ser informado de la misma forma y a la brevedad.

Gestión de incidentes disruptivos en el centro de datos

La persona que recibe la información sobre el incidente deberá evaluar si el incidente, o potencial incidente, es real o falso, y si es real, activa inmediatamente este plan respetando los siguientes pasos:

- Comenzar a controlar y erradicar el incidente de acuerdo con lo detallado en las siguientes secciones del presente documento, ver Tabla N° 4.30

- Informar a todas las personas responsables sobre la ocurrencia del incidente dentro de su área de responsabilidad.

- Notificar a jefe de seguridad y salud ocupacional, que debe evaluar si es necesario alertar a alguna de las partes interesadas.

- Controla el estado del incidente y, si es necesario, informa a los demás empleados involucrados, acerca del progreso en la gestión del incidente.

En caso de que una persona no pueda controlar y/o erradicar el incidente, debe informarlo al gerente de crisis. La información que se envía al gerente de crisis debe incluir la naturaleza y alcance del incidente disruptivo, como también su potencial impacto.

La persona responsable de erradicar el incidente deberá registrar en el registro de incidentes todas las acciones tomadas.

Gerente de crisis

El Gerente de crisis deberá supervisar el progreso en la gestión del incidente y el período de interrupción de las actividades individuales mediante la implementación el plan de respaldo y deberá evaluar el tiempo necesario para solucionar el incidente dentro del centro de datos.

En el caso de que el tiempo necesario para solucionar el incidente es mayor que el objetivo de tiempo de recuperación de una actividad particular, se deberá activar el plan de recuperación para la actividad interrumpida, tal como se puede apreciar en la Tabla N° 4.30. En ese caso, el gerente de crisis deberá notificárselo a todos los gerentes de recuperación, quienes activarán sus planes de recuperación.

- El plan de recuperación de actividades en el centro de datos:

El objetivo de este plan de recuperación será definir de forma precisa cómo el banco financiero recuperará sus actividades críticas dentro de plazos establecidos ante el caso de un desastre o de un incidente disruptivo. A si mismo este plan deberá garantizar la culminación de esta actividad dentro del objetivo de tiempo de recuperación establecido, tal como se puede apreciar en la Tabla N° 4.30

Este plan propuesto incluye todos los recursos y procesos necesarios para la recuperación de esta actividad.

Para llevar a cabo este plan de recuperación es necesario contar con un gabinete de crisis quienes serán los responsables de gestionar, coordinar, controlar y el cumplimiento de la recuperación de las actividades en el centro de datos de la entidad financiera.

Tabla 0:27: Pasos de recuperación para la disponibilidad de los servicios

PROCEDIMIENTOS DE RECUPERACIÓN	GABINETE DE CRISIS
1. Reunión del equipo en la ubicación alternativa	
1.1 Verificar si todos los miembros del equipo se encuentran presentes	Auxiliar de recuperación
1.2 Informar a los miembros del equipo del incidente disruptivo ocurrido	Gerente de recuperación
1.3 Dar directrices puntuales necesarias a los miembros del equipo	Coordinador de recuperación
2. Verificación y recuperación de la infraestructura	
2.1 Verificar si se cuenta con la infraestructura necesaria para iniciar la recuperación de la actividad	Supervisor de recuperación
2.2 Levantar un informe de la infraestructura disponible y de la infraestructura faltante necesaria	Supervisor de recuperación
2.3 Instalación de muebles básicos necesarios para iniciar la recuperación	Auxiliar de recuperación
3. Verificación y recuperación de los equipos y vínculos de TIC	
3.1 Verificar si se cuenta con los equipos y vínculos necesarios para iniciar la recuperación de la actividad	Operador de recuperación
3.2 Levantar un informe sobre los equipos faltantes (si los hubiera) y de cuál es la capacidad operativa con los equipos actuales	Operador de recuperación
3.3 Poner operativos los equipos necesarios para iniciar la recuperación de la actividad	Supervisor de recuperación
4. Verificación y recuperación de aplicaciones	
4.1 Verificar si se cuenta con las aplicaciones y los instaladores de estas para iniciar la recuperación de la actividad	Operador de recuperación
4.2 Poner en marcha las aplicaciones necesarias para la recuperación de la actividad	Supervisor de recuperación
4.3 Levantar un informe sobre el funcionamiento de las aplicaciones puestas en marcha y la carga de trabajo que pueden soportar	Supervisor de recuperación
5. Verificación y recuperación de datos y documentos	
5.1 Verificar si se cuenta con los datos y documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación
5.2 Poner a disposición de las personas correspondientes los datos y los documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación

Fuente y elaboración propia.

Verificar

- ✓ **Plan de prueba y verificación**

El objetivo de este plan es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los arreglos para la gestión de la implementación del plan de respaldo, como también para establecer las acciones correctivas necesarias.

Este plan se aplicará a todos los elementos que se encuentran dentro del alcance de la implementación del plan de respaldo, incluyendo los arreglos con los proveedores y socios.

Los usuarios de este documento son todos los empleados del área de la infraestructura de TI que cumplen una función en la implementación del plan de respaldo.

- **Implementación de pruebas y verificaciones**

La prueba y verificación para la implementación del plan de respaldo en el centro de datos del banco financiero será de la siguiente manera:

- ✓ Plazo: se efectuará durante 3 días luego de la implementación del plan de respaldo.

- ✓ A si mismo será el gerente de producción y servicios de TI la persona responsable de la coordinación e implementación del plan de respaldo.

- ✓ A continuación, mencionaremos los objetivos de esta prueba y su verificación:

- Se verificará si los planes y recursos son precisos para implementar el plan de respaldo.

- Se verificará si los empleados del área de infraestructura de TI son responsables de la implementación del plan de respaldo y si están familiarizados con los detalles del plan.

- Se verificar la implementación de todos los pasos especificados en los planes.

- Se verificará el cumplimento con todas las obligaciones dentro de los plazos predefinidos.

- Se deberá activar procedimientos alternativos en caso de que sea necesario.

- Se deberá asegurar todos los recursos necesarios (incluyendo la recuperación de datos).

- Se deberá lograr la armonización del plan de respaldo de otras actividades.

- Se deberá generar comentarios o sugerencias para mejorar el plan.

✓ Para el alcance de la prueba y verificación: Se validará el correcto funcionamiento de los servicios en el centro de datos con respecto a:

- Comunicaciones
- Aplicativos de Core Bancario y Negocios
- Aplicativos Financieros, Administrativos y Tecnológicos

✓ Para la operatividad de los servicios y actividades incluyen también a los proveedores del banco financiero como:

- Easy Recovery
- Cosapi Data
- SONDA
- IBM
- Level3
- Bloomberg
- Electrodata, etc.

✓ Método de prueba y verificación:

- El chequeo de escritorio: este chequeo será aplicado en los planes con técnicas de auditoría, validación y verificación; realizado por el autor del plan y un moderador.

- El repaso de los planes: este chequeo será aplicado en los planes a través de interacción de equipos; realizada por los principales participantes del plan y por el moderador, cuya interacción se verifica en una reunión conjunta.

- La simulación: esta verificación se aplicará en todos los planes relacionados con recursos de información reales; realizado por todos los empleados necesarios, proveedores y por el moderador.

- La prueba funcional: se procederá a reubican las actividades en la ubicación alternativa bajo un ejercicio controlado (anunciado); participan todos los empleados del área de infraestructura de TI necesarios, proveedores, el moderador y observadores.

- La prueba completa: se trasladan todas las actividades desde la ubicación original a la alternativa (anunciado o no); participan todos los empleados del área de infraestructura de TI necesarios, proveedores, el moderador, observadores y auditores.

- **Revisión de resultados**

El gerente de producción y servicio TI deberá controlar los resultados de las pruebas y deberá preparar un Informe de prueba y verificación.

Este informe deberá incluir las acciones correctivas correspondientes, como también otras recomendaciones de mejora, tal como se puede apreciar en la Tabla N° 4.31

Tabla 0:28: Registros guardados de la revisión de resultados.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Informe de prueba y verificación (en formato electrónico)	Ordenador del Gerente de producción y Servicios TI	Gerente de producción y servicios TI	Solamente el Gerente de producción y Servicios TI puede editar la lista	3 años

Fuente y elaboración propia.

✓ **Plan de mantenimiento y revisión en el centro de datos**

Para mantener la exactitud y utilidad de todos los elementos de esta implementación del plan de respaldo, será necesario revisar y actualizar de acuerdo con las siguientes frecuencias, tal como se puede apreciar en la Tabla N° 4.32

Tabla 0:29: Plan de mantenimiento y revisión en el centro de datos

Elemento del estudio de planes de respaldo	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Realizar copias de seguridad manualmente o las programará para que se realicen automáticamente	X	X	X	X	X	X	X	X	X	X	X	X
Comprobar que las copias de seguridad se pueden usar		X		X			X			X		
Tiempo guardará las copias de seguridad antes de volver a usar el medio	X		X		X			X			X	
Tiempo tardará la restauración a partir de la copia de seguridad más reciente	X					X				X		
Comprobará que las copias de seguridad se han realizado correctamente			X						X			

Fuente y elaboración propia.

- ✓ **Procedimiento para auditoria interna en el centro de datos**

El objetivo de este procedimiento será describir todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Este procedimiento será aplicado a todas las actividades realizadas dentro de la implementación del plan de respaldo.

Los usuarios de este documento son los miembros de la alta gerencia del banco financiero y los auditores internos.

- **Objetivo de la auditoría interna en el centro de datos**

  El objetivo de la auditoría interna en el centro de datos será determinar si los procedimientos, controles, procesos, acuerdos y demás actividades en la implementación del plan de respaldo concuerdan con las normas ISO 22301, con las regulaciones correspondientes y con la documentación interna de la organización; como también verificar si son implementados y sostenidos y si cumplen requisitos de políticas y establecen objetivos.

- **Planificación de la auditoría interna en el centro de datos**

  Sera el gerente de producción y servicios TI quien aprobara el programa anual de auditorías internas.

  A sí mismo el deberá realizar una o más auditorías internas en el transcurso de un año, asegurando una cobertura acumulativa de todo el alcance en la implementación del plan de respaldo. Las auditorías internas son planificadas en base a la evaluación de riesgos, como también por los resultados de auditorías anteriores. Generalmente son realizadas antes de la revisión por parte de la gerencia.

  El programa anual de auditoría interna debe incluir la siguiente información sobre cada auditoría interna individual:

- El momento de la auditoría: La fecha será establecida previa coordinación y disponibilidad con el área de infraestructura de TI
- Alcance de la auditoría: Área de Infraestructura TI
- Criterio de auditoría: Normas ISO 22301.
- Métodos de la auditoría: Revisión de documentación, entrevistas con empleados del área de infraestructura de TI, revisión de registros, de sistemas informáticos, etc.
- Quién realizará la auditoría: Auditor interno del banco financiero.

A si mismo se deberá llevar un registro de las auditorías realizadas en el Programa anual de auditoría interna.

- **Designación de auditores internos en el centro de datos**

El gerente de riesgos será la persona quien designe a los auditores internos.

Un auditor interno puede ser alguien de la organización o una persona externa a la misma. Los criterios para la designación de los auditores se explican a continuación:

- Que conozca las normas ISO/IEC 22301.
- Que esté familiarizado sobre técnicas de auditoría sobre sistemas de gestión.
- Que sepa cómo funcionan las tecnologías de la información y de la comunicación como para estar familiarizado con el objetivo de los sistemas individuales y también con los impactos sobre procedimientos de seguridad.

También se deberá seleccionar a los auditores internos de tal forma que garanticen la objetividad e imparcialidad; es decir, de evitar el conflicto de intereses, ya que los auditores no pueden auditar su propio trabajo.
Y finalmente se recomienda que los auditores internos realicen un curso para auditores internos según la norma ISO/IEC 22301.

Actuar

- ✓ **Procedimiento para acciones correctivas y preventivas en el centro de datos**

El objetivo de este procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de acciones correctivas y preventivas.

Este procedimiento se aplica a todas las actividades concernientes a la implementación del plan de respaldo.

Los usuarios de este documento son todos los empleados del área de infraestructura de TI del banco financiero.

- ✓ **Acciones Correctivas**

  - No conformidad

    Para el caso del estudio las no-conformidad será todo incumplimiento de los requerimientos de las normas, documentación interna, reglamentos, obligaciones contractuales y de otra clase dentro de la implementación del plan de respaldo. A si mismo las no-conformidades podrán ser identificadas durante una auditoría interna o externa, en base a resultados de la revisión por parte de la dirección, luego de incidentes, durante el transcurso normal de las operaciones de negocios o en cualquier otra situación.

    Un empleado del área de infraestructura de TI que detecta una no conformidad deberá tomar acciones inmediatamente para controlarla, contenerla y corregirla y para contener sus consecuencias. Si un empleado no es responsable de esa no conformidad debe transmitir la información sobre ella a la persona responsable que pueda corregirla.

- Acciones correctivas

  La persona responsable deberá evaluar la necesidad de eliminar el origen de la no-conformidad y evitar su recurrencia tomando acciones correctivas.

  Una acción correctiva deberá ser iniciada por cualquier empleado del área de infraestructura de TI, cuando sea pertinente, por cualquier cliente, proveedor o socio de la organización. Una acción correctiva podrá demandar cambios sobre cualquier documento, proceso o acuerdo dentro del marco de la implementación del plan de respaldo.

- Implementación de acciones correctivas

  Los pasos para la implementación de una acción correctiva se dan a conocer de la siguiente forma tal como se puede apreciar en la Tabla N° 4.33

Tabla 0:30: Pasos para la implementación de una acción correctiva en el centro de datos

Pasos	Persona responsable de la Implementación
1. Revisión de la no-conformidad	Cualquiera con una función en la implementación del análisis de vulnerabilidad
2. Determinación de la causa de la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
3. Identificar si la no-conformidad ya existía	Persona responsable del área donde se ha identificado la no-conformidad
4. Evaluación de la necesidad de tomar acciones para eliminar la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
5. Determinación de las acciones necesarias para eliminar las causas de la no-conformidad y para asegurar que no se produzca nuevamente	Persona responsable del área donde se ha identificado la no-conformidad
6. Implementación de las acciones planificadas	Persona a cargo de la implementación, designada por la persona responsable
7. Revisión para determinar si la acción tomada logró eliminar las causas de la no-conformidad	Subgerente de producción y servicios TI
8. Informar a todas las personas involucradas que se ha implementado la acción correctiva	Persona a cargo de la implementación, designada por la persona responsable

Fuente y elaboración propia.

- ✓ **Acciones Preventivas**

El objetivo de la acción preventiva será evitar los efectos no deseados, es decir actividades que estén orientadas a ser eliminadas por ser causa de potenciales de no-conformidades evitando así su ocurrencia.

- Implementación de acciones preventivas

  Las acciones preventivas serán identificadas durante la evaluación de riesgos y el análisis del impacto en el centro de datos generalmente es detallado en el plan de tratamiento del riesgo.

  Las acciones preventivas que no sean atendidas en los documentos mencionados se implementaran de la misma forma que la detallada para las acciones correctivas.

- ✓ **Gestión de documentos**

El propietario de este documento será el subgerente de producción y servicios TI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, será necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas y preventivas iniciadas

- Cantidad de acciones correctivas y preventivas incompletas

- Cantidad de acciones correctivas y preventivas tomadas sin haber sido registradas en un formulario designado.

4.6 Situación Pre Test

Variable de Posibles Riesgos

a) Toma de Muestras Pre-Test

Con la información obtenida se procedió al estudio, análisis e interpretación de los datos obtenidos del número total de posibles riesgos, en tal sentido se presenta el resumen e interpretación de los datos pre-test obtenidos durante el periodo del año 2014 – 2015.

De igual forma, se presentan en la Tabla N° 4.34, los posibles riesgos por nivel, presentados por cada grupo de muestra de dos meses cada uno.

Tabla 0:31: Tipos de posibles Riesgos. Muestra Pre - Test

GRUPO	NÚMERO DE POSIBLES RIESGOS					TOTAL, DE POSIBLES RIESGOS
	NIVEL MUY BAJA	NIVEL BAJA	NIVEL MEDIO	NIVEL ALTO	NIVEL MUY ALTO	
1	4	3	3	4	2	16
2	3	4	2	3	1	13
3	2	5	5	3	3	18
4	2	2	5	3	2	14
5	5	4	4	2	2	17
6	4	3	4	2	3	16
7	4	4	4	1	3	16
8	5	4	2	1	3	15
9	4	4	2	2	2	14
10	4	2	3	2	1	12
11	3	1	3	3	3	13
12	5	3	1	1	2	12
Total	45	39	38	27	27	176

Fuente y elaboración propia.

b) Nivel de incidencia en los Posibles Riesgos

Con los datos obtenidos de la muestra tal como se puede apreciar en la Tabla N° 4.35, se pudo establecer la incidencia que presentan estas causas en los Posibles Riesgos como resultado de un evento ante desastre

mediante el diagrama de Pareto, tal como se puede apreciar en la Figura N° 4.8

Tabla 0:32: Ocurrencia de Posibles Riesgos

	# POSIBLES RIESGOS	% FRECUENCIA	% ACUMULADO
Nivel muy baja	45	25.56	25.56
Nivel baja	39	22.15	47.71
Nivel baja	38	21.59	69.30
Nivel medio	27	15.34	84.64
Nivel muy alto	27	15.34	100.00
Total, de Causas	176	100.00	

oración propia.

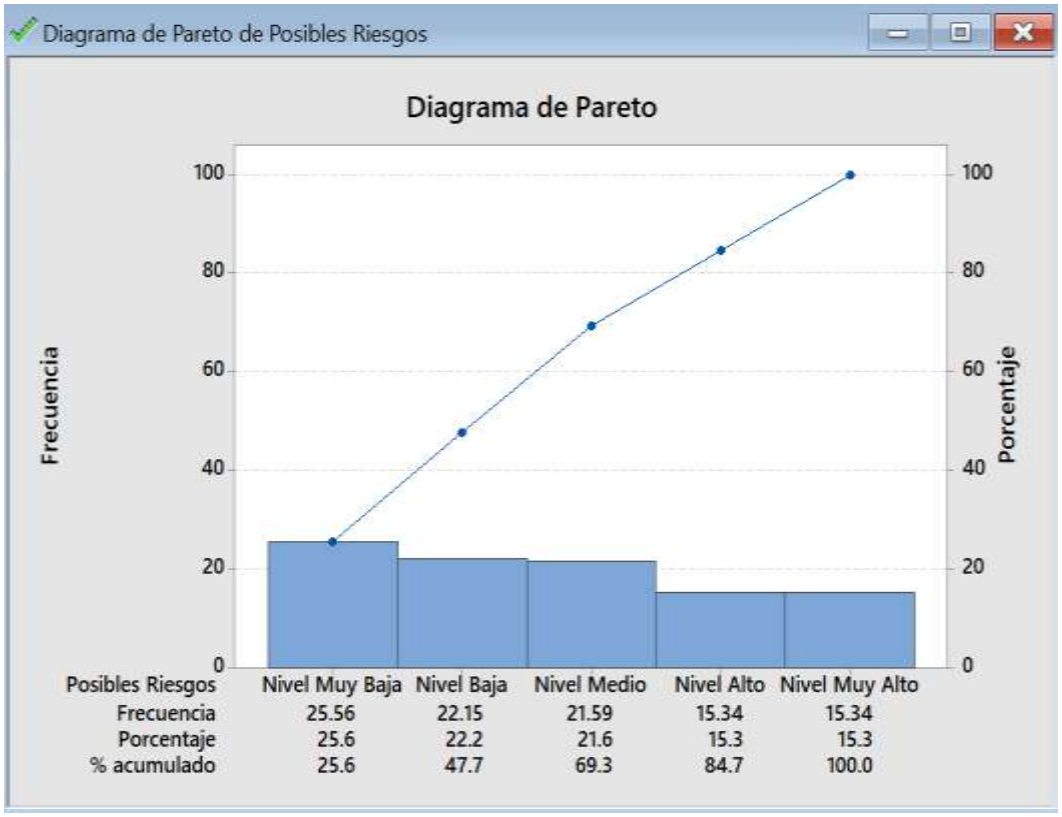

Figura 0.7: Diagrama de Pareto aplicando a los posibles Riesgos

Fuente y elaboración propia.

Con ello se determinó que los posibles riesgos como son los de nivel muy bajo y nivel bajo son las causas con mayor presencia con un 47.71% de presencia, dicho diagrama fue empleado en el ciclo de capacitación a los usuarios a manera informativa.

c) Análisis Descriptivo

Mediante el software MINITAB, se extrajeron las estadísticas descriptivas de la muestra pre-test.

Tabla 0:33: Estadística Descriptiva

ESTADÍSTICO	VALOR
Media	14.66
Desviación estándar	1.96
Primer cuartil (Q1)	13.00
Mediana	14.50
Tercer cuartil (Q3)	16.00
Moda	16
Asimetría	0.13
Curtosis	-1.11

Fuente y elaboración propia.

De acuerdo con la Tabla N° 4.36, la muestra pre-test tiene un promedio de 14.66 posibles riesgos con una desviación estándar de 1.96, cabe resaltar el valor de la moda de 16, un valor de defecto considerado muy alto. En lo que respecta a las medidas de forma, tenemos que:

- ✓ El valor de la curtosis de la muestra pre-test arroja como resultado -1.11, que indica que la distribución tiene colas ligeras y un pico levemente aplanado que la distribución normal (distribución platicurtica), ya que presentan un reducido grado de concentración alrededor de los valores centrales de la variable, aunque de forma leve por su cercanía a cero.
- ✓ El valor de la asimetría de la muestra de la muestra pre-test tiene como resultado 0.13, el cual es mayor que cero, por tanto, se determina que la curva que distribuye a los datos es asimétricamente positiva (x > Md>Mo) o asimétricos a la derecha debido a que la "cola" de la distribución apunta

a la derecha, es decir, una pequeña concentración de valores se encuentra a la derecha de la media.

d) Prueba de Normalidad

Para la prueba de normalidad se plantea las siguientes hipótesis:

Ho = Los datos siguen una distribución normal.

H1 = Los datos no siguen una distribución normal.

Con un nivel de significancia: α=0.05

Mediante el uso del software MINITAB, se aplicó la prueba de normalidad Kolmogorov – Smirnov (K – S), ver la Figura N° 4.9

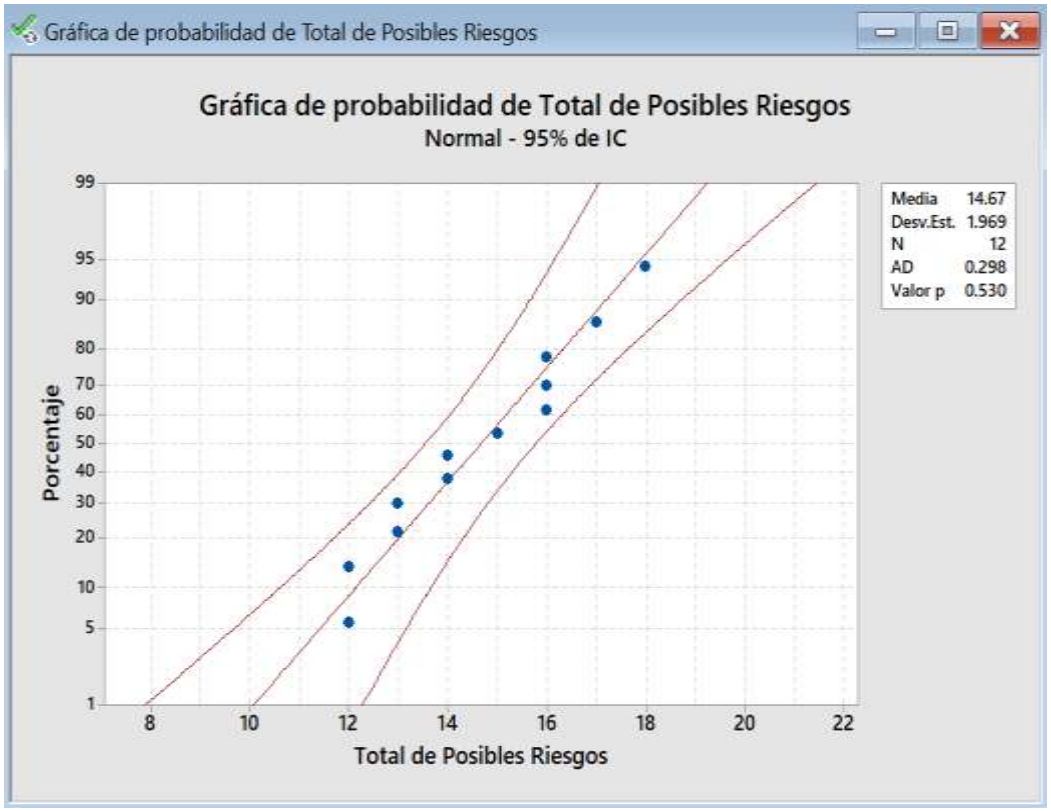

Figura 0.8: Grafica de Probabilidad de Posibles Riesgos: Prueba K - S

Fuente y elaboración propia.

El criterio de evaluación indica que:

Valor P > α → Se acepta Ho

Valor P ≤ α → Se rechaza Ho

Los resultados obtenidos en la prueba de normalidad K – S, muestran un valor P=0.530, valor que es mayor a 0.05 que es el nivel de significancia, por lo tanto, según el criterio de evaluación, se acepta la hipótesis nula (Ho), concluyendo de esta manera, que los datos de la muestra siguen una distribución normal, por lo tanto, son paramétricos.

e) Análisis Aplicando Control Estadístico

Se utiliza la Gráfica de Control C tal como puede ver en la Figura N° 4.10, puesto que el tamaño de las muestras en cada grupo no es constante debido a que existen varios tipos de causas como: los de nivel muy bajo, bajo, medio, alto, muy alto.

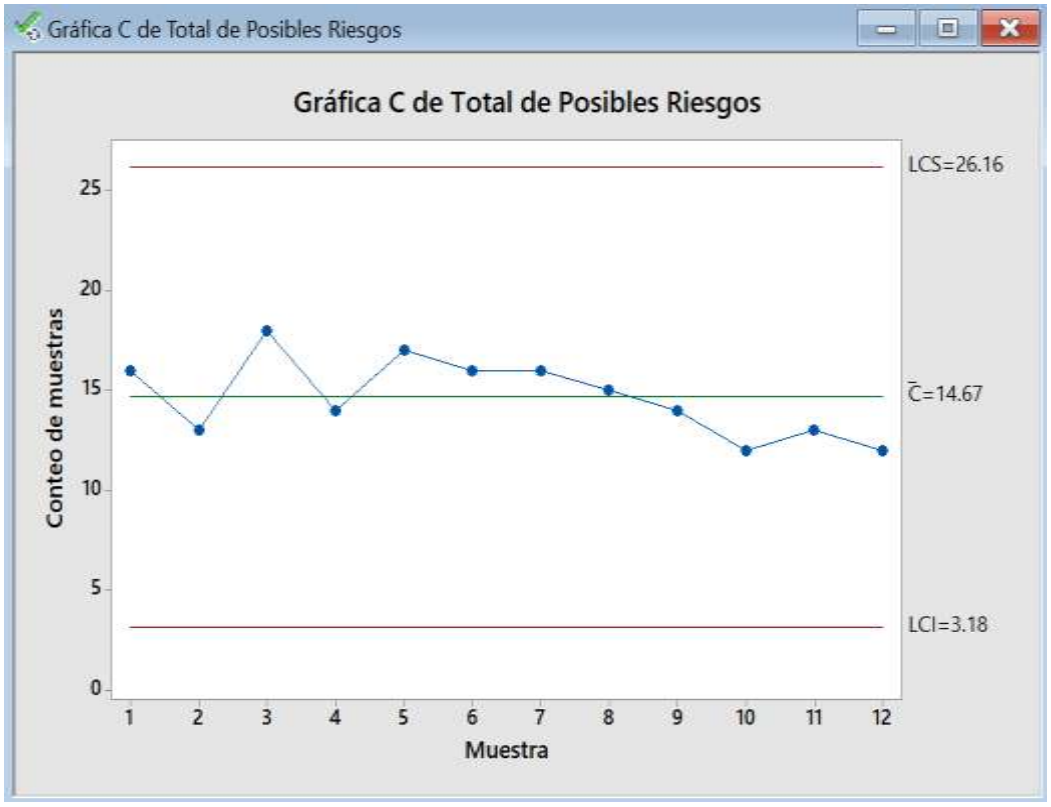

Figura 0.9: Grafica C del total de Posibles Riesgos

Fuente y elaboración propia.

Para tal fin, se empleó el software MINITAB y de acuerdo con la muestra tomada, se espera que el número de causas varié entre 3.18 como LCI (límite de control inferior) y 26.16 como LCS (límite de control superior) con un promedio de 14.67. El límite de una gráfica C refleja la variación esperada para el número de Posibles Riesgos, donde se aprecia que el proceso es estable puesto que no hay puntos fuera de los límites de control.

En la prueba pre-test, a pesar de la estabilidad, se evidencia una alta ocurrencia de causas, por tanto, se aplicó la metodología descrita en el punto 3.1, buscando mejorar este problema reduciendo la variabilidad común, es decir, reducir significativamente el valor del estadístico C y seguir vigilando estadísticamente su normalidad.

Variable de la Capacidad de Respuesta

a) Toma de Muestras Pre-Test

Con la información obtenida se procedió al estudio, análisis e interpretación de los datos obtenidos del tiempo total en la capacidad de respuesta, en tal sentido se presenta el resumen e interpretación de los datos pre-test obtenidos durante el periodo del año 2014 – 2015.

De igual forma, se presentan en la Tabla N° 4.37, la capacidad de respuesta, presentados por cada grupo de muestra de dos meses cada uno.

Tabla 0:34: Tiempos en la Capacidad de Respuesta. Muestra Pre - Test

GRUPO	TIEMPO EN LA CAPACIDAD DE RESPUESTA (en Minutos)		PROMEDIO DE CAPACIDAD DE RESPUESTA
1	80	70	75
2	90	95	92.5
3	60	70	65
4	85	110	97.5
5	80	90	85
6	55	85	70
7	80	75	77.5

8	130	100	115
9	75	90	82.5
10	85	70	77.5
11	70	75	72.5
12	65	50	57.5

Fuente y elaboración propia.

b) Análisis Descriptivo

En la Tabla N° 4.38, se aprecia los principales estadísticos descriptivos que permiten ver claramente el comportamiento y las tendencias de los datos de la muestra pre – test de la variable dependiente: Capacidad de Respuesta, se emplea el MINITAB.

Tabla 0:35: Estadística Descriptiva

ESTADÍSTICO	VALOR
Media	80.63
Desviación estándar	15.49
Primer cuartil (Q1)	70.63
Mediana	77.50
Tercer cuartil (Q3)	90.63
Moda	77.5
Asimetría	0.85
Curtosis	1.06

Fuente y elaboración propia.

De acuerdo con la Tabla N° 4.26, la muestra pre-test tiene un promedio de 80.63 minutos en la capacidad de respuesta con una desviación estándar de 15.49, cabe resaltar el valor de la moda de 77.5, que es un valor en minutos en la capacidad de respuesta que más se repite de la muestra pre – test.

En lo que respecta a las medidas de forma, tenemos que:

- ✓ El valor de la curtosis de la muestra pre-test arroja como resultado 1.06, que indica que la distribución tiene colas ligeras y un pico levemente aplanado que la distribución normal, esta curva se cataloga como distribución platicurtica, ya que presentan un reducido grado de concentración alrededor de los valores centrales de la variable, aunque de forma leve por su cercanía a cero.

- ✓ El valor de la asimetría de la muestra de la muestra pre-test tiene como resultado 0.85, el cual es mayor que cero, por tanto, se determina que la curva que distribuye a los datos es asimétricamente positiva (x > Md>Mo) o asimétricos a la derecha debido a que la "cola" de la distribución apunta a la derecha, pero de acuerdo al valor obtenido la asimetría es muy leve debido a que el valor obtenido es muy cercano a cero, es decir, una pequeña concentración de valores se encuentra la derecha de la media.

c) Prueba de Normalidad

Para la prueba de normalidad se plantea las siguientes hipótesis:

Ho = Los datos siguen una distribución normal.

H1 = Los datos no siguen una distribución normal.

Con un nivel de significancia: α=0.05

Mediante el uso del software MINITAB, se aplicó la prueba de normalidad Kolmogorov – Smirnov (K – S), tal como se puede apreciar en la Figura N° 4.11

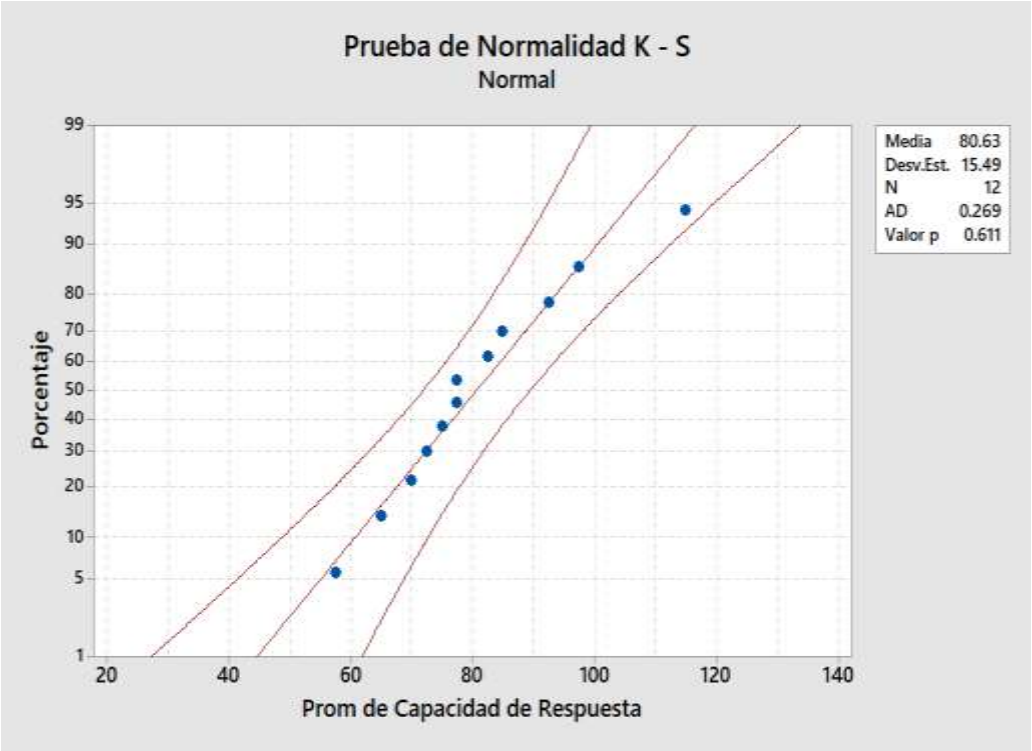

Figura 0.10: Grafica de Probabilidad de Capacidad Respuesta: Prueba K - S

Fuente y elaboración propia.

El criterio de evaluación indica que:

Valor $P > \alpha$ → Se acepta Ho

Valor $P \leq \alpha$ → Se rechaza Ho

Los resultados obtenidos en la prueba de normalidad K – S, muestran un valor P=0.611, valor que es mayor a 0.05 que es el nivel de significancia, por lo tanto, según el criterio de evaluación, se acepta la hipótesis nula (Ho), concluyendo de esta manera, que los datos de la muestra siguen una distribución normal, por lo tanto, son paramétricos.

d) Análisis Aplicando Control Estadístico

Se utiliza la Gráfica de Control X - R, puesto que dicha grafica es aplicable a procesos masivos y los datos son variables. En la Figura N° 4.12, se muestra los resultados pre – test empleando la Gráfica de Control X – R, mediante el software MINITAB.

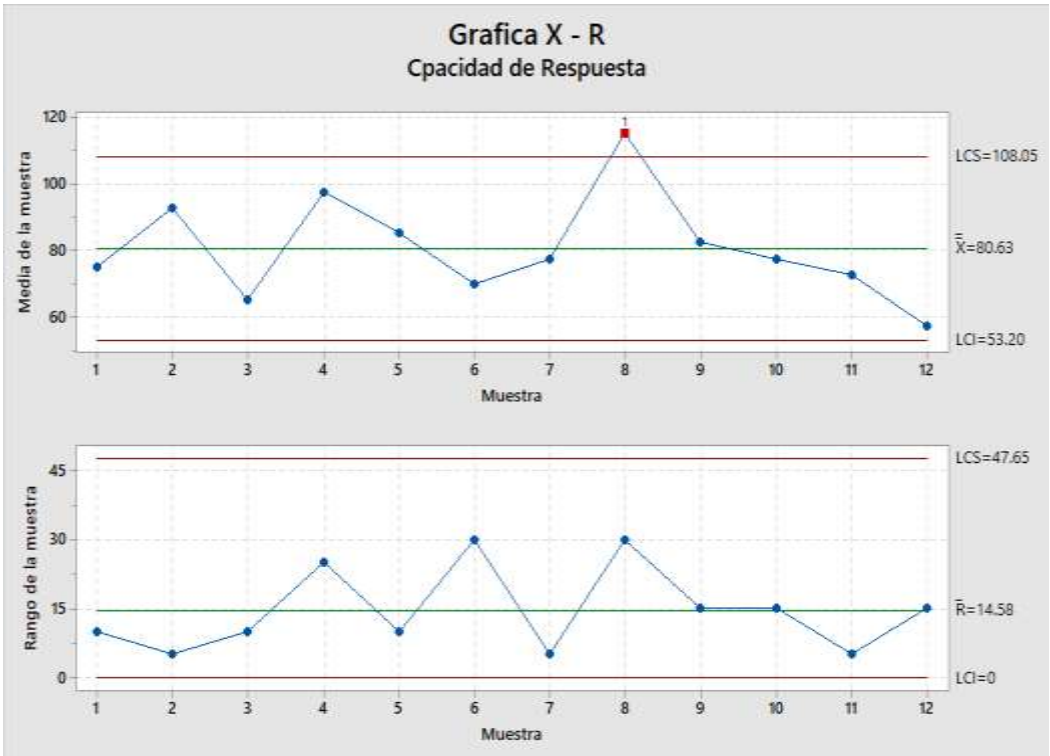

Figura 0.11: Grafica de Control X – R para la Capacidad de Respuesta

Fuente y elaboración propia.

La grafica R indica que los datos están bajo control, por lo tanto, es apropiado examinar la gráfica X que, de acuerdo con la muestra, se espera que el tiempo en la capacidad de respuesta varié entre 53.20 como LCL y 108.05 como LCS con un promedio de 80.63. En la Gráfica de Control X - R se refleja una alta variabilidad, notándose que el proceso no es estable, puesto que hay puntos fuera de los límites de control. Además, no supera una de las pruebas especiales, como es el caso de:

PRUEBA 1. Que advierte un punto con mayor a la desviación estándar desde la línea central, es decir, el punto fuera del límite de control, prueba contundente de falta de control. La prueba fallo en el punto 8 de la gráfica de control.

Variable de la Restauración de la Información

a) Toma de Muestras Pre-Test

Con la información obtenida se procedió al estudio, análisis e interpretación de los datos obtenidos del tiempo total en la restauración de la información, en tal sentido se presenta el resumen e interpretación de los datos pre-test obtenidos durante el periodo del año 2014 – 2015.

De igual forma, se presentan en la Tabla N° 4.39, la capacidad de respuesta, presentados por cada grupo de muestra de dos meses cada uno.

Tabla 0:36: Tiempo en la Restauración de la Información. Muestra Pre - Test

GRUPO	TIEMPO EN LA RESTAURACIÓN DE LA INFORMACIÓN (en Minutos)		PROMEDIO DE RESTAURACIÓN DE LA INFORMACIÓN
1	45	35	40.00
2	45	45	45.00
3	30	35	32.50
4	45	55	50.00
5	40	45	42.50
6	30	45	37.50
7	42	35	38.50
8	65	50	57.50
9	35	45	40.00
10	45	35	40.00
11	35	35	35.00
12	30	30	30.00

Fuente y elaboración propia.

b) Análisis Descriptivo

En la Tabla 4.40, se aprecia los principales estadísticos descriptivos que permiten ver claramente el comportamiento y las tendencias de los datos de la muestra pre – test de la variable dependiente: Restauración de la Información, se emplea el MINITAB

Tabla 0:37: Estadística Descriptiva

ESTADÍSTICO	VALOR
Media	40.71
Desviación estándar	7.52
Primer cuartil (Q1)	35.63
Mediana	40.00
Tercer cuartil (Q3)	44.38
Moda	40
Asimetría	0.93
Curtosis	1.21

Fuente y elaboración propia.

De acuerdo con la Tabla N° 4.28, la muestra pre-test tiene un promedio de 40.71 minutos en la restauración de la información con una desviación estándar de 7.52, cabe resaltar el valor de la moda de 40, que es un valor en minutos en la capacidad de respuesta que más se repite de la muestra pre – test.

En lo que respecta a las medidas de forma, tenemos que:

- ✓ El valor de la curtosis de la muestra pre-test arroja como resultado 1.21, que indica que la distribución tiene colas ligeras y un pico levemente aplanado que la distribución normal, esta curva se cataloga como distribución platicurtica, ya que presentan un reducido grado de concentración alrededor de los valores centrales de la variable, aunque de forma leve por su cercanía a cero.
- ✓ El valor de la asimetría de la muestra de la muestra pre-test tiene como resultado 0.93, el cual es mayor que cero, por tanto, se determina que la curva que distribuye a los datos es asimétricamente positiva (x > Md>Mo) o asimétricos a la derecha debido a que la "cola" de la distribución apunta a la derecha, pero de acuerdo al valor obtenido la asimetría es muy leve debido a que el valor obtenido es muy cercano a cero, es decir, una pequeña concentración de valores se encuentra la derecha de la media.

c) Prueba de Normalidad

Para la prueba de normalidad se plantea las siguientes hipótesis:

Ho = Los datos siguen una distribución normal.

H1 = Los datos no siguen una distribución normal.

Con un nivel de significancia: α=0.05

Mediante el uso del software MINITAB, se aplicó la prueba de normalidad Kolmogorov – Smirnov (K – S), ver la Figura N° 4.13

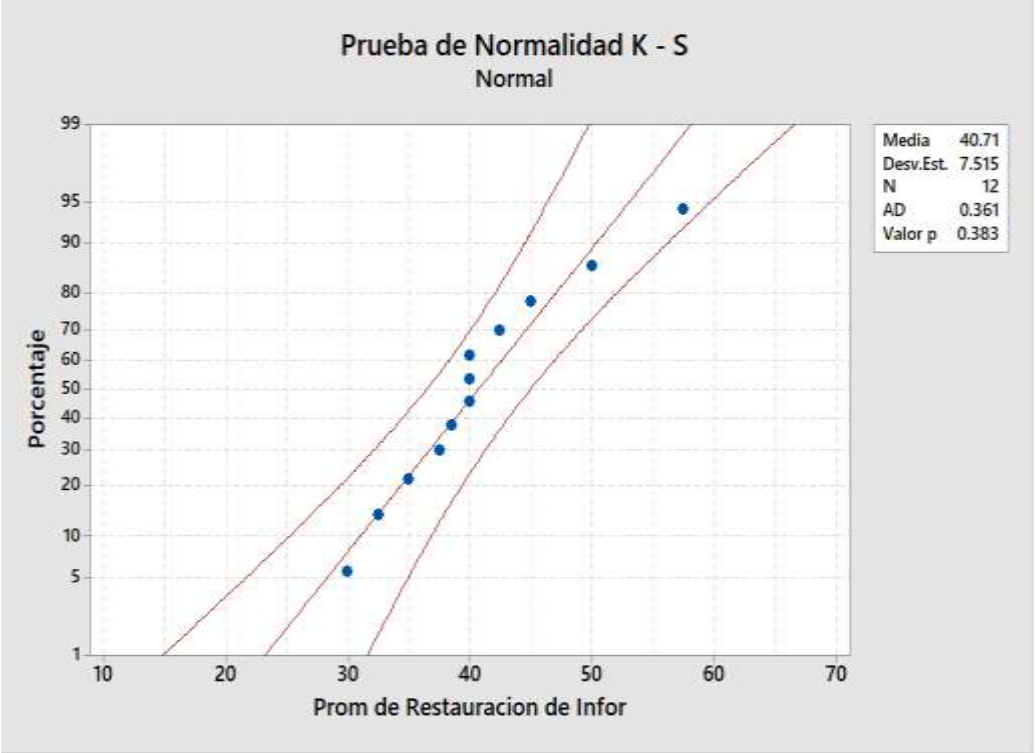

Figura 0.12: Grafica de Probabilidad de Restauración de Información: Prueba K -S

Fuente y elaboración propia.

El criterio de evaluación indica que:

Valor P > α → Se acepta Ho

Valor P ≤ α → Se rechaza Ho

Los resultados obtenidos en la prueba de normalidad K – S, muestran un valor P=0.383, valor que es mayor a 0.05 que es el nivel de significancia, por lo tanto, según el criterio de evaluación, se acepta la hipótesis nula (Ho), concluyendo de esta manera, que los datos de la muestra siguen una distribución normal, por lo tanto, son paramétricos.

d) Análisis Aplicando Control Estadístico

Se utiliza la Gráfica de Control X - R, puesto que dicha grafica es aplicable a procesos masivos y los datos son variables. En la Figura N° 4.14, se muestra los resultados pre – test empleando la Gráfica de Control X – R, mediante el software MINITAB.

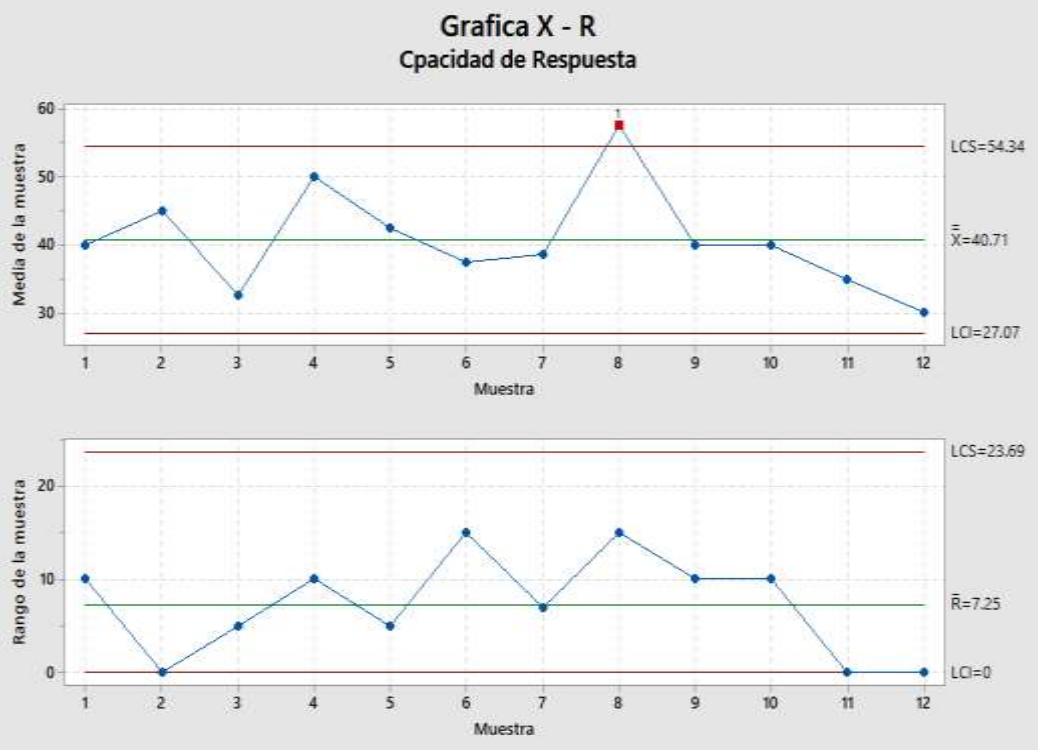

Figura 0.13: Grafica de Control X – R para la Capacidad de Respuesta

Fuente y elaboración propia.

La grafica R indica que los datos están bajo control, por lo tanto, es apropiado examinar la gráfica X que, de acuerdo con la muestra, se espera que el tiempo en la capacidad de respuesta varié entre 27.07 como LCL y 54.34 como LCS con un promedio de 40.71. En la Gráfica de Control X - R se refleja una alta

variabilidad, notándose que el proceso no es estable, puesto que hay puntos fuera de los límites de control. Además, no supera una de las pruebas especiales, como es el caso de:

PRUEBA 1. Que advierte un punto con mayor a la desviación estándar desde la línea central, es decir, el punto fuera del límite de control, prueba contundente de falta de control. La prueba fallo en el punto 8 de la gráfica de control.

4.7 Situación Post Test

Variable de Posibles Riesgos

a) Toma de Muestras Pre-Test

Con la información obtenida se procedió nuevamente al estudio, análisis e interpretación de los datos obtenidos del número total de posibles riesgos, en tal sentido se presenta el resumen e interpretación de los datos post-test obtenidos durante el periodo del año 2016 – 2017.

De igual forma, se presentan en la Tabla N° 4.41, los posibles riesgos por nivel, presentados por cada grupo de muestra de dos meses cada uno.

Tabla 0:38: Tipos de Posibles Riesgos. Muestra Pre – Test.

GRUPO	NÚMERO DE POSIBLES RIESGOS					TOTAL, DE POSIBLES RIESGOS
	NIVEL MUY BAJA	NIVEL BAJA	NIVEL MEDIO	NIVEL ALTO	NIVEL MUY ALTO	
1	3	2	1	2	1	9
2	0	2	2	1	1	6
3	0	3	2	2	0	7
4	2	2	3	2	2	11
5	3	2	2	1	2	10
6	2	3	2	1	1	9
7	2	2	2	0	1	7
8	0	2	1	0	1	4
9	2	2	1	1	0	6
10	2	2	2	2	0	8
11	3	1	2	2	1	9
12	0	1	1	1	0	3
TOTAL	19	24	21	15	10	89

Fuente y elaboración propia.

b) Nivel de incidencia en los Posibles Riesgos

Con los datos obtenidos de la muestra tal como se puede observar en la Tabla N° 4.42, se pudo establecer la incidencia que presentan estas causas en los Posibles Riesgos como resultado de un evento ante desastre mediante el diagrama de Pareto.

Tabla 0:39: Ocurrencia de Posibles Riesgos

	# POSIBLES RIESGOS	% FRECUENCIA	% ACUMULADO
Nivel Baja	24	26.96	26.96
Nivel Medio	21	23.59	50.55
Nivel muy Baja	19	21.34	71.89
Nivel Alto	15	16.85	88.74
Nivel muy Alto	10	11.23	100.00
Total, de Causas	**89**	**100.00**	

Fuente y elaboración propia.

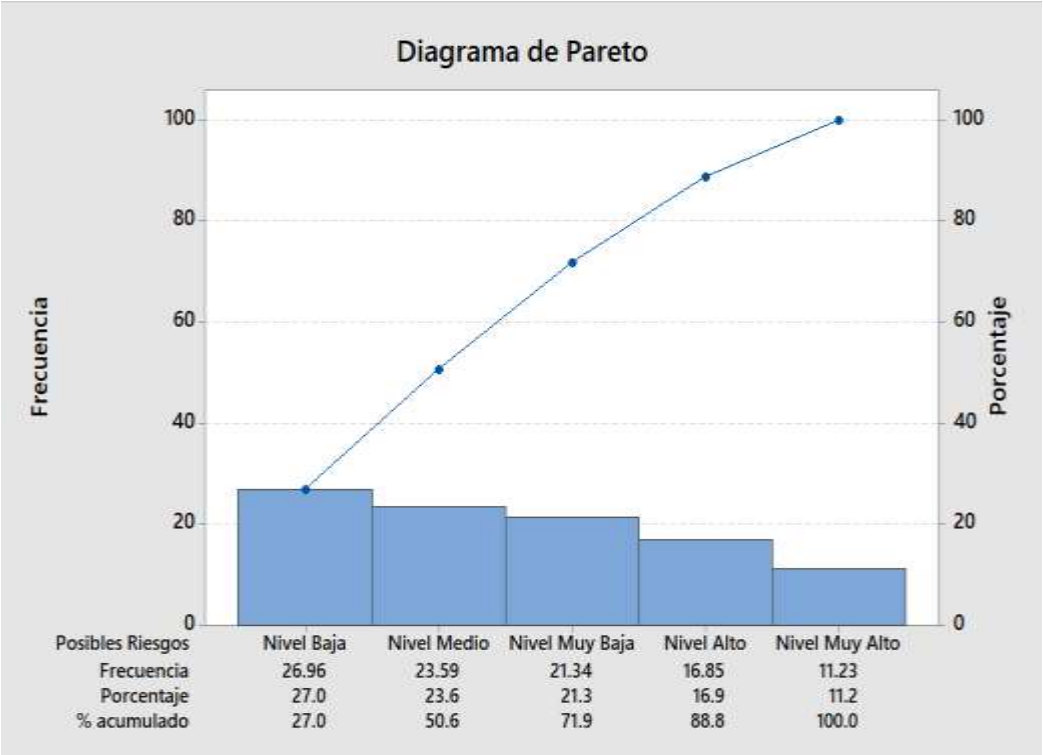

Figura 0.14: Diagrama de Pareto aplicando a los posibles Riesgos

Fuente y elaboración propia.

El diagrama de Pareto determino que los posibles riesgos como son los de nivel baja y nivel medio siguen siendo los causantes con mayor presencia con un 50.55% de presencia, con la aplicación de la propuesta de solución del presente trabajo de tesis, se pudo comprobar que los niveles de incidencia de las causas posibles de riesgo disminuyen en un 49.43%, es decir, de 176 causas disminuye a 89 causas para en un mismo tamaño de muestra, tal como se puede observar en la Figura N° 4.15

c) Análisis Descriptivo

Mediante el software MINITAB, se extrajeron las estadísticas descriptivas de la muestra post - test.

Tabla 0:40: Estadística Descriptiva

ESTADÍSTICO	VALOR
Media	7.42
Desviación estándar	2.39
Primer cuartil (Q1)	6.00
Mediana	7.50
Tercer cuartil (Q3)	9.00
Moda	9
Asimetría	-0.45
Curtosis	-0.41

Fuente y elaboración propia.

Lo que se muestra en la Tabla N° 4.43, es que la muestra post–test tiene un promedio de 7.42 causas por cada muestra, con una desviación estándar de 2.39; con una moda de 9 causas según muestra.

En lo que respecta a las medidas de forma, tenemos que:

- ✓ El valor de la curtosis de la muestra post-test arroja como resultado -0.41, que indica que la distribución tiene colas ligeras y un pico levemente aplanado que la distribución normal (distribución platicúrtica), ya que presentan un reducido grado de concentración alrededor de los valores centrales de la variable, aunque de forma leve por su cercanía a cero.

- ✓ El valor de la asimetría de la muestra de la muestra post-test tiene como resultado -0.45, el cual es menor que cero, por tanto, se determina que la curva que distribuye a los datos es asimétricamente negativa (x< Md<Mo) o asimétricos a la izquierda debido a que la "cola" de la distribución apunta a la izquierda, es decir, una pequeña concentración de valores se encuentra a la izquierda de la media.

d) Prueba de Normalidad

Para la prueba de normalidad se plantea las siguientes hipótesis:

Ho = Los datos siguen una distribución normal.

H1 = Los datos no siguen una distribución normal.

Con un nivel de significancia: α=0.05

Mediante el uso del software MINITAB, se aplicó la prueba de normalidad Kolmogorov – Smirnov (K – S), ver la Figura N° 4.16

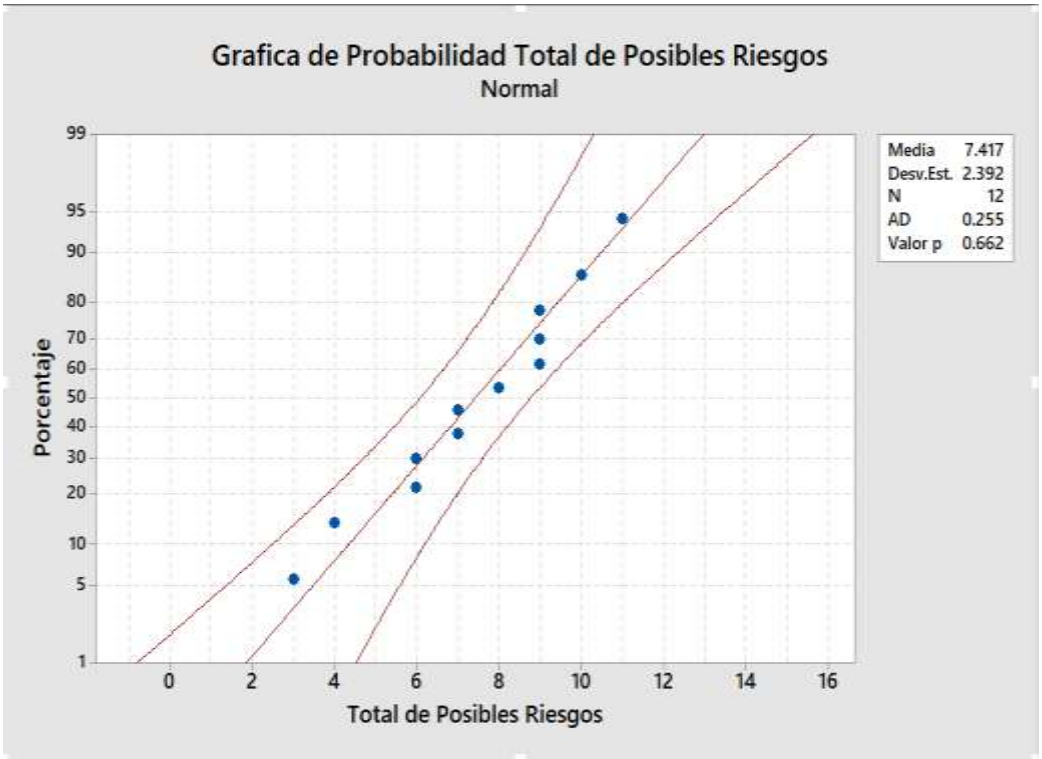

Figura 0.15: Grafica de Probabilidad de Posibles Riesgos: Prueba K - S

Fuente y elaboración propia.

El criterio de evaluación indica que:

Valor P > α → Se acepta Ho

Valor P ≤ α → Se rechaza Ho

Los resultados obtenidos en la prueba de normalidad K – S, muestran un valor P=0.662, valor que es mayor a 0.05 que es el nivel de significancia, por lo tanto, según el criterio de evaluación, se acepta la hipótesis nula (Ho), concluyendo de

esta manera, que los datos de la muestra siguen una distribución normal, por lo tanto, son paramétricos.

e) Análisis Aplicando Control Estadístico

Para el post - test se utiliza nuevamente la Gráfica de Control C, por los motivos expuestos para la prueba pre - test.

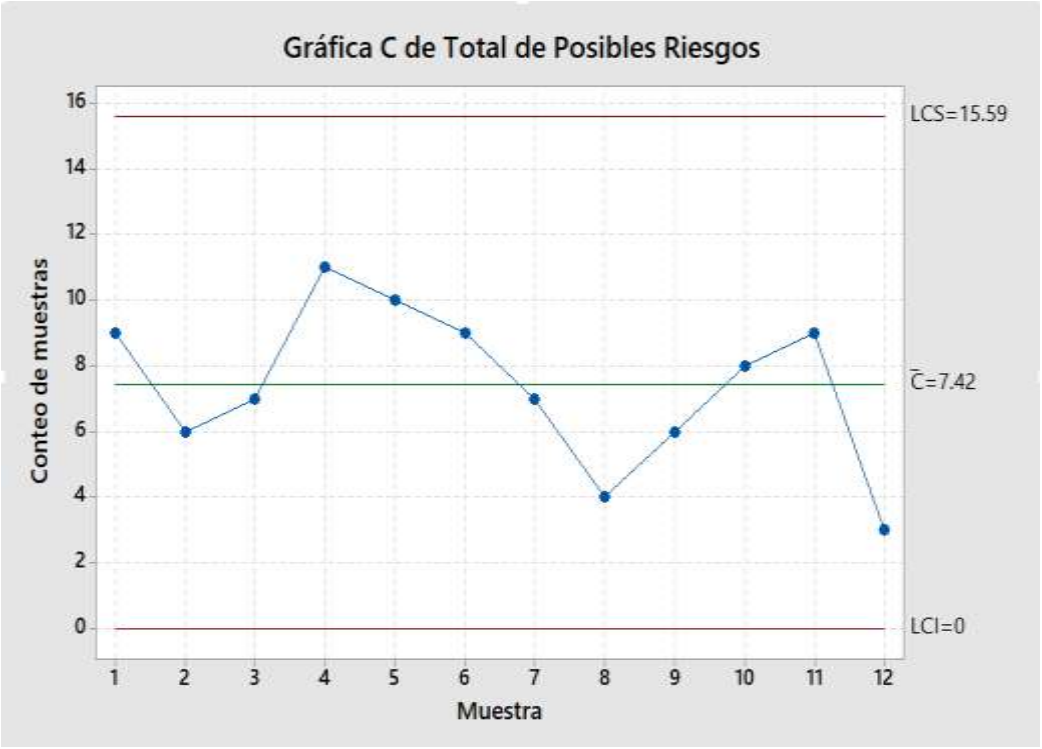

Figura 0.16: Grafica C del total de posibles Riesgos

Fuente y elaboración propia.

De acuerdo con la muestra tomada tal como se muestra en la Figura N° 4.17, se espera que el número de causas varié entre 0 como LCI (límite de control inferior) y 15.59 como LCS (límite de control superior) con un promedio de 7.42, dando una notoria mejoría al disminuir el promedio de causas, con respecto a la muestra pre-test. Los límites de la Grafica C reflejan la variación esperada para el número de causas, donde se aprecia que el proceso sigue siendo estable puesto que no hay puntos fuera de los límites de control. Además, se superan las pruebas para las causas especiales.

Variable de la Capacidad de Respuesta

a) Toma de Muestras Post-Test

Con la información obtenida se procedió nuevamente al estudio, análisis e interpretación de los datos obtenidos del tiempo total en la capacidad de respuesta, en tal sentido se presenta el resumen e interpretación de los datos post-test obtenidos durante el periodo del año 2016 – 2017.

De igual forma, se presentan en la Tabla N° 4.44, la capacidad de respuesta, presentados por cada grupo de muestra de dos meses cada uno.

Tabla 0:41: Tiempos en la Capacidad de Respuesta. Muestra Pre - Test

GRUPO	TIEMPO EN LA CAPACIDAD DE RESPUESTA (en Minutos)		PROMEDIO DE CAPACIDAD DE RESPUESTA
1	22	33	27.50
2	32	29	30.50
3	30	35	32.50
4	30	28	29.00
5	30	30	30.00
6	26	25	25.50
7	38	25	31.50
8	35	20	27.50
9	29	30	29.50
10	30	33	31.50
11	20	35	27.50
12	28	25	26.50

Fuente y elaboración propia.

b) Análisis Descriptivo

En la Tabla N° 4.45, se aprecia los principales estadísticos descriptivos que permiten ver claramente el comportamiento y las tendencias de los datos de la muestra post – test de la variable dependiente: Capacidad de Respuesta, se emplea el MINITAB

Tabla 0:42: Estadística Descriptiva

ESTADÍSTICO	VALOR
Media	29.08
Desviación estándar	2.20
Primer cuartil (Q1)	27.50
Mediana	29.25
Tercer cuartil (Q3)	31.25
Moda	27.50
Asimetría	-0.03
Curtosis	-1.11

Fuente y elaboración propia.

Como se puede apreciar, la muestra post-test tiene un promedio de 29.08 minutos en la capacidad de respuesta con una desviación estándar de 2.20, cabe resaltar el valor de la moda de 27.50, que es un valor en minutos en la capacidad de respuesta que más se repite de la muestra post – test.

En lo que respecta a las medidas de forma, tenemos que:

- ✓ El valor de la curtosis de la muestra post-test arroja como resultado -1.11, que indica que la distribución tiene colas ligeras y un pico levemente aplanado que la distribución normal, esta curva se cataloga como distribución platicúrtica, ya que presentan un reducido grado de concentración alrededor de los valores centrales de la variable, aunque de forma leve por su cercanía a cero.

- ✓ El valor de la asimetría de la muestra de la muestra post-test tiene como resultado -0.03, el cual es menor que cero, por tanto, se determina que la curva que distribuye a los datos es asimétricamente negativa (x < Md<Mo) o asimétricos a la izquierda debido a que la "cola" de la distribución apunta a la izquierda, pero de acuerdo al valor obtenido la asimetría es muy leve debido a que el valor obtenido es muy cercano a cero, es decir, una pequeña concentración de valores se encuentra la derecha de la media.

c) Prueba de Normalidad

Para la prueba de normalidad se plantea las siguientes hipótesis:

Ho = Los datos siguen una distribución normal.

H1 = Los datos no siguen una distribución normal.

Con un nivel de significancia: α=0.05

Mediante el uso del software MINITAB, se aplicó la prueba de normalidad Kolmogorov – Smirnov (K – S), ver la Figura N° 4.18

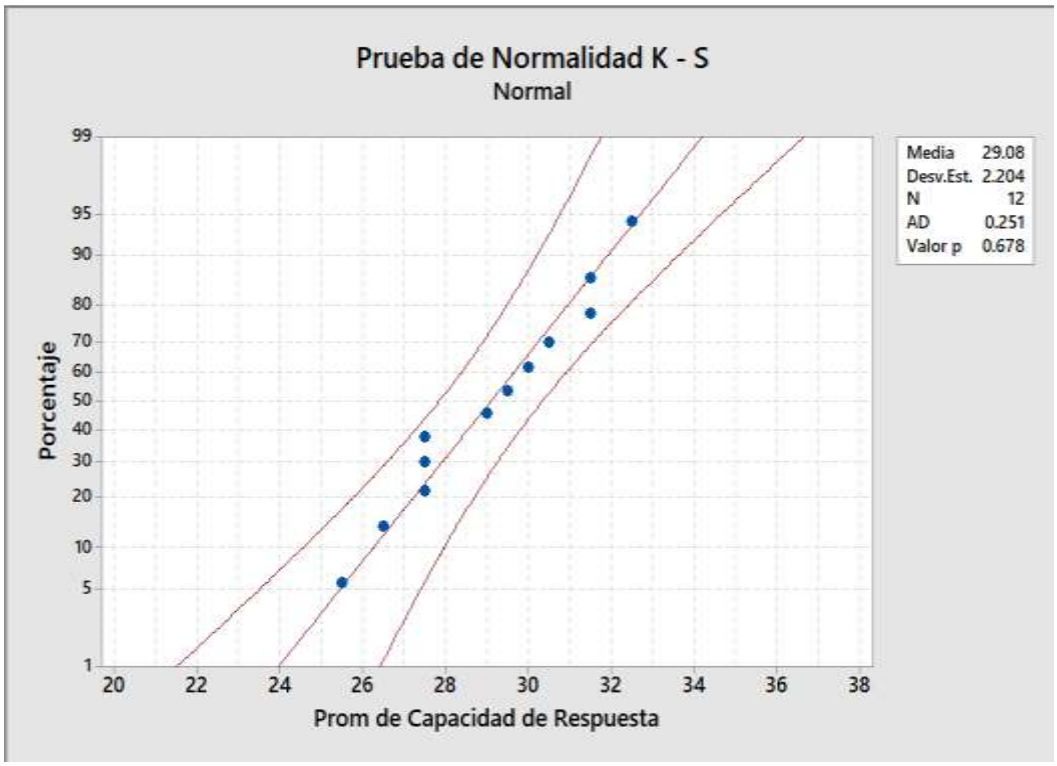

Figura 0.17: Grafica de Probabilidad de Capacidad de Respuesta: Prueba K - S

Fuente y elaboración propia.

El criterio de evaluación indica que:

Valor P > α → Se acepta Ho

Valor P ≤ α → Se rechaza Ho

Los resultados obtenidos en la prueba de normalidad K – S como se aprecia en la Figura N° 4.29, muestran un valor P=0.678, valor que es mayor a 0.05 que es el nivel de significancia, por lo tanto, según el criterio de evaluación, se acepta la hipótesis nula (Ho), concluyendo de esta manera, que los datos de la muestra siguen una distribución normal, por lo tanto, son paramétricos.

d) Análisis Aplicando Control Estadístico

Para la muestra post-test nuevamente se empleó la Gráfica de Control X - R, puesto que dicha grafica es aplicable a procesos masivos y los datos son variables.

Sin embargo, luego de la aplicación de la alternativa de solución propuesta por el presente trabajo de tesis, está o no bajo nivel estadístico

En la Figura N° 4.19, se muestra los resultados post – test empleando la Gráfica de Control X – R, mediante el software MINITAB.

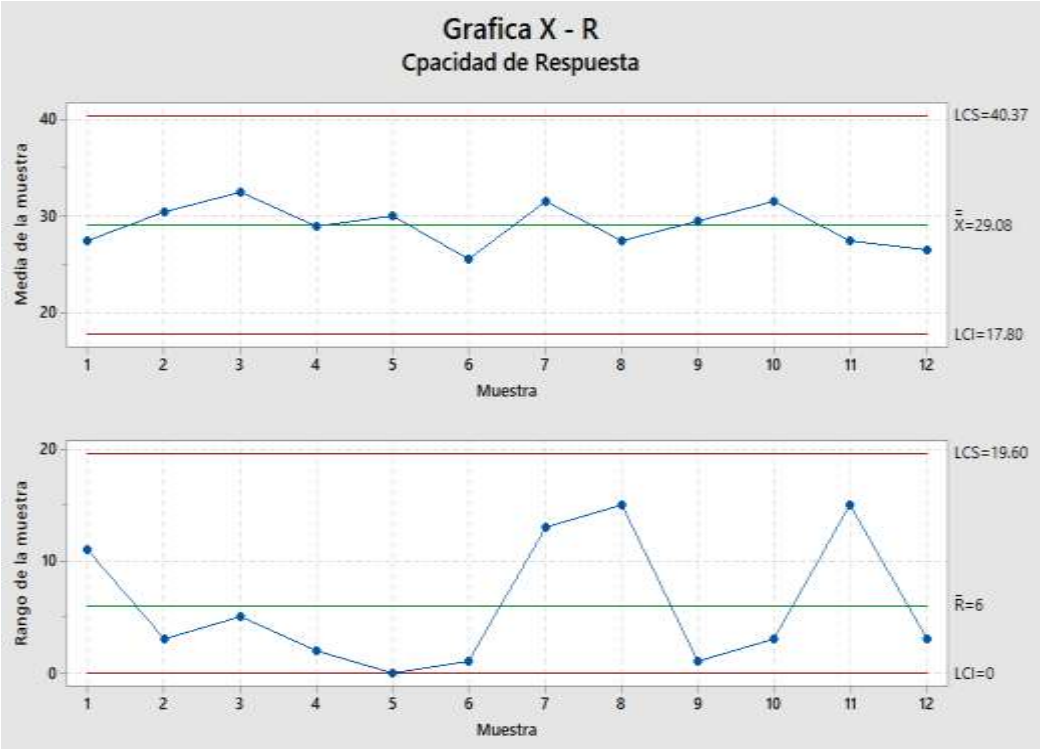

Figura 0.18: Grafica de Control X -R para la Capacidad de Respuesta

Fuente y elaboración propia.

Para los datos obtenidos de la muestra post-test, tanto la gráfica X como la gráfica R están bajo control estadístico, además la muestra logro superar todas las pruebas de causas especiales en la gráfica de control (no se identificaron patrones específicos de datos). Por lo tanto, se concluye que el proceso está bajo control estadístico, porque no hay puntos fuera de los límites de control como resultado de la aplicación de la propuesta de mejora del presente trabajo de tesis.

En comparación con la muestra pre-test, la aplicación de la propuesta de mejora ha conllevado a desplazar la media de 17.80 a 40.37 minutos en la capacidad de respuesta, de esta manera, se está disminuyendo el tiempo en la capacidad de respuesta, que da como resultado mantener estable la continuidad del negocio.

Variable de la Restauración de la Información

a) Toma de Muestras Post-Test

Con la información obtenida se procedió nuevamente al estudio, análisis e interpretación de los datos obtenidos del tiempo total en la restauración de la información, en tal sentido se presenta el resumen e interpretación de los datos post-test obtenidos durante el periodo del año 2016 – 2017.

De igual forma, se presentan en la Tabla N° 4.46, la restauración de información, presentados por cada grupo de muestra de dos meses cada uno.

Tabla 0:43: Tiempo en la Restauración de la Información. Muestra Pre - Test

GRUPO	TIEMPO EN LA RESTAURACIÓN DE LA INFORMACIÓN (en Minutos)		PROMEDIO DE RESTAURACIÓN DE LA INFORMACIÓN
1	22	22	22.00
2	28	20	24.00
3	22	29	25.50
4	24	29	26.50
5	26	25	25.50
6	30	24	27.00
7	26	34	30.00
8	32	30	31.00
9	27	32	29.50
10	31	35	33.00
11	28	30	29.00
12	32	25	28.50

Fuente y elaboración propia.

b) Análisis Descriptivo

En la Tabla N° 4.47, se aprecia los principales estadísticos descriptivos que permiten ver claramente el comportamiento y las tendencias de los datos de la muestra post – test de la variable dependiente: Restauración de la Información, se emplea el MINITAB

Tabla 0:44: Estadística Descriptiva

ESTADÍSTICO	VALOR
Media	27.62
Desviación estándar	3.12
Primer cuartil (Q1)	25.50
Mediana	27.75
Tercer cuartil (Q3)	29.87
Moda	25.50
Asimetría	-0.11
Curtosis	-0.36

Fuente y elaboración propia.

De acuerdo con la Tabla N° 4.47, la muestra post-test tiene un promedio de 27.62 minutos en la restauración de la información con una desviación estándar de 3.12, cabe resaltar el valor de la moda de 25.50, que es un valor en minutos en la capacidad de respuesta que más se repite de la muestra post – test.

En lo que respecta a las medidas de forma, tenemos que:

- ✓ El valor de la curtosis de la muestra post-test arroja como resultado -0.36, que indica que la distribución tiene colas ligeras y un pico levemente aplanado que la distribución normal, esta curva se cataloga como distribución platicúrtica, ya que presentan un reducido grado de concentración alrededor de los valores centrales de la variable, aunque de forma leve por su cercanía a cero.

- ✓ El valor de la asimetría de la muestra de la muestra pre-test tiene como resultado -0.11, el cual es menor que cero, por tanto, se determina que la curva que distribuye a los datos es asimétricamente negativa ($x < Md < Mo$) o asimétricos a la izquierda debido a que la "cola" de la distribución apunta a la izquierda, pero de acuerdo al valor obtenido la asimetría es muy leve debido a que el valor obtenido es muy cercano a cero, es decir, una pequeña concentración de valores se encuentra la izquierda de la media.

c) Prueba de Normalidad

Para la prueba de normalidad se plantea las siguientes hipótesis:

Ho = Los datos siguen una distribución normal.

H1 = Los datos no siguen una distribución normal.

Con un nivel de significancia: $\alpha=0.05$

Mediante el uso del software MINITAB, se aplicó la prueba de normalidad Kolmogorov – Smirnov (K – S), ver la Figura N° 4.20

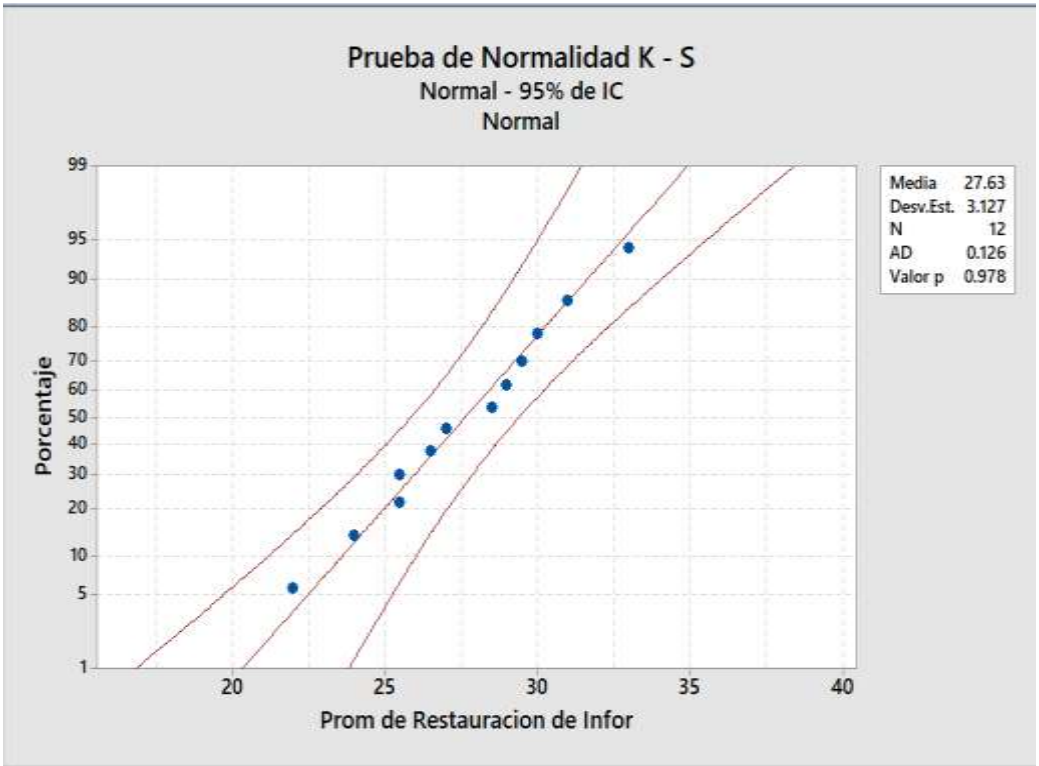

Figura 0.19: Grafica de Probabilidad de Restauración de Información: Prueba K - S

Fuente y elaboración propia.

El criterio de evaluación indica que:

Valor P > α → Se acepta Ho

Valor P ≤ α → Se rechaza Ho

Los resultados obtenidos en la prueba de normalidad K – S, muestran un valor P=0.978, valor que es mayor a 0.05 que es el nivel de significancia, por lo tanto, según el criterio de evaluación, se acepta la hipótesis nula (Ho), concluyendo de esta manera, que los datos de la muestra siguen una distribución normal, por lo tanto, son paramétricos.

d) Análisis Aplicando Control Estadístico

Para la muestra post-test nuevamente se empleó la Gráfica de Control X - R, puesto que dicha grafica es aplicable a procesos masivos y los datos son variables.

Sin embargo, luego de la aplicación de la alternativa de solución propuesta por el presente trabajo de tesis, está o no bajo nivel estadístico

En la Figura N° 4.21, se muestra los resultados post – test empleando la Gráfica de Control X – R, mediante el software MINITAB.

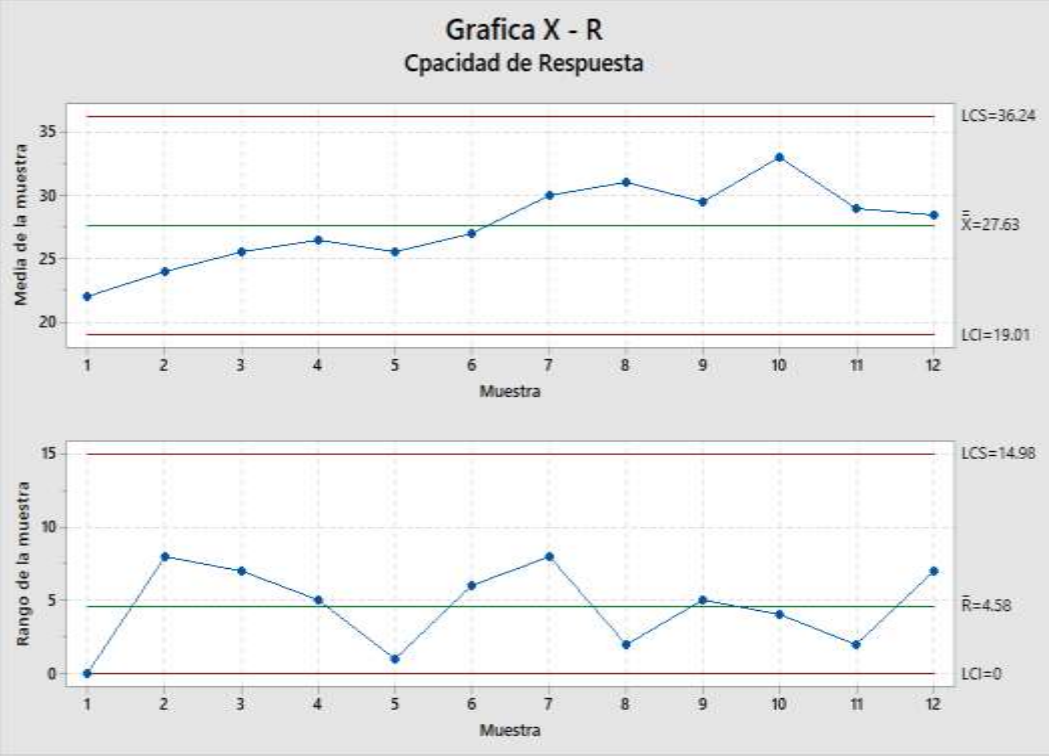

Figura 0.20: Grafica de Control X – S para la capacidad de Respuesta

Fuente y elaboración propia.

Para los datos obtenidos de la muestra post-test, tanto la gráfica X como la gráfica R están bajo control estadístico, además la muestra logro superar todas las pruebas de causas especiales en la gráfica de control (no se identificaron patrones específicos de datos). Por lo tanto, se concluye que el proceso está bajo control estadístico, porque no hay puntos fuera de los límites de control como resultado de la aplicación de la propuesta de mejora del presente trabajo de tesis.

En comparación con la muestra pre-test, la aplicación de la propuesta de mejora ha conllevado a desplazar la media de 19.01 a 36.24 minutos en la capacidad de respuesta, de esta manera, se está disminuyendo el tiempo en la capacidad de respuesta, que da como resultado mantener estable la continuidad del negocio.

4.8 Contrastación de Hipótesis

Hipótesis General

H0: Mediante el diseño e implementación de un plan de recuperación basado en la norma ISO/EIC 22301 **NO** se logrará mantener la continuidad del negocio para un centro de datos para empresas financieras.

H1: Mediante el diseño e implementación de un plan de recuperación basado en la norma ISO/EIC 22301 se logrará mantener la continuidad del negocio para un centro de datos para empresas financieras.

Hipótesis Específica I

H0: Mediante el diseño e implementación de un análisis de vulnerabilidad **NO** se logrará identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras.

H1: Mediante el diseño e implementación de un análisis de vulnerabilidad se logrará identificar los posibles riesgos que puedan afectar adversamente la integridad en un centro de datos para empresas financieras.

Regla para tomar Decisión Estadística

- ✓ Si p-valor > α se acepta la Hipótesis Nula (H0)
- ✓ Si p-valor < α se aceptara la Hipótesis Alternativa (H1)
- ✓ Siendo α = 5% = 0.05
- ✓ Condición: Se aplica / No se aplica
- ✓ Variable Dependiente: Posibles Riesgos
- ✓ Escala: Intervalo
- ✓ Población: Centro de datos de una entidad financiera
- ✓ Muestra: 24 posibles riesgos ,12 y 12 pre y post respectivamente

Estadística de Contraste de Hipótesis

Para la contrastación de la Hipótesis alterna se ha utilizado la prueba estadística Wilcoxon, dado que los datos recolectados pre y post test corresponden a diferentes muestras y son de característica no paramétricos, cuya regla de decisión y resultados se muestra a continuación en la Tabla N° 4.48

Tabla 0:45: Prueba Estadística Wilcoxon – Hipótesis Especifica I

HIPÓTESIS	CASO	PRUEBA ESTADÍSTICA	ZONA DE RECHAZO
H0 → Me1 = Me2	Comprobación de medianas versus medianas constantes para muestras pre y post de grupos diferentes α = 0.05, nivel de confianza 0.95	Wilcoxon	**p-valor > α** Se acepta la hipótesis nula, en consecuencia, se rechaza la Hipótesis Alterna.
H1 → Me1 < Me2			

Fuente y elaboración propia.

Utilizando el software Minitab versión 17, se obtuvieron los siguientes resultados, tal como se pueden visualizar en la Tabla N° 4.49

Tabla 0:46: Resumen de la Prueba Estadística Wilcoxon – Hipótesis Especifica I

GRADO DE LIBERTAD	PRUEBA DE WILCOXON	P – VALOR	MEDIA ESTIMADA	MEDIA CONTRASTE
12	39.50	1.00	7.50	14.50

Fuente y elaboración propia.

P – valor = 1.00 > 0.05 → Se acepta H0, se rechaza H1

Hipótesis Específica II

H0: Mediante el diseño e implementación de pruebas de simulaciones **NO** se logrará fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras.

H1: Mediante el diseño e implementación de pruebas de simulaciones se logrará fortalecer la capacidad de respuesta ante un evento de desastre en un centro de datos para empresas financieras.

Regla para tomar Decisión Estadística

- ✓ Si p-valor > α se acepta la Hipótesis Nula (H0)
- ✓ Si p-valor < α se aceptara la Hipótesis Alternativa (H1)
- ✓ Siendo α = 5% = 0.05
- ✓ Condición: Se aplica / No se aplica
- ✓ Variable Dependiente: Capacidad de Respuesta
- ✓ Escala: Intervalo
- ✓ Población: Centro de datos de una entidad financiera

- ✓ Muestra: 24 posibles riesgos, 12 y 12 pre y post respectivamente

Estadística de Contraste de Hipótesis

Para la contrastación de la Hipótesis alterna se ha utilizado la prueba estadística Wilcoxon, dado que los datos recolectados pre y post test corresponden a diferentes muestras y son de característica no paramétricos, cuya regla de decisión y resultados se muestra a continuación en la siguiente Tabla N° 4.50

Tabla 0:47: Prueba Estadística Wilcoxon – Hipótesis Especifica II

HIPÓTESIS	CASO	PRUEBA ESTADÍSTICA	ZONA DE RECHAZO
H0 → Me1 = Me2	Comprobación de medianas versus medianas constantes para muestras pre y post de grupos diferentes α = 0.05, nivel de confianza 0.95	Wilcoxon	**p-valor > α** Se acepta la hipótesis nula, en consecuencia, se rechaza la Hipótesis Alterna.
H1 → Me1 < Me2			

Fuente y elaboración propia.

Utilizando el software Minitab versión 17, se obtuvieron los siguientes resultados, tal como se puede observar en la Tabla N° 4.51

Tabla 0:48: Resumen de la Prueba Estadística Wilcoxon – Hipótesis Especifica II

GRADO DE LIBERTAD	PRUEBA DE WILCOXON	P – VALOR	MEDIANA ESTIMADA	MEDIANA CONTRASTE
12	36.50	0.875	29.25	77.50

Fuente y elaboración propia.

P – valor = 0.875 > 0.05 → Se acepta H0, se rechaza H1

Hipótesis Específica III

H0: Mediante el diseño e implementación de planes de respaldo **NO** se logrará optimizar la restauración de la información en un centro de datos para empresas financieras.

H1: Mediante el diseño e implementación de planes de respaldo se logrará optimizar la restauración de la información en un centro de datos para empresas financieras.

Regla para tomar Decisión Estadística

- ✓ Si p-valor > α se acepta la Hipótesis Nula (H0)
- ✓ Si p-valor < α se aceptara la Hipótesis Alternativa (H1)
- ✓ Siendo α = 5% = 0.05
- ✓ Condición: Se aplica / No se aplica
- ✓ Variable Dependiente: Restauración de la Información
- ✓ Escala: Intervalo
- ✓ Población: Centro de datos de una entidad financiera
- ✓ Muestra: 24 posibles riesgos ,12 y 12 pre y post respectivamente

Estadística de Contraste de Hipótesis

Para la contrastación de la Hipótesis alterna se ha utilizado la prueba estadística Wilcoxon, dado que los datos recolectados pre y post test corresponden a diferentes muestras y son de característica no paramétricos, cuya regla de decisión y resultados se muestra a continuación en la siguiente Tabla N° 4.52

Tabla 0:49: Prueba Estadística Wilcoxon – Hipótesis Especifica III

HIPÓTESIS	CASO	PRUEBA ESTADÍSTICA	ZONA DE RECHAZO
H0 → Me1 = Me2	Comprobación de medianas versus medianas constantes para muestras pre y post de grupos diferentes α = 0.05, nivel de confianza 0.95	Wilcoxon	**p-valor > α** Se acepta la hipótesis nula, en consecuencia, se rechaza la Hipótesis Alterna.
H1 → Me1 < Me2			

Fuente y elaboración propia.

Utilizando el software Minitab versión 17, se obtuvieron los siguientes resultados, tal como se puede observar en la Tabla N° 4.53

Tabla 0:50: Resumen de la Prueba Estadística Wilcoxon – Hipótesis Especifica III

GRADO DE LIBERTAD	PRUEBA DE WILCOXON	P – VALOR	MEDIANA ESTIMADA	MEDIANA CONTRASTE
12	37.00	0.906	27.75	40.00

Fuente y elaboración propia.

P – valor = 0.906 > 0.05 → Se acepta H0, se rechaza H1

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Ante los diferentes riesgos que el mundo está viviendo, el desarrollo de una solución de continuidad de negocio debe ser tratado de manera prioritaria y realizado en el corto plazo, considerando la necesidad de responder eficientemente ante determinados eventos inesperados.

- Con la implementación del análisis de vulnerabilidad se logró identificar y reducir en un 49.44 % los posibles riesgos que afectaban adversamente la integridad en el centro de datos.

- Con la implementación de las pruebas de simulaciones se logró fortalecer y mejora en un 63.93 % la capacidad de respuesta ante un evento de desastre en el centro de datos.

- Con la implementación de planes de respaldo se logró optimizar y reducir en un 32.14 % el tiempo total en la restauración de la información en un centro de datos.

- La implementación de un análisis de vulnerabilidad en las organizaciones se ha convertido en una necesidad para las entidades que buscan gestionar adecuadamente los riesgos.

- Las empresas que apliquen planes de respaldo garantizaran una adecuada continuidad en los negocios, cumpliendo ser más seguros, más productivos y más motivante al saber que su información siempre estará disponible.

- Las implementaciones de pruebas de simulación permitirán probar la pertinencia y efectividad de planes, protocolos, procedimientos, guías u otros mecanismos operativos de respuesta ante eventos de desastre.

Recomendaciones

- Reunirse con el personal de trabajo quincenal o mensualmente para identificar los problemas y seguir realizando un mejoramiento continuo.

- Al momento de haber realizado la implementación de la prueba de simulación, la empresa y todos los trabajadores deben tener un compromiso constante, ya que ello favorecerá a los mismos con una mayor rapidez en su capacidad de respuesta.

- Se recomienda realizar capacitaciones con respecto al respaldo de su información al personal de todos los niveles de la empresa, de manera que cuando se restablezca la información, puedan ellos estar satisfechos.

- Es importante que cada cierto tiempo se revisen las estrategias a fin de mejorar la gestión de las organizaciones.

- Se recomienda que las mejoras desarrolladas, sean difundidas y puestas en práctica, ya que redundaran en la seguridad del personal, y beneficios para la empresa.

REFERENCIAS BIBLIOGRÁFICAS

Arend, C. (2008). *Nuevas estrategias de archivado, protección de datos y recuperación ante desastres para el cliente*. Madrid, España: IDC Analyze the Future.

Ávila, V. (2013). *Diseño e implementación de un DRP para Departamento de Ingenierías de la Empresa Continental Tire Andina*. (Tesis de Maestría en Gerencia de Sistemas de Información). Universidad de Cuenta, Cuenca, Ecuador.

Bello, R. (2009). *Evaluación del impacto*. Santiago, Chile: Consultoría ILPES / CEPA.

Bonilla, S. y Carbajal, M. (2013). *Elaboración e Implementación de un Plan de Emergencia y Contingencia para el edificio administrativo, modular de cómputo y el auditorio de la Facultad de Mecánica en la Escuela Superior Politécnica de Chimborazo*. (Tesis de Título en Ingeniero Industrial). Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador.

Castillo, J. (2010). *Nueva propuesta evolutiva para el agrupamiento de documentos en Sistemas de Recuperación de Información.* (Tesis de Grado de Doctor en Ciencias de la Computación). Escuela Técnica Superior de Ingeniería Informática, Alcalá, España.

CIIFEN. (2016). *Aproximación para el Cálculo de Riesgo.* Recuperado de: http://www.ciifen.org/index.php?option=com_content&view=category&id=84&layout=blog&Itemid=111&lang=es

Farro, Z. (2015). *Elaboración de un plan de recuperación ante desastres para una empresa operadora satelital en el Perú y diseño de una estación terrena satelital.* (Tesis de Título de Ingeniero de las Telecomunicaciones). Pontificia Universidad Católica del Perú, Lima, Perú.

García, G. (2015). *Propuesta de un plan de recuperación de desastres (DRP) para una institución educativa en la ciudad de México*. (Tesis de Maestría en Administración). Instituto Politécnico Nacional, Guadalajara, México

Gaspar, J. (2010). *El Plan de Continuidad del Negocio*. Madrid, España: Ediciones Diaz de Santos.

Grupo - EPM. (2016). *Sistema de gestión integral de riesgos*. Montevideo, Uruguay: Obras Sanitarias del Estado.

Hernández, R. (2010). *Metodología de la Investigación*. Guadalajara, México: McGraw-Hill.

ISO. (2008). *Guidelines for information and communications technology disaster recovery services*. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso-iec:22301:ed-1:v1:en

Kosutic, D. (2015). *Paquete Premium ISO 27001 y ISO 22301*. Recuperado de: http://advisera.com/27001academy

Mannella, D. (2012). *Diseño de una guía para la implementación del uso de computación en la nube como mecanismo de recuperación ante desastres tecnológicos en pymes en el DMQ.* (Tesis de Maestría en Gerencia de Sistemas). Escuela Politécnica del Ejercito, Sangolquí, Ecuador.

Matos, M. & Beriguete, M. & Reydi, P. (2015). *Diseño de un Plan de Recuperación ante Desastre (DRP)*. Madrid, España: Editorial Académica Española.

Peña, J. (2008). *Planes de contingencia, recuperación de desastre*. Monterrey, Uruguay: Consultoría en Comunicaciones e Informática S.A. – CCISA

Pretell, H. (2014). *Preparación para desastres en hospitales de emergencia*. Lima, Perú: EsSalud.

Sáez, V. (2015). *Modelo Integral para la implementación de un Plan de Continuidad de Negocio en Chile*. Puerto Montt, Chile: Universidad Austral de Chile.

Sánchez, H. y Reyes, C. (2009). *Metodología y Diseño en la Investigación Científica*. Lima, Perú: Visión Universitaria.

Vicente, N. (2015). *Análisis y evaluación para el diseño de un plan de recuperación ante desastres.* Guayaquil, Ecuador: Universidad Politécnica Salesiana Sede Guayaquil.

Vigo, J. y Cardoso, F. & Mello, C. (2010). *Planes de contingencia y continuidad del negocio*. Montevideo, Uruguay: Universidad de la Republica.

Zanetti, P. y Sabatino, P. (2010). *El arte de recuperarse a bajo costo*. Buenos Aires, Argentina: Universidad Tecnológica Nacional Regional Buenos Aires.

ANEXOS

ANEXO 1: PLAN DE RECUPERACIÓN ANTE DESASTRE (DRP)

ANEXO 2: OBJETIVO DE TIEMPO DE RECUPERACIÓN Y OBJETIVO DE PUNTO DE RESTAURACIÓN